Heston COMMUNITY SCHOOL

DATA PROTECTION POLICIES AND PRIVACY NOTICES

Approved by:	Finance and General Purposes	Date: 18/12/25
Last reviewed on:	December 2025	
Next review due by:	December 2026	

TABLE OF CONTENTS

DOCUMENT OWNER AND APPROVAL

DOCUMENT	APPROVAL
Acceptable Use Policy	Facilities, Premises and Compliance Manager
Acceptable Use Agreement	
Biometrics Policy	
Biometric Consent Form [Parent/Carer]	
Bring Your Own Device Policy	
CCTV policy	
Cookie Policy	
Electronic Information and Communications Systems Policy	
Information Security Policy	
Privacy Notice for Visitors and Contractors	
Cyber Security Policy	
Social Media Policy	
Privacy Notice for Job Applicants	HR Manager
Privacy Notice for Staff	
Data Retention Policy	PA to the Headteacher
Data Retention Schedule	
Privacy Notice for Governors and Volunteers	
Privacy Notice for Parents and Students	
The Publication Scheme	
Record of Processing Activities	
Artificial Intelligence Policy For Students And Parents	SIMS and Data Manager
Artificial Intelligence Staff Policy	
Data Breach Policy	
Data Protection Policy [Including Subject Access Request]	
Subject Access Request Form	
Data Protection Impact Assessment	
Data Protection Impact Assessment Form in Full	
Legitimate Interest for DPIA	
Data Sharing Agreement	
Freedom of Information Policy and Publication Scheme	
GDPR - 10 Steps We Can Take Now	

POLICY REVIEW AND FINAL APPROVAL

All policies have been reviewed and approved by the Senior Leadership Team, Headteacher and Governing Body.

ACCEPTABLE USE POLICY

INTRODUCTION

This policy is designed to enable acceptable use for staff and Governors.

The School provides a range of ICT resources which are available to staff members and Governors. In order to ensure the safety of both staff, Governors and students, it is important that all staff members and Governors follow the guidelines detailed below.

This policy aims to:

Promote the professional, ethical, lawful and productive use of the School's ICT systems and infrastructure

- Define and identify unacceptable use of the School's ICT systems and external systems
- Educate users about their data security responsibilities
- Describe why monitoring of the ICT systems may take place
- Define and identify unacceptable use of social networking sites and School devices
- Specify the consequences of non-compliance.

This policy applies to staff members and Governors, and all users of the School's ICT systems are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to the Facilities, Premises and Compliance Manager.

PROVISION OF ICT SYSTEMS

All equipment that constitutes the School's ICT systems is the sole property of the School.

No personal equipment should be connected to or used with the School's ICT systems. Users must not try to install any software on the ICT systems without permission from the Facilities, Premises and Compliance Manager. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

The Facilities, Premises and Compliance Manager is responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptop/desktop computers or ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

Users are not permitted to make any physical alteration, either internally or externally, to the School's computer and network hardware.

NETWORK ACCESS AND SECURITY

All users of the ICT systems at the School must first be registered. Following registration, a network user account will be created, consisting of a username, password and an e-mail address. All passwords should be complex to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.

All users are personally responsible and accountable for all activities carried out under their user account[s]. Users must take all reasonable precautions to protect their user account details and must not share them with any other person, except to designated members of the IT Network Team for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to SIMS and Data Manager as soon as possible.

Users should only access areas of the School's computer systems to which they have authorised access.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the School's ICT systems, or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the School's ICT systems or cause difficulties for any other users.

Under no circumstances should a student be allowed to use a staff computer account, unless being directly supervised by the account owner.

SCHOOL EMAIL

Where email is provided, it is for academic and professional use, with reasonable personal use being permitted. Personal use should be limited to short periods during recognised break times and comply with this Acceptable Use Policy. The School's email system can be accessed from both the School computers, and via the internet from any computer. Wherever possible, all School related communication must be via the School email address.

The sending of emails is subject to the following rules:

- Language must not include swear words, or be offensive or abusive
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted
- Sending of attachments which contain copyright material to which the School does not have distribution rights is not permitted
- The use of personal email addresses by staff for any official School business is not permitted
- The forwarding of any chain messages/emails etc is not permitted. Spam or junk mail will be blocked and reported to the email provider
- Any electronic communication which contains any content which could be subject to data protection legislation [e.g. sensitive or personal information] will only be sent using secure and encrypted email or password protection
- Emails should never contain children's full names either in the subject line or preferably not in the main body of the text. Initials should be used wherever possible
- Access to School/setting email systems will always take place in accordance to data protection legislation and in line with other appropriate School/setting policies e.g. confidentiality.

- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the relevant files/records [such as safeguarding]
- Staff will be encouraged to develop an appropriate work life balance when responding to email
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on School headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts
- Where possible emails must not contain personal opinions about other individuals, e.g. other staff members, children or parents. Descriptions of individuals must be kept in a professional and factual manner.

INTERNET ACCESS

Internet access is provided for academic and professional use, with reasonable personal use being permitted. Priority must always be given to academic and professional use.

The School's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a School. In this case the website must be reported immediately to a member of the IT Network Team.

Staff must not therefore access from the School's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct [this list is not exhaustive]:

- Accessing pornographic material [that is writings, pictures, films, video clips of a sexually explicit or arousing nature], racist or other inappropriate or unlawful materials
- Transmitting a false and/or defamatory statement about any person or organisation;
- Sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others
- Transmitting confidential information about the School and any of its staff, students or associated third parties
- Transmitting any other statement which is likely to create any liability [whether criminal or civil, and whether for the employee or for the School]
- Downloading or disseminating material in breach of copyright
- Engaging in online chat rooms, instant messaging, social networking sites and online gambling
- Forwarding electronic chain letters and other materials
- Accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary such information may be handed to the police in connection with a criminal investigation.

DIGITAL CAMERAS

The School encourages the use of digital cameras and video equipment; however staff should be aware of the following guidelines:

- Photos should only be named with the student's name if they are to be accessible in School only and if consent has been received
- Student consent has been given
- The use of personal digital cameras in School is not permitted, including those which are integrated into mobile phones, iPads or similar
- All photos should be downloaded to the School network as soon as possible
- The use of mobile phones for taking photos of students is not permitted.

FILE STORAGE

Staff members have their own personal area on the network, as well as access to shared network drives. Any School related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files. Any files stored on removable media must be stored in accordance with the Information Security Policy, summarised as follows:

- If information/data has to be transferred it must be saved on an encrypted, password protected, storage device
- No School data is to be stored on a home computer, or un-encrypted storage device
- No confidential, or School data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email
- To eliminate the need for manual removal of files from the Schools Network, School files can be accessed by all staff remotely and securely using CC4 Access.

MOBILE PHONES

Mobile phones are permitted in School, with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children. Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard/locker
- Personal mobile phone cameras are not to be used on School trips. The School provides [digital cameras/trip phones] for this purpose
- All phone contact with parents regarding School issues will be through the School's phones. Personal mobile numbers should not be given to parents at the School.

USE OF WHATSAPP

WhatsApp is not permitted for use on School issued devices or personal devices for School business. Members of staff are able to use WhatsApp on their own devices for personal communication. However, staff should not communicate internally with other staff members for School business using their personal WhatsApp accounts, sharing School related information which could include categories of personal data.

SOCIAL NETWORKING

The School has a Social Media Policy which should be read in conjunction with this policy. The key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the School, staff and students at all times and that they treat colleagues, students and associates of the School with professionalism and respect whilst using social networking sites
- Social networking sites should be used responsibly and users should ensure that neither their personal or professional reputation and/or the School's reputation, nor the reputation of individuals within the School are compromised by inappropriate postings
- Use of social networking sites for School business is not permitted, unless via an officially recognised School site and with the permission of the Facilities, Premises and Compliance Manager
- Members of staff will notify the Facilities, Premises and Compliance Manager if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the School/setting
- No School information, communication, documents, videos and/or images should be posted on any personal social networking sites
- No details or opinions relating to any student are to be published on any website
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others [cyber bullying] via social networking sites
- No opinions regarding another member of staff, which could cause offence, are to be posted
- No photos or videos, which show students of the School who are not directly related to the person posting them, should be uploaded to any site other than the School's website
- No comment, images or other material may be posted anywhere, by any method that may bring the School or, the profession into disrepute
- Users must not give students access to their area on a social networking site, [for example adding a student as a friend on Facebook]. If, in exceptional circumstances, users wish to do so, please seek advice from Facilities, Premises and Compliance Manager.

MONITORING OF THE ICT SYSTEMS

The School may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the School's ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by the Facilities, Premises and Compliance Manager to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

Other reasons for monitoring the ICT systems include the need to:

- Ensure operational effectiveness of the services provided
- Maintain the systems
- Prevent a breach of the law, this policy, or any other School policy
- Investigate a suspected breach of the law, this policy, or any other School policy.

FAILURE TO COMPLY WITH THE POLICY

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

Any unauthorised use of the School's ICT systems, Cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which the Facilities, Premises and Compliance Manager considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The School reserves the right to audit and/or suspend a user's network, e-mail and/or application account[s] pending an enquiry, without notice to the user concerned.

ACCEPTABLE USE AGREEMENT

TO BE COMPLETED BY ALL STAFF

As a School user of the network resources/equipment, I hereby confirm that I have read and understood the Acceptable Use Policy and that I agree to follow the School rules [set out within this policy] on its use. I will use the network/equipment in a responsible way and observe all the restrictions explained in the School's Acceptable Use Policy. If I am in any doubt I will consult the Facilities, Premises and Compliance Manager.

I agree to report any misuse of the network to the Facilities, Premises and Compliance Manager. Moreover, I agree to report any websites that are available on the School internet that contain inappropriate material to the Facilities, Premises and Compliance Manager.

I finally agree to ensure that portable equipment such as cameras, iPads or laptops will be kept secured when not in use and to report any lapses in physical security to the SIMS and Data Manager.

Specifically when using School devices:

- I must not use these devices for inappropriate purposes
- I must only access those services I have been given permission to use
- I will not download, use or upload any material which is unsuitable within a School setting or that may cause disruption to the School network.

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I understand that the School will monitor communications in order to uphold this policy and to maintain the School's network [as set out within this policy].

Signed _____ Date _____

Print Name _____ Job Title _____

BIOMETRICS POLICY

WHAT IS BIOMETRIC DATA?

Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

All biometric data is considered to be Special Category Data under the UK General Data Protection Regulation [UK GDPR]. This means the data is more sensitive and requires more protection and this type of data could create more significant risks to a person's fundamental rights and freedoms.

This policy complies with The Protection of Freedoms Act 2012 [sections 26 to 28], the Data Protection Act 2018 and the UK GDPR.

The School has carried out a Data Protection Impact Assessment with a view to evaluating whether the use of biometric data is a necessary and proportionate means of achieving the legitimate objectives set out below.

The result of the Data Protection Impact Assessment has informed the School's use of biometrics and the contents of this policy

WHAT IS AN AUTOMATED BIOMETRIC RECOGNITION SYSTEM?

An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' i.e. electronically. Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.

THE LEGAL REQUIREMENTS UNDER UK GDPR.

'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including [but not limited to] disclosing it, deleting it, organising it or altering it.

As biometric data is Special Category Data in order to lawfully process this data, the School must have a legal basis for processing personal data and a separate condition for processing Special Category Data. When processing biometric data, the School relies on explicit consent [which satisfies the fair processing conditions for personal data and Special Category Data]. Consent is obtained from the parents/carers.

The School processes biometric data as an aim to make significant improvements to our canteen lunch facilities and Learning Resource Centre. This is to ensure efficiency and to do away with the need for swipe cards and cash being used, to safeguard the children.

Facial recognition technology is likely to result in high data protection risks under UK GDPR. We have carried out a Data Protection Impact Assessment [DPIA] prior to its use. In addition, we have consulted parents and students about its use. We have alternatives available if someone prefers to not given their explicit consent for its use, for example [DETAILS OF ALTERNATIVES AVAILABLE, I.E., CARDS].

CONSENT AND WITHDRAWAL OF CONSENT

The School will not process biometric information without the relevant consent.

CONSENT FOR STUDENTS

When obtaining consent for students, both parents will be notified that the School intends to use and process their child's biometric information. The School only requires written consent from one parent [in accordance with the Protection of Freedoms Act 2012], provided no parent objects to the processing.

If a parent objects to the processing, then the School will not be permitted to use that child's biometric data and alternatives will be provided.

The child may also object to the processing of their biometric data. If a child objects, the School will not process or continue to process their biometric data, irrespective of whether consent has been provided by the parent[s].

Where there is an objection, the School will provide reasonable alternatives which will allow the child to access the same facilities that they would have had access to had their biometrics been used.

Students and parents can also object at a later stage to the use of their child's/their biometric data. Should a parent wish to withdraw their consent, they can do so by writing to the School at info@hestoncs.org requesting that the School no longer uses their child's biometric data.

Students who wish for the School to stop using their biometric data should put this in writing to Heston Community School, Heston Road, Hounslow, Middlesex, TW5 0QR, Telephone: 020 8572 1931, Email: info@hestoncs.org.

The consent will last for the time period that your child attends the School [unless it is withdrawn].

CONSENT FOR STAFF

The School will seek consent of staff before processing their biometric data. If a member of staff objects, the School will not process or continue to process the biometric data and will provide reasonable alternatives. Staff who wish for the School to stop using their biometric data should do so by writing to the Facilities, Premises and Compliance Manager.

The consent will last for the time period that the staff member remains employed by the School [unless it is withdrawn].

RETENTION OF BIOMETRIC DATA

Biometric data will be stored by the School for as long as consent is provided [and not withdrawn].

Once a student or staff member leaves, the biometric data will be deleted from the School's system no later than 72 hours.

At the point that consent is withdrawn, the School will take steps to delete their biometric data from the system and no later than 72 hours.

STORAGE OF BIOMETRIC DATA

Biometric data will be kept securely and systems will be put in place to prevent any unauthorised or unlawful access/use.

The biometric data is only used for the purposes for which it was obtained and such data will not be unlawfully disclosed to third parties.

BIOMETRIC CONSENT FORM [PARENT/CARER]

Please complete this form to give consent to Heston Community School for taking and using information from your child's fingerprint as part of an automated biometric recognition system.

This biometric information will be used by the School for the purpose of providing catering and library services.

In signing this form, you are authorising the School to use your child's biometric information for this purpose until he/she either leaves the School or ceases to use the system.

If you wish to withdraw your consent at any time, this must be done so in writing and sent to the School at the following address: Heston Community School, Heston Road, Hounslow, Middlesex, TW5 0QR, Telephone: 0208 572 1931, Email: info@hestoncs.org

Once your child ceases to use the biometric recognition system, his/her biometric information will be securely deleted by the School.

PARENT CONSENT

Having read guidance provided to me by Heston Community School, I give consent to information from the fingerprint of my child being taken and used by Heston Community School. This will be used as part of an automated biometric recognition system for catering and library services.

I understand that an image of my child's fingerprint is not stored. The template/measurements taken from my child's fingerprint is what will be used to permit access to the canteen and library services.

I understand that I can withdraw this consent at any time in writing.

Name of Child _____ Registration Group _____

Parent Name _____ Signature _____

Date _____

Heston Community School, Heston Road, Hounslow, Middlesex, TW5 0QR
Telephone: 0208 572 1931, Email: info@hestoncs.org

BRING YOUR OWN DEVICE POLICY

The School has implemented this policy to protect the School and all parties when using ICT and media devices. Staff are able to use devices at work and outside of work for work related activities provided the terms of this policy are met. The School reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of the School's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. This policy is not designed to offer protection for the device itself. The safety of the user's own device is the responsibility of the user.

Mobile devices within the context of this policy include any mobile phone, tablet, laptop, MP3/iPod or other device which is capable of connecting with the internet or mobile networks or taking image or sound recordings.

This guidance must be read alongside the School's Acceptable Use Policy.

All employees must agree to the terms and conditions set out in this policy in order to be able to connect their devices to the School's network.

ACCEPTABLE USE

- The School embrace the use of new and mobile technologies and acknowledge they are a valuable resource in the classroom having educational purpose
- However by accessing the School's systems and networks, it is likely that staff will use personal data and so must abide by the terms of the Data Protection Act 2018 when doing [including ensuring adequate security of that personal information]
- All staff who wish to use their own devices to access the School's network must sign and return the statement at the conclusion of this policy.
- When in School staff can connect their device via the School's wireless network for security
- When out of School, staff can access work systems on their mobile device using RMUnify or CC4
- All internet access via the network is logged and, as set out in the Acceptable Use Policy, employees are blocked from accessing certain websites whilst connected to the School network
- The use of camera, microphone and/or video capabilities are prohibited whilst in School unless this has been approved by the SIMS and Data Manager. If approved, any pictures, videos or sound recordings can only be used for School purposes and cannot be posted or uploaded to any website or system outside of the School network
- You must not use your device to take pictures/video/recordings of other individuals
- WhatsApp must not be used on personal devices for School related communication. Members of staff are able to use WhatsApp on their own devices for personal communication. However, staff should not communicate internally with other staff members for School business using their personal WhatsApp accounts, sharing School related information which could include categories of personal data.

Non-acceptable Use

Any apps or software that are downloaded onto the user's device whilst using the School's own network is done at the users risk and not with the approval of the School

- Devices may not be used at any time to

    - Store or transmit illicit materials
    - Store or transmit proprietary information belonging to the School
    - Harass others
    - Act in any way against the School's Acceptable Use Policy and other safeguarding and data related policies
- Technical support is not provided by the School on the user's own devices.

DEVICES AND SUPPORT

- Smartphones including iPhones and Android phones are allowed
- Tablets including iPad and Android are allowed.

SECURITY

- Devices must be presented to IT for proper job provisioning and configuration of standard apps such as browsers, office productivity software and security tools, before they can access the network.
- In order to prevent unauthorised access, devices must be password/pin/fingerprint protected using the features of the device and a strong password is required to access the School's network
- When using personal data, it is the user's responsibility to ensure they keep data secure on their device. This includes preventing theft and loss of data [for example through password protection and cloud back up] keeping information confidential [for example by ensuring access to emails or sensitive information is password protected] and maintaining that information
- The School does not accept responsibility for any loss or damage to the user's device when used on the School's premises. It is up to the user to ensure they have their own protection on their own device [such as insurance]
- Staff are prevented from installing email apps which allow direct access to School emails without use of a login/password
- If information is particularly sensitive then users should ensure that the data is either appropriately secured or deleted from the device [including from any local copies which may have been stored on the device
- In the event of any loss or theft of personal data, this must be reported immediately as a data breach in accordance with the School's Data Breach Policy
- The School may require access to a device when investigating policy breaches [for example to investigate cyber bullying]
- Staff are not permitted to share access details to the School's network or Wi-Fi password with anyone else
- The School will not monitor the content of the user's own device but will monitor any traffic over the School system to prevent threats to the School's network.

CCTV POLICY

INTRODUCTION

The School recognises that CCTV systems can be privacy intrusive.

Review of this policy will be repeated regularly, and whenever new equipment is introduced a review will be conducted and a risk assessment put in place. The School aims to conduct reviews no later than every two years.

OBJECTIVES

a) The purpose of the CCTV system is to assist the School in reaching these objectives
b) To protect students, staff and visitors against harm to their person and/or property
c) To increase a sense of personal safety and reduce the fear of crime
d) To protect the School buildings and assets
e) To support the police in preventing and detecting crime
f) To assist in identifying, apprehending and prosecuting offenders
g) To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence
h) To assist in managing the School.

PURPOSE OF THIS POLICY

The purpose of this policy is to regulate the management, operation and use of the CCTV system [closed circuit television] at the School.

CCTV cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets [not including wash basins], changing facilities, etc.

STATEMENT OF INTENT

The CCTV system will seek to comply with the requirements both of the Data Protection Act and the most recent Commissioner's Code of Practice.

The School will treat the system, all information, documents and recordings [both those obtained and those subsequently used] as data protected under the Act.

The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site and make clear who is responsible for the equipment.

Where wireless communication takes place between cameras and a receiver, signals will be encrypted to prevent interception.
Recorded images will only be retained long enough for any incident to come to light [e.g. for a theft to be noticed] and the incident to be investigated. In the absence of compelling a need to retain images for longer [such as an ongoing investigation or legal action], data will be retained for no longer than 30 days.

SYSTEM MANAGEMENT

Access to the CCTV system and data will be password protected.

The CCTV system will be administered and managed by Facilities, Premises and Compliance Manager who takes responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Facilities, Premises and Compliance Manager the system will be managed by the IT Team.

The system and the data collected will only be available to the Facilities, Premises and Compliance Manager, his/her replacement and appropriate members of the Senior Leadership Team as determined by the Headteacher.

The CCTV system is designed to be in operation for 24 hours each day, every day of the year, though the School does not guarantee that it will be working during these hours.

The Facilities, Premises and Compliance Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that cameras are functional.

Cameras have been selected and positioned so as to best achieve the objectives set out in this policy in particular by proving clear, usable images.

Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

Where a person other than the Senior Leadership Team or Learning Coordinators, requests access to the CCTV data or system, the Facilities, Premises and Compliance Manager must satisfy him/herself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists access will be refused.

Details of all visits and visitors will be recorded in a system log book including time/data of access and details of images viewed and the purpose for so doing.

DOWNLOADING CAPTURED DATA ONTO OTHER MEDIA

In order to maintain and preserve the integrity of the data [and to ensure their admissibility in any legal proceedings] any downloaded media used to record events from the hard drive must be prepared in accordance with the following procedures:

a) Each downloaded media must be identified by a unique mark
b) Before use, each downloaded media must be cleaned of any previous recording
c) The Facilities, Premises and Compliance Manager will register the date and time of downloaded media insertion, including its reference

d) Downloaded media required for evidential purposes must be sealed, witnessed and signed by the Facilities, Premises and Compliance Manager, then dated and stored in a separate secure evidence store. If a downloaded media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the Facilities, Premises and Compliance Manager, then dated and returned to the evidence store
e) If downloaded media is archived the reference must be noted.

Images may be viewed by the police for the prevention and detection of crime and by the Facilities, Premises and Compliance Manager, his/her replacement and the Headteacher and other authorised senior leaders. However, where one of these people may be later called as a witness to an offence and where the data content may be used as evidence, it will be preferable if possible, for that person to withhold viewing of the data until asked to do so by the police.

A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.

Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded media [and any images contained thereon] remains the property of the School, and downloaded media [and any images contained thereon] are to be treated in accordance with Data Protection legislation. The School also retains the right to refuse permission for the police to pass the downloaded media [and any images contained thereon] to any other person. On occasions when a Court requires the release of a downloaded media this will be produced from the secure evidence store, complete in its sealed bag.

The police may require the School to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until they are needed by the police.

Applications received from outside bodies [e.g. solicitors or parents] to view or release images will be referred to the School's Data Protection Officer and a decision made by a senior leader of the School in consultation with the School's Data Protection Officer.

COMPLAINTS ABOUT THE USE OF CCTV

Any complaints in relation to the School's CCTV system should be addressed to the PA to the Headteacher.

REQUEST FOR ACCESS BY THE DATA SUBJECT

The Data Protection Act provides Data Subjects – those whose image has been captured by the CCTV system and can be identified - with a right to access data held about themselves, including those obtained by CCTV. Requests for such data should be made to the PA to the Headteacher.

PUBLIC INFORMATION

Copies of this policy will be available to the public from the School office.

COOKIE POLICY

The School asks that you read this Cookie Policy carefully as it contains important information on and our use of cookies on our website.

WHAT ARE COOKIES?

Cookies are small data files that are placed on your computer or mobile device when you visit a website. Cookies are widely used by online service providers to help build a profile of users. Some of this data will be aggregated or statistical, which means that the School will not be able to identify you individually.

You can set your browser not to accept cookies and the websites below explain how to remove cookies from your browser. However, some of our website features may not function as a result.

TYPES OF COOKIES

The cookies the School places on your device fall into the following categories:

- **Targeting cookies** — also known as advertising cookies, these cookies are used to deliver adverts relevant to you and your interests. They are also used to limit the number of times you see an advertisement on our website and help measure the effectiveness of the advertising campaign. They are usually placed by advertising networks with the website operator's permission. They remember that you have visited a website and this information is shared with other organisations such as advertisers.
- **Persistent Cookies:** These are stored on your device in between browser sessions. These allow your preferences or actions across our website to be remembered. These will remain on your device until they expire, or you delete them from your cache.
- **Session cookies** — these cookies allow our website to link your actions during a particular browser session. They expire each time you close your browser and do not remain on your device afterwards.
- **Strictly Necessary Cookies: T**hese cookies are essential for you to be able to navigate our website and use its features. Without these cookies, the services you have asked for could not be provided.
- **Performance Cookies**: These cookies collect information about how you use our website, e.g. which pages you go to most often. These cookies do not collect personally identifiable information about you. All information collected by these cookies is aggregated and anonymous, and is only used to improve how our website works.
- **Functionality Cookies: T**hese cookies allow our website to remember the choices you make [such as your user name, language, last action and search preferences] and provide enhanced, more personal features. The information collected by these cookies is anonymous and cannot track your browsing activity on other websites.

THE COOKIES THE SCHOOL USES

The table below provides more information about the cookies the School uses and why:

The cookies the School uses	What they do

You Tube Videos	This cookie is set by the YouTube video service and aims to limit repeat advertising and deliver more relevant advertising to you.

The School would suggest contacting your webpage provider for further details about what cookies are used and what they do.

HOW THE SCHOOL USES YOUR COOKIES

Heston Community School may request cookies to be set on your computer or device. Cookies are used to let us know when you visit our website, how you interact with us and to make your experience using the School website better for you. The cookies the School collects will differ depending on what you are looking at on our website. You are able to adapt your cookie preferences, but by blocking certain types of cookie it may mean that your experience on the website is impacted.

CONSENT TO USE COOKIES

The School asks for your permission [consent] to place cookies or other similar technologies on your device, except where these are essential for us to provide you with a service that you have requested [e.g. to enable you to put items in your shopping basket and use our check-out process].

There is a notice on our home page which describes how the School uses cookies and requests your consent to place cookies on your device.

HOW TO TURN OFF COOKIES

If you do not want to accept cookies, you can change your browser settings so that cookies are not accepted. If you do this, please be aware that you may lose some of the functionality of this website. For further information about cookies and how to disable them please go to the Information Commissioner's webpage on cookies: https://ico.org.uk/for-the-public/online/cookies/.

HOW TO CONTACT US

Please contact the School if you have any questions about this Cookie Policy.

If you wish to contact the School, please send an email to the School at info@hestoncs.org.

DATA BREACH POLICY

The UK General Data Protection Regulation [UK GDPR] aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The UK GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the School of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

DEFINITIONS

PERSONAL DATA

Personal data is any information relating to an individual where the individual can be identified [directly or indirectly] from that data alone or in combination with other identifiers the School possesses or can reasonably access. This includes Special Category Data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual [for examples a name, email address, location or date of birth] or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

SPECIAL CATEGORY DATA

Previously termed 'Sensitive Personal Data', Special Category Data is similar by definition and refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

PERSONAL DATA BREACH

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or Special Category Data transmitted, stored or otherwise processed.

DATA SUBJECT

Person to whom the personal data relates.

ICO

ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

RESPONSIBILITY

The Headteacher has overall responsibility for breach notification within the School. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

In the absence of the Headteacher, please do contact the Deputy Headteacher.

The Data Protection Officer [DPO] is responsible for overseeing this policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed.

The DPO's contact details are set out below:

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0203 326 9174
Lead Contact: Craig Stilwell

SECURITY AND DATA-RELATED POLICIES

Staff should refer to the following policies that are related to this Data Protection Policy:

- Information Security Policy which sets out the School's guidelines and processes on keeping personal data secure against loss and misuse.
- Data Protection Policy which sets out the School's obligations under UK GDPR about how they process personal data.
- Cyber Security Policy which sets out the School's obligations and guidelines for cyber security issues.

These policies are also designed to protect personal data and can be found on the School's website https://www.hestoncommunitySchool.co.uk/

DATA BREACH PROCEDURE

WHAT IS A PERSONAL DATA BREACH?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or Special Category Data transmitted, stored or otherwise processed.

Examples of a data breach could include the following [but are not exhaustive]:

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file [this includes accidental loss]
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error [for example sending an email or SMS to the wrong recipient]
- Unforeseen circumstances such as a fire or flood
- Hacking, phishing and other 'blagging' attacks where information is obtained by deceiving whoever holds it.

WHEN DOES IT NEED TO BE REPORTED

The School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes:

- Potential or actual discrimination
- Potential or actual financial loss
- Potential or actual loss of confidentiality
- Risk to physical safety or reputation
- Exposure to identity theft [for example through the release of non-public identifiers such as passport details]
- The exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

REPORTING A DATA BREACH

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should:

- Complete a Data Breach Report Form which can be obtained from the SIMS and Data Manager
- Email the completed form to info@hestoncs.org

Where appropriate, you should liaise with your Line Manager about completion of the Data Report Form. Breach reporting is encouraged throughout the School and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from the SIMS and Data Manager.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The SIMS and Data Manager will acknowledge receipt of the data breach report and take appropriate steps to deal with the report in collaboration with the DPO.

MANAGING AND RECORDING THE BREACH

On being notified of a suspected personal data breach, the SIMS and Data Manager will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:

- Where possible, contain the data breach
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed
- Assess and record the breach in the School's Data Breach Register
- Notify the ICO where required
- Notify Data Subjects affected by the breach if required
- Notify other appropriate parties to the breach
- Take steps to prevent future breaches.

Containment and Recovery

[NAME] with the support of our DPO will identify how the breach occurred and take immediate steps to stop of minimise further loss, destruction or unauthorised disclosure of personal data.

[NAME] with the support of our DPO will identify ways to recover, correct or delete data. This may include contacting the police, e.g., where the breach involves stolen hardware or data.

Depending on the nature of the breach, [NAME] with the support of our DPO, will notify [Professional Indemnity Insurer and/or cyber insurer and/or crime insurer], as the insurer can provide access to data breach management experts.

NOTIFYING THE ICO

Craig Stilwell, Data Protection Officer, will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays [I.e. it is not 72 working hours]. If the School are unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

NOTIFYING DATA SUBJECTS

Where the data breach is likely to result in a high risk to the rights and freedoms of Data Subjects, The SIMS and Data Manager will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures the School has or intends to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, the SIMS and Data Manager will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities [such as the police].

If it would involve disproportionate effort to notify the Data Subjects directly [for example, by not having contact details of the affected individual] then the School will consider alternative means to make those affected aware [for example by making a statement on the School website] https://www.hestoncommunitySchool.co.uk/

NOTIFYING OTHER AUTHORITIES

The School will need to consider whether other parties need to be notified of the breach. For example:

- Insurers
- Parents
- Third parties [for example when they are also affected by the breach]
- Local Authority
- The police [for example if the breach involved theft of equipment or data].

This list is non-exhaustive.

ASSESSING THE BREACH

Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

The School will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. The School will identify ways to recover, correct or delete data [for example notifying our insurers or the police if the breach involves stolen hardware or data].

Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken [for example notifying the ICO and/or Data Subjects as set out above]. These factors include:

- What type of data is involved and how sensitive it is
- The volume of data affected
- Who is affected by the breach [i.e. the categories and number of people involved]
- The likely consequences of the breach on affected Data Subjects following containment and whether further issues are likely to materialise
- Are there any protections in place to secure the data [for example, encryption, password protection, pseudonymisation]
- What has happened to the data
- What could the data tell a third party about the Data Subject
- What are the likely consequences of the personal data breach on the School
- Any other wider consequences which may be applicable.

PREVENTING FUTURE BREACHES

Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, the School will:

- Establish what security measures were in place when the breach occurred
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice
- Consider whether it is necessary to conduct a privacy or Data Protection Impact Assessment
- Consider whether further audits or data protection steps need to be taken
- To update the data breach register
- To debrief Governors/management following the investigation.

REPORTING DATA PROTECTION CONCERNS

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and the School would encourage you to report any concerns [even if they do not meet the criteria of a data breach] that you may have to the SIMS and Data Manager or the DPO. This can help capture risks as they emerge, protect the School from data breaches and keep our processes up to date and effective.

TRAINING

The School will ensure that staff are trained and aware on the need to report data breaches to ensure that they know to detect a data breach and the procedures of reporting them. This policy will be shared with staff.

MONITORING

The School will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

DATA PROTECTION POLICY [INCLUDING SUBJECT ACCESS REQUESTS]

INTRODUCTION

The UK General Data Protection Regulation [UK GDPR] ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how the School handles the personal data of our students, parents, suppliers, employees, workers and other third parties.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedures up to and including summary dismissal depending on the seriousness of the breach.

The School is registered with the Information Commissioners Office [ICO] as required. ICO number Z4886326.

SECTION 1 - DEFINITIONS

PERSONAL DATA

Personal data is any information relating to an individual where the individual can be identified [directly or indirectly] from that data alone or in combination with other identifiers the School possesses or can reasonably access. This includes Special Category Data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual [for examples a name, email address, location or date of birth] or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

SPECIAL CATEGORY DATA

Previously termed 'Sensitive Personal Data', Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

DATA SUBJECT

An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

DATA CONTROLLER

The organisation storing and controlling such information [i.e. the School] is referred to as the Data Controller.

PROCESSING

Processing data involves any activity that involves the use of personal data. This includes but is not limited to obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

AUTOMATED PROCESSING

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing [without human intervention] which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

DATA PROTECTION IMPACT ASSESSMENT [DPIA]

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

CRIMINAL RECORDS INFORMATION

This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

SECTION 2 - WHEN CAN THE SCHOOL PROCESS PERSONAL DATA, DATA PROTECTION PRINCIPLES

The School is responsible for and adhere to the principles relating to the processing of personal data as set out in the UK GDPR. The principles the School must adhere to are set out below.

PRINCIPLE 1: PERSONAL DATA MUST BE PROCESSED LAWFULLY, FAIRLY AND IN A TRANSPARENT MANNER

The School will only collect, process and share personal data fairly and lawfully and for specified purposes. The School must have a specified purpose for processing personal data and special category of data as set out in the UK GDPR.

Before the processing starts for the first time, the School will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. The School will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis [i.e. that there is no other reasonable way to achieve that purpose].

PERSONAL DATA

The School may only process a Data Subject's personal data if one of the following fair processing conditions are met:

- The Data Subject has given their consent
- The processing is necessary for the performance of a contract with the Data Subject or for taking steps at their request to enter into a contract
- To protect the Data Subject's vital interests
- To meet our legal compliance obligations [other than a contractual obligation]
- To perform a task in the public interest or in order to carry out official functions as authorised by law
- For the purposes of the School's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the Data Subject.

SPECIAL CATEGORY DATA

The School may only process Special Category Data if they are entitled to process personal data [using one of the fair processing conditions above] AND one of the following conditions are met:

- The Data Subject has given their explicit consent
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the School in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay
- To protect the Data Subject's vital interests
- To meet our legal compliance obligations [other than a contractual obligation]
- Where the data has been made public by the Data Subject
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- Where it is necessary for reasons of public interest in the area of public health
- The processing is necessary for archiving, statistical or research purposes.

The School identifies and documents the legal grounds being relied upon for each processing activity.

CONSENT

Where the School relies on consent as a fair condition for processing [as set out above], it will adhere to the requirements set out in the UK GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon [i.e. more than just mere action is required].

A Data Subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data Subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

If explicit consent is required, the School will normally seek another legal basis to process that data. However if explicit consent is require the Data Subject will be provided with full information in order to provide explicit consent.

The School will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

PRINCIPLE 2: PERSONAL DATA MUST BE COLLECTED ONLY FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

Personal data will not be processed in any matter that is incompatible with the legitimate purposes.

The School will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless the School has informed the Data Subject of the new purpose [and they have consented where necessary].

PRINCIPLE 3: PERSONAL DATA MUST BE ADEQUATE, RELEVANT AND LIMITED TO WHAT IS NECESSARY IN RELATION TO THE PURPOSES FOR WHICH IT IS PROCESSED

The School will only process personal data when our obligations and duties require us to. The School will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the School will delete or anonymise the data. Please refer to the School's Data Retention Policy for further guidance.

PRINCIPLE 4: PERSONAL DATA MUST BE ACCURATE AND, WHERE NECESSARY, KEPT UP TO DATE

The School will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. The School will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data Subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data Subjects have the right to request rectification to incomplete or inaccurate data held by the School.

PRINCIPLE 5: PERSONAL DATA MUST NOT BE KEPT IN A FORM WHICH PERMITS IDENTIFICATION OF DATA SUBJECTS FOR LONGER THAN IS NECESSARY FOR THE PURPOSES FOR WHICH THE DATA IS PROCESSED

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The School will ensure that they adhere to legal timeframes for retaining data.

The School will take reasonable steps to destroy or erase from our systems all personal data that the School no longer require. The School will ensure that Data Subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the School's Data Retention Policy for further details about how the School retains and removes data.

PRINCIPLE 6: PERSONAL DATA MUST BE PROCESSED IN A MANNER THAT ENSURES ITS SECURITY USING APPROPRIATE TECHNICAL AND ORGANISATIONAL MEASURES TO PROTECT AGAINST UNAUTHORISED OR UNLAWFUL PROCESSING AND AGAINST ACCIDENTAL LOSS, DESTRUCTION OR DAMAGE

In order to assure the protection of all data being processed, the School will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as:

- Encryption
- Pseudonymisation [this is where the School replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure]
- Ensuring authorised access [i.e. that only people who have a need to know the personal data are authorised to access it]
- Adhering to confidentiality principles
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The School will follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The School will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

Full details on the School's security measures are set out in the Information Security Policy.

SHARING PERSONAL DATA

The School will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. The following points will be considered:

- Has a need to know the information for the purposes of providing the contracted services
- Sharing the personal data complies with the privacy notice that has been provided to the Data Subject and, if required, the Data Subject's consent has been obtained
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place
- The transfer complies with any applicable cross border transfer restrictions

- A fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

There may be circumstances where the School is required either by law or in the best interests of our students, parents or staff to pass information onto external authorities, for example, the Local Authority, Ofsted or the department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of the School will be clearly defined within written notifications and details and basis for sharing that data given.

TRANSFER OF DATA OUTSIDE THE EUROPEAN ECONOMIC AREA [EEA]

The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

The School will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the School's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

TRANSFER OF DATA OUTSIDE THE UK

The School may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, standard data protection clauses or compliance with an approved code of conduct.

SECTION 3 - DATA SUBJECT'S RIGHTS AND REQUESTS

Personal data must be made available to Data Subjects as set out within this policy and Data Subjects must be allowed to exercise certain rights in relation to their personal data.

The rights Data Subjects have in relation to how the School handles their personal data are set out below:

a) [Where consent is relied upon as a condition of processing] To withdraw consent to processing at any time
b) Receive certain information about the School's processing activities
c) Request access to their personal data that the School holds [see Subject Access Requests]
d) Prevent our use of their personal data for marketing purposes
e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data
f) Restrict processing in specific circumstances
g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest
h) Request a copy of an agreement under which personal data is transferred outside of the EEA
i) Object to decisions based solely on automated processing

j) Prevent processing that is likely to cause damage or distress to the Data Subject or anyone else
k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms
l) Make a complaint to the supervisory authority
m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the School to verify the identity of the individual making the request.

DIRECT MARKETING

The School is subject to certain rules and privacy laws when marketing. For example, a Data Subject's prior consent will be required for electronic direct marketing [for example, by email, text or automated calls].

The School will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The School will promptly respond to any individual objection to direct marketing.

EMPLOYEE OBLIGATIONS

Employees may have access to the personal data of other members of staff, suppliers, parents or students of the School in the course of their employment or engagement. If so, the School expects those employees to help meet the School's data protection obligations to those individuals. Specifically, you must:

- Only access the personal data that you have authority to access, and only for authorised purposes
- Only allow others to access personal data if they have appropriate authorisation
- Keep personal data secure [for example by complying with rules on access to School premises, computer access, password protection and secure file storage and destruction [please refer to the Information Security Policy for further details about our security processes]
- Not to remove personal data or devices containing personal data from the School premises unless appropriate security measures are in place [such as pseudonymisation, encryption, password protection] to secure the information
- Not to store personal information on local drives.

SECTION 4 - ACCOUNTABILITY

The School will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. The School is responsible for and demonstrate accountability with the UK GDPR principles.

The School has taken the following steps to ensure and document UK GDPR compliance:

DATA PROTECTION OFFICER [DPO]

Please find below details of the School's Data Protection Officer:

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk
Telephone: 0203 326 9174
Lead Contact: Craig Stilwell

The DPO is responsible for overseeing this Data Protection Policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed, please contact Lipika Acharya [Data Manager] in the first instance. In particular, you must always contact the DPO in the following circumstances:

a) If you are unsure of the lawful basis being relied on by the School to process personal data
b) If you need to rely on consent as a fair reason for processing [please see below the section on consent for further detail]
c) If you need to draft privacy notices or fair processing notices
d) If you are unsure about the retention periods for the personal data being processed [but would refer you to the School's Data Protection Policy in the first instance]
e) If you are unsure about what security measures need to be put in place to protect personal data
f) If there has been a personal data breach [and would refer you to the procedure set out in the School's Data Protection Policy
g) If you are unsure on what basis to transfer personal data outside the EEA
h) If you need any assistance dealing with any rights invoked by a Data Subject
i) Whenever you are engaging in a significant new [or a change in] processing activity which is likely to require a Data Protection Impact Assessment or if you plan to use personal data for purposes other than what it was collected for
j) If you plan to undertake any activities involving automated processing or automated decision making
k) If you need help complying with applicable law when carrying out direct marketing activities
l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

PERSONAL DATA BREACHES

The UK GDPR requires the School to notify any applicable personal data breach to the Information Commissioner's Office [ICO].

The School has put in place procedures to deal with any suspected personal data breach and will notify Data Subjects or any applicable regulator where the School is legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches is the SIMS and Data Manager or your DPO.

TRANSPARENCY AND PRIVACY NOTICES

The School will provide detailed, specific information to Data Subjects. This information will be provided through the School's Privacy Notices [and/or fair processing notices] which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a Data Subject can easily understand them. Privacy notices sets out information for Data Subjects about how the School uses their data and the School's Privacy Notices are tailored to suit the Data Subject.

Whenever the School collects personal data directly from Data Subjects, including for human resources or employment purposes, the School will provide the Data Subject with all the information required by the UK GDPR including the identity of the Data Protection Officer, the School's contact details, how and why the School will use, process, disclose, protect and retain personal data. This will provided in our privacy notice.

When personal data is collected indirectly [for example from a third party or publically available source], the School will provide the Data Subject with the above information as soon as possible after receiving the data. The School will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

Notifications will be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'children' under the UK GDPR

PRIVACY BY DESIGN

The School has adopted a privacy be design approach to data protection to ensure that the School adheres to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the School takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of Data Subjects when implementing data processes.

DATA PROTECTION IMPACT ASSESSMENTS [DPIAS]

In order to achieve a privacy by design approach, the School will conduct DPIAs for any new technologies or programmes being used by the School which could affect the processing of personal data. In any event the School will carry out DPIAs when required by the UK GDPR in the following circumstances:

- For the use of new technologies [programs, systems or processes] or changing technologies
- For the use of automated processing
- For large scale processing of Special Category Data
- For large scale, systematic monitoring of a publicly accessible area [through the use of CCTV].

Our DPIAs contain:

- A description of the processing, its purposes and any legitimate interests used
- An assessment of the necessity and proportionality of the processing in relation to its purpose
- An assessment of the risk to individuals
- The risk mitigation measures in place and demonstration of compliance.

RECORD KEEPING

The School is required to keep full and accurate records of our data processing activities. These records include:

- The name and contact details of the School
- The name and contact details of the Data Protection Officer

- Descriptions of the types of personal data used
- Description of the Data Subjects
- Details of the School's processing activities and purpose
- Details of any third party recipients of the personal data
- Where personal data is store
- Retention periods
- Security measures in place.

TRAINING

The School will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

AUDIT

The School, through its Data Protection Officer, will regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place annually in order to review use of personal data.

RELATED POLICIES

Staff should refer to the following policies that are related to this Data Protection Policy:

Data Retention Policy
Data Breach Policy
Information Security Policy

These policies are also designed to protect personal data and can be found on the School's website.

MONITORING

The School will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.
https://www.hestoncommunitySchool.co.uk/

SECTION 5 - AUTOMATED PROCESSING AND AUTOMATED DECISION MAKING

Generally, automated decision making is prohibited when a decision has a legal or similar significant effect on an individual unless:

a) The Data Subject has given explicit consent;
b) The processing is authorised by law; or
c) The processing is necessary for the performance of or entering into a contract.

If certain types of sensitive data
are being processed, then [b] or [c] above will not be allowed unless it is necessary for the substantial public interest [for example fraud prevention].

If a decision is to be based solely on automated processing, then Data Subjects must be informed of their right to object. This right will be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

The School will also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

The School will carry out a Data Protection Impact Assessment before any automated processing or automated decision making activities are undertaken.

SUBJECT ACCESS REQUESTS

Under Data Protection Law, Data Subjects have a general right to find out whether the School holds or processes personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a Data Subject Access Request [SAR]. The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that the School is undertaking.

The Subject Access Request Form provides guidance for staff members on how data subject access requests should be handled and for all individuals on how to make a SAR.

Failure to comply with the right of access under UK GDPR puts both staff and the School at potentially significant risk and so the School takes compliance with this policy very seriously.

A Data Subject has the right to be informed by the School of the following:

a) Confirmation that their data is being processed
b) Access to their personal data
c) A description of the information that is being processed
d) The purpose for which the information is being processed
e) The recipients/class of recipients to whom that information is or may be disclosed
f) Details of the School's sources of information obtained
g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision-making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct
h) Other supplementary information.

HOW TO RECOGNISE A SUBJECT ACCESS REQUEST

A Data Subject Access Request is a request from an individual [or from someone acting with the authority of an individual, e.g. a solicitor or a parent making a request in relation to information relating to their child]:

- For confirmation as to whether the School processes personal data about him or her and, if so
- For access to that personal data
- And/or certain other supplementary information.

A valid SAR can be both in writing [by letter, email, WhatsApp text] or verbally [e.g. during a telephone conversation]. The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the School holds about me' will be a Data Subject Access Request and should be treated as such.

A Data Subject is generally only entitled to access their own personal data, and not information relating to other people.

HOW TO MAKE A DATA SUBJECT ACCESS REQUEST

Whilst there is no requirement to do so, the School encourages any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the School to recognise easily that you wish to make a Data Subject Access Request and the nature of your request. If the request is unclear/vague the School may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

WHAT TO DO WHEN YOU RECEIVE A DATA SUBJECT ACCESS REQUEST

All Data Subject Access Requests should be immediately directed to the PA to the Headteacher who should contact Judicium as DPO in order to assist with the request and what is required.

ACKNOWLEDGING THE REQUEST

When receiving a SAR the School will acknowledge the request as soon as possible and inform the requester about the statutory deadline [of one calendar month] to respond to the request.

In addition to acknowledging the request, the School may ask for:

- Proof of ID [if needed]
- Further clarification about the requested information
- If it is not clear where the information will be sent, the School must clarify what address/email address to use when sending the requested information
- Consent [if requesting third party data].

The School should work with their DPO in order to create the acknowledgment.

VERIFYING THE IDENTITY OF A REQUESTER OR REQUESTING CLARIFICATION OF THE REQUEST

Before responding to a SAR, the School will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The School is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the School has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the School may ask the requester for more information for the purpose of clarifying the request, but the requester will never be asked why the request has been made. The School will let the requestor know as soon as possible where more information is needed before responding to the request.

In both cases, the period of responding begins when the additional information has been received. If the School does not receive this information, they will be unable to comply with the request.

REQUESTS MADE BY THIRD PARTIES OR ON BEHALF OF CHILDREN

The School needs to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The School may also require proof of identity in certain circumstances.

If the School is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the School should consider whether the child is mature enough to understand their rights. If the School is confident that the child can understand their rights, then the School should usually respond directly to the child or seek their consent before releasing their information.

It will be assessed if the child is able to understand [in broad terms] what it means to make a Subject Access Request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- The child's level of maturity and their ability to make decisions like this
- The nature of the personal data
- Any court orders relating to parental access or responsibility that may apply
- Any duty of confidence owed to the child or young person
- Any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information
- Any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the School is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester, or provide the personal data directly to the child.

The School may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example if it is likely to cause detriment to the child.

FEE FOR RESPONDING TO A SAR

The School will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the School will inform the requester why this is considered to be the case and that the School will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the period of responding begins when the fee has been received.

TIME PERIOD FOR RESPONDING TO A SAR

The School has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The circumstances where the School is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third party requester, the written authorisation of the data subject has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the School will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

SCHOOL CLOSURE PERIODS

Requests received during or just before School closure periods may not be able to be responded to within the one calendar month response period. This is because the School may be closed and there may not be staff on site to comply with the request during this period. As a result, it is unlikely that your request will be able to be dealt with during this time. The School may not be able to acknowledge your request during this time [i.e. until a time when the School receives the request], however, if the School can acknowledge the request the School may still not be able to deal with it until the School re-opens. The School will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

INFORMATION TO BE PROVIDED IN RESPONSE TO A REQUEST

The individual is entitled to receive access to the personal data the School processes about him or her and the following information:

- The purposes for which the School processes the data
- The recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations
- Where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period
- The fact that the individual has the right:
    - To request that the Company rectifies, erases or restricts the processing of his personal data; or
    - To object to its processing
    - To lodge a complaint with the ICO
    - Where the personal data has not been collected from the individual, any information available regarding the source of the data
    - Any automated decision the School has taken about him or her [see paragraph 9 below], together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response will be given in writing if the SAR was made in writing in a commonly-used electronic format.

The information that the School is required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the School has one month in which to respond the School is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

The School is therefore, allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The School is not allowed to amend or delete data to avoid supplying the data.

HOW TO LOCATE INFORMATION

The personal data the School needs to provide in response to a Data Subject Access Request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.
Depending on the type of information requested, the School may need to search all or some of the following:

- Electronic systems, e.g. databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV
- Manual filing systems in which personal data is accessible according to specific criteria, e.g. chronologically ordered sets of manual records containing personal data
- Data systems held externally by our Data Processors [e.g. external payroll service providers]
- Occupational Health Records
- Pensions Data held by the West Yorkshire Pension Fund and Teacher's Pension
- Data held by [insert details of consultants engaged by the School that may hold data,
- e.g. consultants engaged to provide assistance with performance management and/or disciplinary and grievance procedures]
- Capita Payroll Services.

The School should search these systems using the individual's name, employee number or other personal identifier as a search determinant.

PROTECTION OF THIRD PARTIES -EXEMPTIONS TO THE RIGHT OF SUBJECT ACCESS

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The School will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted [for example, after redaction it is still obvious who the data relates to] then the School does not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual [including information identifying the other individual as the source of information] who can be identified from the information unless:

- The other individual has consented to the disclosure; or
- It is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individuals consent, all of the relevant circumstances will be taken into account, including:

- The type of information that they would disclose
- Any duty of confidentiality they owe to the other individual
- Any steps taken to seek consent from the other individual
- Whether the other individual is capable of giving consent
- Any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the Data Subject's right of access against the other individual's rights. If the other person consents to the School disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the School must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

OTHER EXEMPTIONS TO THE RIGHT OF SUBJECT ACCESS

In certain circumstances the School may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The School does not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The School does not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- Education, training or employment of the individual
- Appointment of the individual to any office; or
- Provision by the individual of any service.

This exemption does not apply to confidential references that the School receives from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual [i.e. the person giving the reference], which means that the School must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: The School does not have to disclose any personal data which are subject to legal professional privilege.

Management forecasting: The School does not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The School does not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

REFUSING TO RESPOND TO A REQUEST

The School can refuse to comply with a request if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If a request is found to be manifestly unfounded or excessive the School can:

- Request a 'reasonable fee' to deal with the request
- Refuse to deal with the request

In either case the School needs to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the School should contact the individual promptly and inform them. The School does not need to comply with the request until the fee has been received.

RECORD KEEPING

A record of all Subject Access Requests will be kept by the PA to the Headteacher. The record will include the date the SAR was received, the name of the requester, what data the School sent to the requester and the date of the response.

SUBJECT ACCESS REQUEST FORM

The Data Protection Act 2018 provides you, the Data Subject, with a right to receive a copy of the data/information the School holds about you or to authorise someone to act on your behalf. Please complete this form if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

Proof of identity: The School requires proof of your identity before the School can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving license, official letter addressed to you at your address bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

SECTION 1

Please fill in the details of the Data Subject i.e. the person whose data you are requesting]. If you are not the Data Subject and you are applying on behalf of someone else, please fill in the details of the Data Subject below and not your own.

Title	
Surname/Family Name	
First Name[s] / Forename	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	
I am enclosing the following copies as proof of identity [please tick the relevant box]: ❑ Birth Certificate ❑ Driving Licence ❑ Passport ❑ An official letter to my address	
Personal Information If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year[s] that you think may be relevant.	
Details	
Employment Records If you are, or have been employed by the School and are seeking personal information in relation to your employment please provide details of your Staff number/Unit/Team/Dates of employment.	
Details	

SECTION 2

Please complete this section of the form with your details if you are acting on behalf of someone else i.e. the Data Subject].

If you are NOT the Data Subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the Data Subject and proof of your right to act on their behalf.

Title	
Surname/ Family Name	
First Name[s]/Forenames	
Date of Birth	
Address	
Post Code	
Phone Number	
I am enclosing the following copies as proof of identity [please tick the relevant box]: ❑ Birth Certificate ❑ Driving License ❑ Passport ❑ An official letter to my address	
What is your relationship to the Data Subject? [e.g. parent, carer, legal representative]	
I am enclosing the following copy as proof of legal authorisation to act on behalf of the Data Subject: ❑ Letter of authority ❑ Lasting or Enduring Power of Attorney ❑ Evidence of parental responsibility ❑ Other [give details]:	

SECTION 3

Please describe as detailed as possible what data you request access to [time period/ categories of data/information relating to a specific case/paper records/electronic records].

I wish to: ❑ Receive the information by post* ❑ Receive the information by email ❑ Collect the information in person ❑ View a copy of the information only ❑ Go through the information with a member of staff *Please be aware that if you wish us to post the information to you, the School takes every care to ensure that it is addressed correctly. However, the School cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity by email to the PA to the Headteacher at info@hestoncs.org

DATA RETENTION POLICY

The School has a responsibility to maintain its records and record keeping systems. When doing this, the School will take account of the following factors:

- The most efficient and effective way of storing records and information
- The confidential nature of the records and information stored
- The security of the record systems used
- Privacy and disclosure
- Their accessibility.

This policy does not form part of any employee's contract of employment and is not intended to have contractual effect. It does, however, reflect the School's current practice, the requirements of current legislation and best practice and guidance. It may be amended by the School from time to time and any changes will be notified to employees within one month of the date on which the change is intended to take effect. The School may also vary any parts of this procedure, including any time limits, as appropriate in any case.

DATA PROTECTION

This policy sets out how long employment-related and student data will normally be held by us and when that information will be confidentially destroyed in compliance with the terms of the UK General Data Protection Regulation [UK GDPR] and the Freedom of Information Act 2000.

Data will be stored and processed to allow for the efficient operation of the School. The School's Data Protection Policy outlines its duties and obligations under the UK GDPR.

RETENTION SCHEDULE

Information [hard copy and electronic] will be retained for at least the period specified in the attached retention schedule. When managing records, the School will adhere to the standard retention times listed within that schedule.

Paper records will be regularly monitored by the PA to the Headteacher.

Electronic records will be regularly monitored by the PA to the Headteacher.

The schedule is a relatively lengthy document listing the many types of records used by the School and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements.

DESTRUCTION OF RECORDS

Where records have been identified for destruction they should be disposed of in an appropriate way. All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

All paper records containing personal information, or sensitive policy information should be shredded before disposal where possible. All other paper records should be disposed of by an appropriate waste paper merchant. All electronic information will be deleted.

The School maintains a database of records which have been destroyed and who authorised their destruction. When destroying documents, the appropriate staff member should record in this list at least:

- File reference [or other unique identifier]
- File title/description
- Number of files
- Name of the authorising Officer
- Date destroyed or deleted from system
- Person[s] who undertook destruction.

RETENTION OF SAFEGUARDING RECORDS

Any allegations made that are found to be malicious must not be part of the personnel records.

For any other allegations made, the School must keep a comprehensive summary of the allegation made, details of how the investigation was looked into and resolved and any decisions reached. This should be kept on the personnel files of the accused.

Any allegations made of sexual abuse should be preserved by the School for the term of an inquiry by the Independent Inquiry into Child Sexual Abuse. All other records [for example, the personnel file of the accused] should be retained until the accused has reached normal pension age or for a period of 10 years from the date of the allegation if that is longer. Guidance from the Independent Inquiry Child Sexual Abuse states that prolonged retention of personal data at the request of an Inquiry would not contravene data protection regulation provided the information is restricted to that necessary to fulfil potential legal duties that a School may have in relation to an Inquiry.

Whilst the Independent Inquiry into Child Sexual Abuse is ongoing, it is an offence to destroy any records relating to it. At the conclusion of the Inquiry, it is likely that an indication regarding the appropriate retention periods of the records will be made.

ARCHIVING

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. A database of the records sent to the archives is maintained by the PA to the Headteacher. The appropriate staff member, when archiving documents should record in this list the following information:

- File reference [or other unique identifier]
- File title/description
- Number of files
- Name of the authorising officer.

TRANSFERRING INFORMATION TO OTHER MEDIA

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as digital media or virtual storage centres [such as cloud storage]. The lifespan of the media and the ability to migrate data where necessary should always be considered.

TRANSFERRING INFORMATION TO ANOTHER SCHOOL

We retain the student's educational record whilst the child remains at the School. Once a student leaves the School, the file should be sent to their next school. The responsibility for retention then shifts onto the next school. We retain the file for a year following transfer in case any issues arise as a result of the transfer.
We may delay destruction for a further period where there are special factors such as potential litigation.

RESPONSIBILITY AND MONITORING

The PA to the Headteacher has primary and day-to-day responsibility for implementing this Policy. The Data Protection Officer, in conjunction with the School is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation. The Data Protection Officer will consider the suitability and adequacy of this policy and report improvements directly to management.

Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining and removing records.

Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this Policy and are given adequate and regular training on it.

EMAILS

Emails accounts are not a case management tool in itself. Generally emails may need to fall under different retention periods [for example, an email regarding a health and safety report will be subject to a different time frame to an email which forms part of a student record]. It is important to note that the retention period will depend on the content of the email and it is important that staff file those emails in the relevant areas to avoid the data becoming lost.

STUDENT RECORDS

All Schools with the exception of independent Schools, are under a duty to maintain a student record for each student. If a child changes Schools, the responsibility for maintaining the student record moves to the next School. The School retains the file for a year following transfer in case any issues arise as a result of the transfer.

DATA RETENTION SCHEDULE

FILE DESCRIPTION	RETENTION PERIOD	RESPONSIBILITY
EMPLOYMENT RECORDS		
Job applications and interview records of unsuccessful candidates	6 months after notifying unsuccessful candidates, unless the School has applicants' consent to keep their CVs for future reference. In this case, application forms will give applicants the opportunity to object to their details being retained	HR Manager
Job applications and interview records of successful candidates	7 years after employment ceases	HR Manager
Written particulars of employment, contracts of employment and changes to terms and conditions	7 years after employment ceases	HR Manager
Right to work documentation including identification documents	7 years after employment ceases	HR Manager
Immigration checks	7 years after the termination of employment	HR Manager
DBS checks and disclosures of criminal records forms	As soon as practicable after the check has been completed and the outcome recorded [i.e. whether it is satisfactory or not] unless in exceptional circumstances [for example to allow for consideration and resolution of any disputes or complaints] in which case, for no longer than 6 months.	HR Manager
Change of personal details notifications	No longer than 6 months after receiving this notification	HR Manager
Emergency contact details	Destroyed on termination	HR Manager
Personnel records	While employment continues and up to 7 years after employment ceases	HR Manager
Annual leave records	7 years after the end of tax year they relate to or possibly longer if leave can be carried over from year to year	HR Manager
Consents for the processing of personal and sensitive data	For as long as the data is being processed and up to 7 years afterwards	HR Manager
Working Time Regulations: Opt out forms Records of compliance with WTR	2 years from the date on which they were entered into 2 years after the relevant period	HR Manager
Disciplinary records	7 years after employment ceases	HR Manager
Training	7 years after employment ceases or length of time required by the professional body	HR Manager

FILE DESCRIPTION	RETENTION PERIOD	RESPONSIBILITY
Staff training where it relates to safeguarding or other child related training	Date of the training plus 40 years	HR Manager
Annual appraisal/assessment records	Current year plus 7 years	HR Manager
Professional Development Plans	7 years from the life of the plan	HR Manager
Allegations of a child protection nature against a member of staff including where the allegation is founded	10 years from the date of the allegation or the person's normal retirement age [whichever is longer]. This should be kept under review. Malicious allegations should be removed.	Designated Safeguarding Lead and HR Manager
FINANCIAL AND PAYROLL RECORDS		
Pension Records	12 years	Finance Manager
Retirement Benefits Schemes – Notifiable Events [for example, relating to incapacity]	6 years from the end of the scheme year in which the event took place	Finance Manager
Payroll and Wage Records	6 years after end of tax year they relate to	Finance Manager
Maternity/Adoption/Paternity Leave Records	3 years after end of tax year they relate to	Finance Manager
Statutory Sick Pay	3 years after the end of the tax year they relate to	Finance Manager
Current Bank Details	Until updated plus 3 years	Finance Manager
Bonus Sheets	Current year plus 3 years	Finance Manager
Time Sheets/Clock Cards/Flexitime	Current year plus 3 years	Finance Manager
Student Premium Fund Records	Date student leaves the provision plus 6 years	Finance Manager
National Insurance [Schedule of Payments]	Current year plus 6 years	Finance Manager
Insurance	Current year plus 6 years	Finance Manager
Overtime	Current year plus 3 years	Finance Manager
Annual Accounts	Current year plus 6 years	Finance Manager
Loans and grants managed by the School	Date of last payment on the loan plus 12 years	Finance Manager
All records relating to the creation and management of budgets	Life of the budget plus 3 years	Finance Manager
Invoices, receipts, order books and requisitions, delivery notices	Current financial year plus 6 years	Finance Manager

FILE DESCRIPTION	RETENTION PERIOD	RESPONSIBILITY
Student Grant Applications	Current year plus 3 years	Finance Manager
Student Premium Fund Records	Date student leaves the School plus 7 years	Finance Manager
School Fund Documentation [including but not limited to invoices, cheque books, receipts, bank statements etc].	Current year plus 7 years	Finance Manager
Free School meals registers [where the register is used as a basis for funding]	Current year plus 6 years	Finance Manager
School Meal Registers and Summary Sheets	Current year plus 3 years	Finance Manager
AGREEMENTS AND ADMINISTRATION PAPERWORK		
Collective workforce agreements and past agreements that could affect present employees	Permanently	Academy Business Manager
Trade union agreements	10 years after ceasing to be effective	Academy Business Manager
School Development Plans	3 years from the life of the plan	Academy Business Manager
Visitors Book and Signing In Sheets	6 years	PA to Headteacher
Newsletters and circulars to staff, parents and students	1 year [and the School may decide to archive one copy]	PA to Headteacher
Minutes of Senior Management Team meetings	Date of the meeting plus 3 or as required	PA to Headteacher
Reports created by the Head Teacher or the Senior Management Team.	Date of the report plus a minimum of 3 years or as required	PA to Headteacher
Records relating to the creation and publication of the School Prospectus	Current academic year plus 3 years	PA to Headteacher
HEALTH AND SAFETY RECORDS		
Health and Safety consultations	Permanently	Facilities, Premises and Compliance Manager
Health and Safety Risk Assessments	Life of the risk assessment plus 3 years	Facilities, Premises and Compliance Manager
Health and safety Policy Statements	Life of policy plus 3 years	Facilities, Premises and Compliance Manager
Any records relating to any reportable death, injury, disease or dangerous occurrence	Date of incident plus 3 years provided that all records relating to the incident are held on personnel file	Facilities, Premises and Compliance Manager

FILE DESCRIPTION	RETENTION PERIOD	RESPONSIBILITY
Accident reporting records relating to individuals who are under 18 years of age at the time of the incident	Until the child reaches the age of 21.	Facilities, Premises and Compliance Manager
Accident reporting records relating to individuals who are over 18 years of age at the time of the incident	Accident book should be retained 3 years after last entry in the book	Facilities, Premises and Compliance Manager
Fire precaution log books	Current year plus 3 years	Facilities, Premises and Compliance Manager
Medical records and details of: • control of lead at work • employees exposed to asbestos dust • records specified by the Control of Substances Hazardous to Health Regulations [COSHH]	40 years from the date of the last entry made in the record	Facilities, Premises and Compliance Manager
Records of tests and examinations of control systems and protection equipment under COSHH	7 years from the date on which the record was made	Facilities, Premises and Compliance Manager
TEMPORARY AND CASUAL WORKERS		
Records relating to hours worked and payments made to workers	7 years	Finance Manager
GOVERNING BODY DOCUMENTS		
Instruments of Government	For the life of the School	PA to Headteacher
Meetings schedule	Current year	PA to Headteacher
Minutes – principal set [signed]	10 Years from the date of the meeting	PA to Headteacher
Agendas – principal copy	Where possible the agenda should be stored with the principal set of the minutes	PA to Headteacher
Agendas – additional copies	Date of meeting	PA to Headteacher
Policy documents created and administered by the Governing Body	Until replaced.	PA to Headteacher
Register of attendance at full Governing Board Meetings	Date of last meeting in the book plus 7 years	PA to Headteacher
Annual reports required by the Department of Education	Date of report plus 10 years	PA to Headteacher
Records relating to complaints made to and investigated by the Governing Body or head teacher	Major complaints: current year plus 7 years. If negligence involved: current year plus 15 years. If child protection or safeguarding issues are involved then: current year plus 40 years.	PA to Headteacher

FILE DESCRIPTION	RETENTION PERIOD	RESPONSIBILITY
Correspondence sent and received by the Governing Body or Headteacher	General correspondence should be retained for current year plus 7 years.	PA to Headteacher
Records relating to the terms of office of serving Governors, including evidence of appointment	Date appointment ceases plus 7 years	PA to Headteacher
Register of business interests	Date appointment ceases plus 10 years [Companies Act 2006]	PA to Headteacher
Records relating to the training required and received by Governors	Date appointment ceases plus 7 years	PA to Headteacher
Records relating to the appointment of a clerk to the Governing Body	Date on which clerk appointment ceases plus 7 years	PA to Headteacher
Governor personnel files	Date of appointment plus 7 years	PA to Headteacher
STUDENT RECORDS		
Details of whether admission is successful/unsuccessful	1 year from the date of admission/non-admission	PA to Headteacher
Proof of address supplied by parents as part of the admissions process	Current year plus 1 year	PA to Headteacher
Admissions Register	Entries to be preserved for 7 years from date of entry	Student Welfare Manager
Student Record	Secondary – until the child reaches the age of 25	Student Welfare Manager
Attendance Registers	7 years from the date of entry	Student Welfare Manager
Correspondence relating to any absence [authorised or unauthorised]	Current academic year plus 7 years	Student Welfare Manager
Special Educational Needs files, reviews and Education, Health and Care Plan, including advice and information provided to parents regarding educational needs and accessibility strategy	Date of birth of the student plus 31 years [Education, Health and Care Plan is valid until the individual reaches the age of 25 years – the retention period adds an additional 6 years from the end of the plan].	SENCO
Child protection information [to be held in a separate file].	DOB of the child plus 25 years then review Note: These records will be subject to any instruction given by IICSA	Designated Safeguarding Lead
Exam Results [student copy]	7 year from the date the results are released.	Examinations Officer
Examination Results [School's copy]	Current year plus 6 years	Examinations Officer
Allegations of Sexual Abuse	For the time period of an inquiry by the Independent Inquiry into Child Sexual Abuse.	HR Manager

FILE DESCRIPTION	RETENTION PERIOD	RESPONSIBILITY
Records relating to any allegation of a child protection nature against a member of staff	Until the accused normal retirement age or 10 years from the date of the allegation [whichever is the longer]	HR Manager
Consents relating to School activities as part of UK GDPR compliance [for example, consent to be sent circulars or mailings]	Consent will last whilst the student attends the School.	Person/Curriculum Lead
Mark Books	Current year plus 1 year.	Curriculum Leaders
Schemes of Work	Current year plus 1 year	Curriculum Leaders
Timetable	Current year plus 1 year	Deputy Head
Class Record Books	Current year plus 1 year	Curriculum Leaders
Record of homework set	Current year plus 1 year	Facilities, Premises and Compliance Manager
Photographs of students	For the time the child is at the School and for a short while after. Please note select images may also be kept for longer [for example to illustrate history of the School].	Facilities, Premises and Compliance Manager
Parental consent forms for School trips where there has been no major incident	End of the trip or end of the academic year [subject to a risk assessment carried out by the School]	PA to Headteacher
Parental permission slips for School trips where there has been a major incident	Date of birth of the student involved in the incident plus 25 years. Permission slips for all the students on the trip should be retained to demonstrate the rules had been followed for all students	PA to Headteacher
OTHER RECORDS		
Emails	2-3 years is our recommended timeframe	Facilities, Premises and Compliance Manager
CCTV	Should not be longer than a calendar month	Facilities, Premises and Compliance Manager
Privacy notices	Until replaced plus 6 years.	SIMS & Data Manager
Inventories of furniture and equipment	Current year plus 6 years	Facilities, Premises and Compliance Manager
All records relating to the maintenance of the School carried out by contractors or employees of the School	Whilst the building belongs to the School.	Facilities, Premises and Compliance Manager

FILE DESCRIPTION	RETENTION PERIOD	RESPONSIBILITY
Records relating to the letting of School premises	Current financial year plus 6 years	Facilities, Premises and Compliance Manager
Records relating to the creation and management of Parent Teacher Associations and/or Old Students Associations	Current year plus 6 years then review	PA to Headteacher
Referral forms	While the referral is current	PA to Headteacher
Contact data sheets	Current year then review, if contact is no longer active then destroy	PA to Headteacher

ELECTRONIC INFORMATION AND COMMUNICATIONS SYSTEMS POLICY

INTRODUCTION

The School's electronic communications systems and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of our provision of excellent service.

This policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. It is provided for guidance to all members of staff at the School who are required to familiarise themselves and comply with its contents. The School reserves the right to amend its content at any time.

This policy outlines the standards that the School requires all users of these systems to observe, the circumstances in which the School will monitor use of these systems and the action the School will take in respect of any breaches of these standards.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the UK General Data Protection Regulation [UK GDPR] and all data protection laws and guidance in force.

Staff are referred to the School's Data Protection Policy for further information. The School is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications [Lawful Business Practice] [Interception of Communications] Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

All members of staff are required to comply with the provisions set out in this policy at all times to protect the School's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the School's Disciplinary Procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

The School has the right to monitor all aspects of its systems, including data which is stored under the School's computer systems in compliance with the UK GDPR.

This policy mainly deals with the use [or misuse] of computer equipment, e-mail, internet connection, telephones, iPads [and other mobile device tablets], Blackberries, personal digital assistants [PDAs] and voicemail, but it applies equally to the use of fax machines, copiers, scanners, and the like.

Prohibited use and breach of this policy

We consider this policy to be extremely important. Any breach of the policy will be dealt with under our disciplinary policy. In certain circumstances, breach of this policy may be considered gross misconduct and may result in immediate termination of employment or engagement without notice or payment in lieu of notice. In addition, or as an alternative, we may withdraw an individual's internet and/or email access.

Examples of matters that will usually be treated as gross misconduct include [this list is not exhaustive]:

- unauthorised use of the internet
- creating, transmitting or otherwise publishing any false and defamatory statement about any person or organisation

- creating, viewing, accessing, transmitting or downloading any material which is discriminatory or may cause embarrassment to other individuals, including material which breaches the principles set out in our equality, diversity and inclusion policies
- accessing, transmitting or downloading any confidential information about the School and/or any of our staff and/or current, former or prospective students or parents, suppliers, contractors or other such third parties, except where authorised in the proper performance of your duties
- accessing, transmitting or downloading unauthorised software
- viewing, accessing, transmitting or downloading any material in breach of copyright.

EQUIPMENT SECURITY AND PASSWORDS

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

Passwords are unique to each user and staff are required to select a password that cannot be easily broken and which contains at least 6 characters including both numbers and letters.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Team who will liaise with the Facilities, Premises and Compliance Manager as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If given access to the School e-mail system or to the internet, staff are responsible for the security of their terminals. Staff are required to log off when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Senior Leadership Team and/or the Facilities, Premises and Compliance Manager may do spot checks from time to time to ensure compliance with this requirement.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Logging off prevents another member of staff accessing the system in the user's absence and may help demonstrate in the event of a breach in the user's absence that he or she was not the party responsible.

Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of the Facilities, Premises and Compliance Manager.

On the termination of employment for any reason, staff are required to provide a full handover detailing the drives, folders and files where their work can be located and accessed. The School reserves the right to require employees to hand over all School data held in computer useable format.

Members of staff who have been issued with a laptop, iPad [or other mobile device tablet], PDA or Blackberry must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the machine is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g. ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport documents can be easily read by other passengers.

SYSTEMS USE AND DATA SECURITY

Members of staff should not delete, destroy or modify any of the School's existing systems, programs, information or data which could have the effect of harming or exposing to risk or harm the School's, its staff, students, or any other party.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the Facilities, Premises and Compliance Manager who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

Where consent is given all files and data should always be virus checked before they are downloaded onto the School's systems. If in doubt, the employee should seek advice from the Facilities, Premises and Compliance Manager or a member of the Senior Leadership Team.

The following must never be accessed from the network because of their potential to overload the system or to introduce viruses:

- Audio and video streaming
- Instant messaging
- Chat rooms
- Social networking sites
- Web mail [such as Hotmail or Yahoo].

No device or equipment should be attached to our systems without the prior approval of the Facilities, Premises and Compliance Manager or Senior Leadership Team. This includes, but is not limited to, any PDA or telephone, iPad [or other mobile device tablet], USB device, i-pod, digital camera, MP3 player, infra-red connection device or any other device.

The School monitors all e-mails passing through its systems for viruses. Staff should be cautious when opening e-mails from unknown external sources or where for any reason an e-mail appears suspicious [such as ending in '.exe']. The Facilities, Premises and Compliance Manager should be informed immediately if a suspected virus is received. The School reserves the right to block access to attachments to e-mail for the purpose of effective use of the system and compliance with this policy. The School also reserves the right not to transmit any e-mail message.

Staff should not attempt to gain access to restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

Misuse of the School's computer systems may result in disciplinary action up to and including summary dismissal. For further guidance on what constitutes misuse please see the section entitled Inappropriate Use of the School's Systems and guidance under 'E-mail etiquette and content' below.

E-MAIL ETIQUETTE AND CONTENT

E-mail is a vital business tool, but often lapses inappropriately into an informal means of communication and should therefore be used with great care and discipline.

The School's e-mail facility is intended to promote effective communication within the business on matters relating to the School's business activities and access to the School's e-mail facility is provided for work purposes only.

Staff are permitted to make reasonable personal use of the School's e-mail facility provided such use is in strict accordance with this policy [see Personal Use below]. Excessive or inappropriate personal use of the School's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

Staff should always consider if e-mail is the appropriate medium for a particular communication. The School encourages all members of staff to make direct contact with individuals rather than communicate by e-mail wherever possible to maintain and enhance good working relationships.

Messages sent on the e-mail system should be written as professionally as a letter or fax message and should be concise and directed only to relevant individuals on a need to know basis. The content and language used in the message must be consistent with the School's best practice.

E-mails should never be sent in the heat of the moment or without first checking the content and language and considering how the message is likely to be received. Staff are encouraged wherever practicable to write a draft e-mail first, print it out and review it carefully before finalising and sending. As a rule of thumb if a member of staff would not be happy for the e-mail to be read out in public or subjected to scrutiny then it should not be sent. Hard copies of e-mails should be retained on the appropriate file.

All members of staff should remember that e-mails can be the subject of legal action for example in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc against both the member of staff who sent them and the School. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the School in the same way as the contents of letters or faxes.

Email messages may of course be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail is obliterated and all e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software. This should be borne in mind when considering whether e-mail is an appropriate forum of communication in the circumstances of the case and if so the content and language used.

Staff should assume that e-mail messages may be read by others and not include in them anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain. The School's standard disclaimer should always be used on every e-mail.

Staff should ensure that they access their e-mails at least once every working day, stay in touch by remote access when travelling or working out of the office and should use an out of office response when away from the office for more than a day. Staff should endeavour to respond to e-mails marked 'high priority' as soon as is reasonably practicable.

Members of staff are strictly forbidden from sending abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages. If such messages are received, they should not be forwarded and should be reported to a member of the Senior Leadership Team immediately. If a recipient asks you to stop sending them personal messages then always stop immediately. Where appropriate, the sender of the e-mail should be referred to this policy and asked to stop sending such material.

If you feel that you have been harassed or bullied, or are offended by material sent to you by a colleague via e-mail, you should inform your Line Manager who will usually seek to resolve the matter informally. You should refer to our Equal Opportunities and Diversity Policy and the Anti-Harassment and Bullying Policy for further information and guidance.

If an informal procedure is unsuccessful, you may pursue the matter formally under the School's formal grievance procedure.

AS GENERAL GUIDANCE, STAFF MUST NOT:

- Send any e-mail, including resending and forwarding, containing sexually explicit or otherwise offensive material either internally or externally
- Send any e-mail communication which may be regarded as harassing or insulting. Complaints about the performance or service of other departments or individuals must be made on a face-to-face basis in accordance with normal and courteous practice
- Send or forward private e-mails at work which they would not want a third party to read
- Send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside the School
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them
- Sell or advertise using the systems or broadcast messages about lost property, sponsorship or charitable appeals
- Agree to terms, enter into contractual commitments or make representations by e-mail unless the appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written in ink at the end of a letter
- Download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this
- Send messages containing any reference to other individuals or any other business that may be construed as libellous
- Send messages from another worker's computer or under an assumed name unless specifically authorised
- Send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure
- E-mail may normally only be used to communicate internally with colleagues and students [where appropriate and necessary] and externally to parents, suppliers and third parties on academic/service related issues. Urgent or important messages to family and friends are permitted, but must be of a serious nature
- The School recognises that it is not always possible to control incoming mail. Any material which would be considered as inappropriate or unprofessional, sexually explicit or offensive should be deleted at once. Any member of staff who finds that they are receiving such communications from known sources is responsible for contacting that source in order to request that such communication is not repeated.

- Staff who receive an e-mail which has been wrongly delivered should return it to the sender of the message. If the e-mail contains confidential information or inappropriate material [as described above] it should not be disclosed or forwarded to another member of staff or used in any way. The Facilities, Premises and Compliance Manager should be informed as soon as reasonably practicable.

USE OF THE WEB AND THE INTERNET

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is an inappropriate one such a marker could be a source of embarrassment to the School, especially if a member of staff has accessed, downloaded, stored or forwarded inappropriate material from the website. Staff may even be committing a criminal offence if, for example, the material is pornographic in nature.

Staff must not therefore access from the School's system any web page or any files [whether documents, images or other] downloaded from the web which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition.

As a general rule, if any person within the School [whether intending to view the page or not] might be offended by the contents of a page, or if the fact that the School's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Staff should not under any circumstances use School systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information even in their own time.

Remember also that text, music and other content on the internet are copyright works. Staff should not download or e-mail such content to others unless certain that the owner of such works allows this.

The School's website may be found at www.hestoncommunityschool.co.uk. This website is intended to convey our core values and excellence in the educational sector. All members of staff are encouraged to give feedback concerning the site, and new ideas and inclusions are welcome. All such input should be submitted to the Senior Leadership Team in the first instance. Only expressly authorised and designated members of staff are permitted to make changes to the website.

The School should refrain from texting and using systems such as WhatsApp for School related matters using personal phones. The School require staff to use alternative systems to make contact with staff [such as emails].

The School has published relevant information on its own intranet for the use of all staff. All such information is regarded as confidential to the School and may not be reproduced electronically or otherwise for the purposes of passing it to any individual not directly employed by the School. Any exceptions to this must be authorised by the Facilities, Premises and Compliance Manager who will liaise with the Senior Leadership Team as appropriate and necessary.

OPTIONAL-PERSONAL USE OF THE SCHOOL'S SYSTEMS

The School permits the incidental use of its internet, e-mail and telephone systems to send personal e-mail, browse the web and make personal telephone calls subject to certain conditions set out below.

Our policy on personal use is a privilege and not a right. The policy is dependent upon it not being abused or overused and the School reserve the right to withdraw our permission or amend the scope of this policy at any time.

The following conditions must be met for personal usage to continue:

- Use must be minimal and take place substantially out of normal working hours [that is, during the member of staff's usual break time or shortly, before or after normal working hours]
- Personal e-mails must be labelled 'personal' in the subject header
- Use must not interfere with business or office commitments
- Use must not commit the School to any marginal costs
- Use must comply at all times with the rules and guidelines set out in this policy
- Use must also comply with the School's compliment of operational policies and procedures including but not limited to, the Equal Opportunities and Diversity Policy, Anti-Harassment and Bullying Policy, Data Protection Policy and Code of Conduct.

Staff should be aware that any personal use of the systems may also be monitored [see below] and, where breaches of this policy are found, action may be taken under our Disciplinary Policy and Procedure. Excessive or inappropriate personal use of the School's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

The School reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers that personal use is excessive or otherwise in breach of this policy.

INAPPROPRIATE USE OF EQUIPMENT AND SYSTEMS

Reasonable personal use is permissible provided it is in full compliance with the School's rules, policies and procedures [including this policy, the Equal Opportunities and Diversity Policy, Anti-Harassment Policy, Data Protection Policy, Code of Conduct and Disciplinary Policy and Procedure.

Misuse or abuse of our telephone or e-mail system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the School's Disciplinary Policy and Procedure.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct [this list is not exhaustive]:

- Accessing pornographic material [that is writings, pictures, films, video clips of a sexually explicit or arousing nature], racist or other inappropriate or unlawful materials
- Transmitting a false and/or defamatory statement about any person or organisation

- Sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others
- Transmitting confidential information about the School and any of its staff, students or associated third parties
- Transmitting any other statement which is likely to create any liability [whether criminal or civil, and whether for the employee or for the School
- Downloading or disseminating material in breach of copyright
- Copying, downloading, storing or running any software without the express prior authorisation of the Facilities, Premises and Compliance Manager
- Engaging in online chat rooms, instant messaging, social networking sites and online gambling
- Forwarding electronic chain letters and other materials
- Accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal. Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with our Disciplinary Policy and Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary such information may be handed to the police in connection with a criminal investigation.

FREEDOM OF INFORMATION POLICY AND PUBLICATION SCHEME

INTRODUCTION

The Freedom of Information Act 2000 gives individuals the right to access official information from public bodies. Under the Act, any person has a legal right to ask for access to information held by the School. They are entitled to be told whether the School holds the information, and to receive a copy, subject to certain exemptions. While the Act assumes openness, it recognises that certain information is sensitive. There are exemptions to protect this information. Full details on how requests can be made are set out in section 1 of this policy.

Public Authorities should be clear and proactive about the information they will make public. For this reason, a publication scheme is available and can be found at section 2 of this policy.

This Policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect.

This policy should be used in conjunction with the School's Data Protection Policy.

SECTION 1 – FREEDOM OF INFORMATION REQUESTS

Requests under Freedom of Information should be made to the PA to the Headteacher. However the request can be addressed to anyone in the School; so all staff need to be aware of the process for dealing with requests.

Requests for information that are not data protection or environmental information requests will be covered by the Freedom of Information Act:

- Data Protection enquiries [or Subject Access Requests/SARs] are requests where the enquirer asks to see what personal information the School holds about the enquirer. If the enquiry is a Data Protection request, the School's Data Protection Policy should be followed
- Environmental Information Regulations enquiries are those which relate to air, water, land, natural sites, built environment, flora and fauna, health, and any decisions and activities affecting any of these. These could, therefore, include enquiries about recycling, phone masts, School playing fields, car parking etc. If the enquiry is about environmental information, follow the guidance on the Department for Environment, Food and Rural Affairs [DEFRA] website.

Freedom of Information requests must be made in writing, [including email] and should include the enquirer's name, correspondence address [email addresses are allowed], and state what information they require. There must be enough information in the request to be able to identify and locate the information. If this information is covered by one of the other pieces of legislation [as referred to above], they will be dealt with under the relevant policy/procedure related to that request.

If the request is ambiguous and/or the School requires further information in order to deal with your request, the School will request this further information directly from the individual making the request. Please note that the School does not have to deal with the request until the further information is received. Therefore, the time limit starts from the date that the School receives all information required in order to deal with the request.

The requester does not have to mention the Act, nor do they have to say why they want the information. There is a duty to respond to all requests, telling the enquirer whether or not the information is held, and supplying any information that is held, except where exemptions apply.

Standard Timescale:

- **20 Working Days**: The standard deadline for most public authorities to provide a substantive response after receiving your request
- **Working Days**: Exclude Saturdays, Sundays, and public holidays/bank holidays.

When the Clock Stops/Starts:

- **Clarification Needed**: The 20 days pause until you provide the requested clarification
- **Fees**: The clock stops when a fee notice is issued and restarts upon payment
- **Transfers**: If the authority transfers your request to another body, the original body informs you, and the clock starts for the new body upon their receipt.

Extensions [And Why]:

- **Public Interest Test**: If the authority needs to balance disclosing vs. withholding information, they must inform you within 20 days and can take a reasonable extension [often up to another 20 days]
- **Complex Requests [EIRs]**: Under EIR, complex requests can take up to 40 working days
- **Specific Bodies**: Schools and archives have different rules, sometimes allowing up to 60 working days.

INFORMATION

Provided all requirements are met for a valid request to be made, the School will provide the information that it holds [unless an exemption applies].

Holding information means information relating to the business of the School:

- That the School has created
- That the School has received from another body or person; or
- Held by another body on the School's behalf.

Information means both hard copy and digital information, including email.

If the information is held by another public authority, such as the Local Authority, first check whether they hold the information and if so, transfer the request to them. If this applies, the School will notify the enquirer that they do not hold the information and to whom they have transferred the request. The School will continue to answer any parts of the enquiry in respect of information it does hold.

When the School does not hold the information, it has no duty to create or acquire it just to answer the enquiry; although a reasonable search will be made before confirming whether the School has the information requested.

If the information requested is already in the public domain, for instance, through the Publication Scheme or on the School's website, the School will direct the enquirer to the information and explain how to access it.

The requester has the right to be told if the information requested is held by the School [subject to any of the exemptions]. This obligation is known as the School's duty to confirm or deny that it holds the information. However, the School does not have to confirm or deny if:

- The exemption is an absolute exemption; or
- In the case of qualified exemptions, confirming or denying would itself disclose exempted information.

VEXATIOUS REQUESTS

There is no obligation on the School to comply with vexatious requests. A vexatious request is one which is designed to cause inconvenience, harassment or expense rather than to obtain information, and would require a substantial diversion of resources or would otherwise undermine the work of the School. However, this does not provide an excuse for bad records management.

In addition, the School does not have to comply with repeated identical or substantially similar requests from the same applicant unless a reasonable interval has elapsed between requests.

FEES

Most requests are free, especially if provided via email. However, the School may charge the requester a fee for providing the requested information. This will be dependent on whether the staffing costs in complying with the request exceeds the threshold. The threshold is currently £450. If the request exceeds this [e.g., over a day's work], the School can charge for staff time [finding, retrieving, extracting info] but must notify the requester first.

If a request would cost less than the threshold, then the School can only charge for the cost of informing the applicant whether the information is held, and communicating the information to the applicant [e.g. photocopying, printing and postage cost, but this is often waived below £10].

When calculating costs/threshold, the School can take account of the staff costs/time in determining whether the information is held by the School, locating and retrieving the information, and extracting the information from other documents. The School will not take account of the costs involved with considering whether information is exempt under the Act.

If a request would cost more than the appropriate limit, [£450] the School can turn the request down, answer and charge a fee or answer and waive the fee.

If the School are going to charge they will send the enquirer a fees notice. The School does not have to comply with the request until the fee has been paid. More details on fees can be found on the ICO website.

If planning to turn down a request for cost reasons, or charge a high fee, you should contact the applicant in advance to discuss whether they would prefer the scope of the request to be modified so that, for example, it would cost less than the appropriate limit.

Where two or more requests are made to the School by different people who appear to be acting together or as part of a campaign the estimated cost of complying with any of the requests may be taken to be the estimated total cost of complying with them all.

TIME LIMITS

Compliance with a request must be prompt and within the time limit of 20 School days [this does not include the School holidays or weekends] or 60 working days if this is shorter. Failure to comply could result in a complaint by the requester to the Information Commissioner's Office. The response time starts counting as the first day from the next working day after the request is received [so if a request was received on Monday, 06 October the time limit would start from the next working day, the 07 October].

Where the School has asked the enquirer for more information to enable it to answer, the 20 School days start time begins when this further information has been received.

If some information is exempt this will be detailed in the School's response.

If a qualified exemption applies and the School needs more time to consider the public interest test, the School will reply in 20 School days stating that an exemption applies but include an estimate of the date by which a decision on the public interest test will be made. This should be within a 'reasonable' time.

Where the School has notified the enquirer that a charge is to be made, the time period stops until payment is received.

THIRD PARTY DATA

Consultation of third parties may be required if their interests could be affected by release of the information requested, and any such consultation may influence the decision.

Consultation will be necessary where:

- Disclosure of information may affect the legal rights of a third party, such as the right to have certain information treated in confidence or rights under Article 8 of the European Convention on Human Rights
- The views of the third party may assist the School to determine if information is exempt from disclosure; or
- The views of the third party may assist the School to determine the public interest test.

Personal information requested by third parties is also exempt under this policy where release of that information would breach the Data Protection Act. If a request is made for a document [e.g. Governing Body minutes] which contains personal information whose release to a third party would breach the Data Protection Act, the document may be issued by blanking out the relevant personal information as set out in the redaction procedure.

EXEMPTIONS

The presumption of the Freedom of Information Act is that the School will disclose information unless the Act provides a specific reason to withhold it. The Act recognises the need to preserve confidentiality and protect sensitive material in certain circumstances.

The School may refuse all/part of a request, if one of the following applies:

1) There is an exemption to disclosure within the act
2) The information sought is not held
3) The request is considered vexatious or repeated
4) The cost of compliance exceeds the threshold.

A series of exemptions are set out in the Act which allow the withholding of information in relation to an enquiry. Some are specialised in their application [such as national security] and would not usually be relevant to Schools.

There are two general categories of exemptions:

1) **Absolute**: Where there is no requirement to confirm or deny that the information is held, disclose the information or consider the public interest
2) **Qualified**: Where, even if an exemption applies, there is a duty to consider the public interest in disclosing information.

ABSOLUTE EXEMPTIONS

There are eight absolute exemptions set out in the Act. However the following are the only absolute exemptions which will apply to the School:

- Information accessible to the enquirer by other means [for example by way of the School's Publication Scheme]
- National Security/Court Records
- Personal information [i.e. information which would be covered by the Data Protection Act]
- Information provided in confidence. If an absolute exemption exists, it means that disclosure is not required by the Act. However, a decision could be taken to ignore the exemption and release the information taking into account all the facts of the case if it is felt necessary to do so.

QUALIFIED EXEMPTIONS

If one of the below exemptions apply [i.e. a qualified disclosure], there is also a duty to consider the public interest in confirming or denying that the information exists and in disclosing information.

The qualified exemptions under the Act which would be applicable to the School are:

- Information requested is intended for future publication [and it is reasonable in all the circumstances for the requester to wait until such time that the information is actually published]
- Reasons of National Security
- Government/International Relations
- Release of the information is likely to prejudice any actual or potential legal action or formal investigation involving the School
- Law enforcement [i.e. if disclosure would prejudice the prevention or detection of crime, the prosecution of offenders or the administration of justice]
- Release of the information would prejudice the ability of the School to carry out an effective audit of its accounts, resources and functions
- For Health and Safety purposes
- Information requested is Environmental information
- Information requested is subject to Legal professional privilege
- For Commercial Interest reasons.

Where the potential exemption is a qualified exemption, the School will consider the public interest test to identify if the public interest in applying the exemption outweighs the public interest in disclosing it.

In all cases, before writing to the enquirer, the person given responsibility by the School for dealing with the request will need to ensure that the case has been properly considered, and that the reasons for refusal, or public interest test refusal, are sound.

REFUSAL

If it is decided to refuse a request, the School will send a refusals notice, which must contain:

- The fact that the responsible person cannot provide the information asked for
- Which exemption[s] apply
- Why the exemption[s] apply to this enquiry [if it is not self-evident]
- Reasons for refusal
- The School's Complaints Procedure.

For monitoring purposes and in case of an appeal against a decision not to release the information or an investigation by the Information Commissioner, the responsible person must keep a record of all enquiries where all or part of the requested information is withheld and exemptions are claimed. The record must include the reasons for the decision to withhold the information.

FREEDOM OF INFORMATION COMPLIANCE REPORTING

In line with best practice guidance from the ICO, the School will publish statistics on its compliance with the FOI Act 2000, provide regular summaries of:

- The number of FOI requests received
- The percentage of responses issued within the statutory 20 school days deadline
- The number of requests where exemptions were applied
- The number of internal reviews and ICO complaints [if applicable].

These compliance statistics are published annually on the School's website and are reviewed by the Board of Trustee to ensure continued compliance and transparency.

The School is committed to maintaining high standards of accountability and responding to FOI requests within the legal timeframe. In addition, a summary of FOI requests and its responses will be published through our FOI Disclosure Log [Appendix 1] available on the school website, where appropriate and subject to data protection considerations.

SECTION 2 – FREEDOM OF INFORMATION PUBLICATION SCHEME INTRODUCTION

This publication scheme follows a model approved by the Information Commissioners Office.

This scheme is not a list of individual publications but rather a description of the classes of types of information that the School is committed to publishing. This list is not an exhaustive list of all of the types of information that the School publish. The School tries publish proactively as much information as the School can where the information would have a wider public interest.

This scheme does not include information that the School considers being sensitive, such as personal information, information prevented from disclosure by law or information about security matters.

CLASSES OF INFORMATION

There are six classes of information that the School holds:

- Who the School is and what the School does
- What the School spends and how the School spends it
- What our priorities are and how the School is doing
- How the School makes decisions
- Our policies and procedures
- The services the School offers.

MAKING INFORMATION AVAILABLE

Information will generally be made available on the School's website. Where it is not possible to include this information on the School website, or when an individual does not wish to access the information by the website the School will indicate how information can be obtained by other means and provide it by those means. This may be detailed in response to a request or within the scheme itself. This will usually be by way of a paper copy.

In some exceptional circumstances, some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

Information will be provided in the language in which it is held or in such other language that is legally required. Where the School is legally required to translate any information, the School will do so.

CHARGES FOR INFORMATION PUBLISHED UNDER THIS SCHEME

The School may charge individuals for information published under this scheme. The purpose of this scheme is to make the maximum amount of information readily available at the minimum inconvenience and cost to the public. Charges made by the School for routinely published material will be justified and transparent and kept to a minimum.

Material which is published and accessed on the website will be provided free of charge.

Charges may be made for information subject to a charging regime specified by law.

Charges will be made to cover:

- Photocopying
- Postage and Packaging
- The costs directly incurred as a result of viewing information.

Single copies of information requested which are covered by the publication scheme will be provided free unless otherwise stated within the scheme. If the request involved a large amount of photocopying, printing or postage, then this may be at a cost. If this is the case, The School will let you know as well as let you know the cost before fulfilling your request.

HOW TO REQUEST INFORMATION

If you require a paper version of any of the documents within the scheme please contact the School using the contact details below.

Telephone: 020 8572 1931

Email: info@hestoncs.org
Address: Heston Community School, Heston Road, Hounslow, Middlesex, TW5 0QR

Please mark all correspondence Publication Scheme Request in order to help us process your request quickly. If the information you are looking for isn't available via the scheme, you can still contact the School to ask if the School has this information.

THE PUBLICATION SCHEDULE

WHO WE ARE AND WHAT WE DO	DESCRIPTION
Information relating to the Governing Body	Information contained in official Governing Body documents including the Governor's annual report: • Who is who • Basis of Governors appointment • The manner in which the Governing Body is constituted • Category of the School • A statement on progress in implementing the action plan drawn up following an inspection • Agreed minutes from Governors Board and Committee Meetings • A financial statement – including gifts made to the School and amounts paid to the Governors for expenses • Information about the implementation of the Governing body's policy on students with special educational needs and any changes to the policy during the last year • A description of arrangements for the admission of students with disabilities, including details of the steps to prevent disabled students being treated less favourably than other students, details of existing facilities to assist access to the School by students with disabilities, the accessibility plan covering future policies for increasing access by those with disabilities to the School • A statement of policy on whole staff development identifying how teacher's professional development impacts on teaching and learning. • Number of students on roll and rates of students authorised and unauthorised absence • National curriculum assessment results for appropriate key stages with national summary figures • Instruments of Government, including the date it takes effect • The term of office of each category of Governor if it lasts less than 4 years and the name of anybody entitled to appoint any category of Governor.
School prospectus	• The name, address, website and telephone number of the school and the type of school • The name of the school Headteacher • The School's staffing structure • Information about the School's policy on providing for students with Special Educational Needs • Statement on the School's aims and values • Information on the School's policy on admissions • School term dates, times and attendance • Uniform • Number of Students on roll and rates of student absence • Details of any affiliations with a particular religion or religious denomination, the religious education and collective worship and the alternative provision for these students.

WHAT WE SPEND AND HOW WE SPEND IT	DESCRIPTION
Financial statement for the current and previous financial year	Relating to projected and actual income and expenditure, procurement, contracts and financial audit. Includes budget plans, financial statements and financial audit reports
Details of expenditure	Sets out details of items of expenditure over £5,000 including the cost, name of supplier and information about the transaction
Procurement and contracts	Details of the procurement and contracts the School has entered into or details relating to the organisation who has carried out this process on the School's behalf [for example the Local Authority].
Pay policy	A copy of the pay policy that the School uses to govern staff pay.
Allowances	Details of allowances and expenses that can be incurred by staff and Governors.
Student Premium	How the School uses student premium.
Utilities and School running expenditure	Details of the School's overheads and running costs.

WHAT OUR PRIORITIES ARE AND HOW WE ARE DOING	DESCRIPTION
Ofsted report	A published report of the outcome of our latest Ofsted inspection.
Performance management policy	Statement of procedures adopted by the Governing Body relating to the performance management of staff and the annual report of the Headteacher on the effectiveness of appraisal procedures.
Charging and remissions policies	A statement of the School's policy with respect to charges and remissions for any optional extra or board and lodging for which charges are permitted, for example School publication, music tuition, and trips.
Health and Safety Policy and Risk Assessment	Statement of general policy with respect to health and safety at work of employees [and others] and the organisation and arrangements for carrying out the policy.
Staff Conduct, Discipline and Grievance	Statement of procedure for regulating conduct and discipline of School staff and procedures by which staff may seek redress for grievance.
Curriculum circulars and Statutory Instruments	Any statutory instruments, departmental circulars and administrative memoranda sent by the Department of Education to the Headteacher or Governing Body relating to the curriculum.

HOW WE MAKE DECISIONS	DESCRIPTION
Admissions Policy/ Decisions [not individual]	This does not include individual decisions. This is a statement of our policy with regards to admissions and how the School make decisions regarding admissions.

OUR POLICIES AND PROCEDURES	DESCRIPTION
Home-School Agreement	Written statements of the School's aims and values, the School's responsibilities, the parental responsibilities the School's expectations of its students for example homework arrangements.
Curriculum Policy	Statement on following the national curriculum subjects, including any syllabus used by the School.
Complaints Policy	Statement of procedures for dealing with complaints
Equality and Diversity Policy	Statement on ensuring that the School follows and promotes equality and diversity.
Child protection and safeguarding policy	Statement of policy for safeguarding and promoting welfare of students at the School.
Relationships and Sex Education Policy	Statement of policy with regard to sex and relationship education
SEND and Inclusion Policy	Information about the School's policy on providing for students with special educational needs.
Behaviour for Learning Policy	Statement of general principles on behaviour and discipline and of measures taken by the Headteacher to prevent bullying.
Collective Worship	Statement of arrangements for the required daily act of collective worship

THE SERVICES WE OFFER	DESCRIPTION
Extra-curricular Activities and out of School clubs	Details of these are contained on the School's website

Lists and Registers	Description
Disclosure Log [FOI Requests] [Appendix 1]	A summary of FOI requests received and how the school responded. Includes date, topic of request and summary of response.

INTERNAL REVIEW

The requester has the right to ask for an internal review if they are dissatisfied with the handling of a request.

Internal review requests should be made within 40 working days of the initial response. This deadline should be communicated to the requester in that response. We are not obliged to provide a review if it is requested after more than 40 working days.

Requests for internal review must make clear why they are dissatisfied with the original decision, detailing why they feel that the School has not complied with Freedom of Information Law.

COMPLAINTS AND/OR APPEALS

Any written [including email] expression of dissatisfaction should be handled through the School's existing Complaints Procedure. Wherever practicable the review should be handled by someone not involved in the original decision.

The Governing Body should set and publish a target time for determining complaints and information on the success rate in meeting the target. The School should maintain records of all complaints and their outcome.

If the outcome is that the School's original decision or action is upheld, then the applicant can appeal to the Information Commissioner. The appeal can be made via their website or in writing to:

Customer Contact
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

INFORMATION SECURITY POLICY

The UK General Data Protection Regulation [UK GDPR] aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School is dedicated to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This documents sets out the measures taken by the School to achieve this, including to:

- protect against potential breaches of confidentiality
- ensure that all information assets and IT facilities are protected against damage, loss or misuse
- support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data
- increase awareness and understanding at the School of the requirements of information security and the responsibility to staff to protect the confidentiality and integrity of the information that they themselves handle.

INTRODUCTION

Information Security can be defined as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

Staff are referred to the School's Data Protection Policy, Data Breach Policy and Electronic Information and Communication Systems Policy for further information. These policies are also designed to protect personal data and can be found at on the School's website at www.hestoncommunitySchool.co.uk

For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to, laptops, tablets, digital cameras, memory sticks and smartphones.

SCOPE

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the School, in whatever media. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

This policy applies to all members of staff, including temporary workers, other contractors, volunteers, interns, Governors and any and all third parties authorised to use the IT systems.

All members of staff undergo GDPR training annually and sign a pledge to adhere to its' principles. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

GENERAL PRINCIPLES

All data stored on our IT systems are to be classified appropriately [including, but not limited to, personal data, sensitive personal data and confidential information. Further details on the categories of data can be found in the School's Data Protection Policy and Record of Processing Activities. All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss with their Line Manager the appropriate security arrangements for the type of information they access in the course of their work.

All data stored on our IT Systems and our paper records will be available only to members of staff with legitimate need for access and will be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by the IT Team or by such third party/parties as the Facilities, Premises and Compliance Manager may authorise.

The responsibility for the security and integrity of all IT Systems and the data stored thereon [including, but not limited to, the security, integrity, and confidentiality of that data] lies with Facilities, Premises and Compliance Manager unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to the SIMS and Data Manager who will investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data will be reported to the Data Protection Officer [full details of the officer can be found in our Data Protection Policy.

PHYSICAL SECURITY AND PROCEDURES

Paper records and documents containing personal information, sensitive personal information, and confidential information will be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows. At the end of the working day, or when you leave your desk unoccupied, all paper documents will be securely locked away to avoid unauthorised access.

Available [storage rooms, locked cabinets, and other storage systems with locks] will be used to store paper records when not in use.

Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of School.

The physical security of buildings and storage systems will be reviewed on a regular basis. If you find the security to be insufficient, you must inform the Facilities, Premises and Compliance Manager as soon as possible. Increased risks of vandalism and or burglary will be taken into account when assessing the level of security required.

The School carries out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.

The School has the InVentry sign-in system to minimise the risk of unauthorised people from entering the School premises.

The School closes the School gates during certain hours to prevent unauthorised access to the building. An alarm system is set nightly.

CCTV Cameras are in use across the School site and monitored by the IT Team.

Visitors should be required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

COMPUTERS AND IT

RESPONSIBILITIES OF THE FACILITIES, PREMISES AND COMPLIANCE MANAGER

The Facilities, Premises and Compliance Manager, will be responsible for the following:

a) Ensuring that all IT Systems are assessed and deemed suitable for compliance with the School's security requirements
b) Ensuring that IT Security standards within the School are effectively implemented and regularly reviewed, working in consultation with the School's management, and reporting the outcome of such reviews to the School's management
c) Ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the UK GDPR and the Computer Misuse Act 1990
d) Assisting all members of staff in understanding and complying with this policy
e) Providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems
f) Ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements
g) Receiving and handling all reports relating to IT Security matters and taking appropriate action in response [including, in the event that any reports relate to personal data, informing the SIMS and Data Manager
h) Taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff
i) Monitoring all IT security within the School and taking all necessary action to implement this policy and any changes made to this policy in the future
j) Ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

RESPONSIBILITIES – MEMBERS OF STAFF

All members of staff must comply with all relevant parts of this policy at all times when using the IT Systems.

Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

You must immediately inform **both** the Facilities, Premises and Compliance Manager and SIMS and Data Manager of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Data Breach Policy.

Any other technical problems [including, but not limited to, hardware failures and software errors] which may occur on the IT Systems will be reported to the IT Team immediately.

You are not entitled to install any software of your own without the approval of the Facilities, Premises and Compliance Manager. Any software belonging to you must be approved by the Facilities, Premises and Compliance Manager and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

Prior to installation of any software onto the IT Systems, you must obtain written permission by the Facilities, Premises and Compliance Manager. This permission must clearly state which software you may install, and onto which computer[s] or device[s] it may be installed.

Prior to any usage of physical media [e.g. USB memory sticks or disks of any kind] for transferring files, you must make sure to have the physical media is virus-scanned. The Facilities, Premises and Compliance Manager approval must be obtained prior to transferring of files using cloud storage systems.

If you detect any virus this must be reported immediately to the Facilities, Premises and Compliance Manager [this rule will apply even where the anti-virus software automatically fixes the problem].

ACCESS SECURITY

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

The School has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the School's network. The School also teaches individuals about e-safety to ensure everyone is aware of how to protect the School's network and themselves.

All IT Systems [in particular mobile devices] will be protected with a secure password or passcode, or such other form of secure log-in system as approved by the IT Department. Biometric log-in methods can only be used if approved by the IT Department.

All passwords must, where the software, computer, or device allows:

- Be at least 8 characters long including both numbers, letters and symbols
- Be changed on a regular basis [forced after 48 days]
- Not be obvious or easily guessed [e.g. birthdays or other memorable dates, memorable names, events, or places etc.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of SLT who will liaise with the Facilities, Premises and Compliance Manager as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If you forget your password, you should notify the IT Team to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

You should not write down passwords if it is possible to remember them. If necessary you may write down passwords provided that you store them securely [e.g. in a locked drawer or in a secure password database]. Passwords should never be left on display for others to see.

Computers and other electronic devices with displays and user input devices [e.g. mouse, keyboard, touchscreen etc.] will be protected with a screen lock that will activate after a period of inactivity. You may not change this this time period or disable the lock.

All mobile devices provided by the School, will be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not alter this time period.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

DATA SECURITY

Personal data sent over the School network will be encrypted or otherwise secured.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from Facilities, Premises and Compliance Manager who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given all files and data should always be virus checked before they are downloaded onto the School's systems.

You may connect your own devices [including, but not limited to, laptops, tablets, and smartphones] to the School's Wi-Fi provided that you follow the Facilities, Premises and Compliance Manager's requirements and instructions governing this use. All usage of your own device[s] whilst connected to the School's network or any other part of the IT Systems is subject to all relevant School Policies [including, but not limited to, this policy]. The Facilities, Premises and Compliance Manager may at any time request the immediate disconnection of any such devices without notice.

ELECTRONIC STORAGE OF DATA

All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by Facilities, Premises and Compliance Manager.

All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

You should not store any personal data on any mobile device, whether such device belongs to the School or otherwise without prior written approval of the Facilities, Premises and Compliance Manager. You should delete data copied onto any of these devices as soon as possible and make sure it is stored on the School's computer network in order for it to be backed up.

All electronic data must be securely backed up by the end of the each working day and is done by Facilities, Premises and Compliance Manager.

HOME WORKING

You should not take confidential or other information home without prior permission of your Line Manager, and only do so where satisfied appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information.

When you have been given permission to take confidential or other information home, you must ensure that:

a) The information is kept in a secure and locked environment where it cannot be accessed by family members or visitors
b) All confidential material that requires disposal is shredded or, in the case of electronic material, securely destroyed, as soon as any need for its retention has passed.

COMMUNICATIONS, TRANSFER, INTERNET AND EMAIL USE

When using the School's IT Systems you are subject to and must comply with the School's Electronic Information and Communication Systems Policy.

The School works to ensure the systems do protect students and staff and are reviewed and improved regularly.

If staff or students discover unsuitable sites or any material which would be unsuitable, this should be reported to Facilities, Premises and Compliance Manager

Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the School cannot accept liability for the material accessed or its consequence.

All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email, or sent by tracked DX [document exchange] or recorded delivery. You may not send such information by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

Postal, DX, fax and email addresses and numbers should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

You should be careful about maintaining confidentiality when speaking in public places.

You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the School.

Personal or confidential information should not be removed from the School without prior permission of your Line Manager except where the removal is temporary and necessary. When such permission is given you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. You must ensure that the information is:

a) Not transported in see-through or other un-secured bags or cases
b) Not read in public places [e.g. waiting rooms, cafes, trains, etc]
c) Not left unattended or in any place where it is at risk [e.g. in car boots, cafes, etc].

REPORTING SECURITY BREACHES

All concerns, questions, suspected breaches, or known breaches will be referred immediately to the SIMS and Data Manager. All members of staff have an obligation to report actual or potential data protection compliance failures.

When receiving a question or notification of a breach, the SIMS and Data Manager will immediately assess the issue, including but not limited to, the level of risk associated with the issue, and will take all steps necessary to respond to the issue.

Members of staff should under no circumstances attempt to resolve an IT security breach on their own without first consulting the Facilities, Premises and Compliance Manager. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of, the Facilities, Premises and Compliance Manager.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to SIMS and Data Manager.

All IT security breaches will be fully documented.

Full details on how to notify of data breaches are set out in the Breach Notification Policy.

Related Policies

Staff should refer to the following policies that are related to this Information Security Policy:

- Data Breach Policy
- Data Protection Policy .

CYBER SECURITY POLICY

INTRODUCTION

Cyber security has been identified as a risk for the School and every employee needs to contribute to ensure data security.

The School has invested in technical cyber security measures but we also need our employees to be vigilant and to act to protect the School IT systems.

The Facilities, Premises and Compliance Manager is responsible for cyber security within the School.

If you are an employee, you may be liable to disciplinary action if you breach this policy.

This policy supplements other data management and security policies, namely our [Data Protection Policy, Data Breach Policy, Information Security Policy, Acceptable Use Policy, Home Working Policy, Electronic Information and Communications Policy and Clear Desk Policy.]

PURPOSE AND SCOPE

The purpose of this document is to establish systems and controls to protect the School from cyber criminals and associated cyber security risks, as well as to set out an action plan should the School fall victim to cyber-crime.

This policy is relevant to all staff.

WHAT IS CYBER-CRIME?

Cyber-crime is simply a criminal activity carried out using computers or the internet including hacking, phishing, malware, viruses or ransom attacks.
The following are all potential consequences of cyber-crime which could affect an individual and/or individuals:

- Cost
- Confidentiality and data protection
- Potential for regulatory breach
- Reputational damage
- Business interruption; and
- Structural and financial instability.

CYBER-CRIME PREVENTION

Given the seriousness of the consequences noted above, it is important for the School to take preventative measures and for staff to follow the guidance within this policy.

This cyber-crime policy sets out the systems we have in place to mitigate the risk of cyber-crime. The Facilities, Premises and Compliance Manager can provide further details of other aspects of the School/Trust risk assessment process upon request.

The School have put in place a number of systems and controls to mitigate the risk of falling victim to cyber-crime. These include technology solutions as well as controls and guidance for staff.

TECHNOLOGY SOLUTIONS

The School have implemented the following technical measures to protect against cyber-crime:

i) Firewalls
ii) Anti-virus software
iii) Anti-spam software
iv) Auto or real-time updates on our systems and applications
v) URL filtering
vi) Secure data backup
vii) Encryption
viii) Deleting or disabling unused/unnecessary user accounts
ix) Deleting or disabling unused/unnecessary software
x) Using strong passwords; and
xi) Disabling auto-run features.

CONTROLS AND GUIDANCE FOR STAFF

- All staff must follow the policies related to cyber-crime and cyber security as listed in this policy
- All staff will be provided with training at induction and refresher training as appropriate; when there is a change to the law, regulation or policy; where significant new threats are identified and in the event of an incident affecting the School or any third parties with whom we share data.

All staff must:

- Choose strong passwords [the School's IT team advises that a strong password contains [list of types of characters, password length etc. as permitted by your IT systems]]
- Keep passwords secret
- Never reuse a password
- Never allow any other person to access the school's systems using your login details;
- Not turn off or attempt to circumvent any security measures [antivirus software, firewalls, web filtering, encryption, automatic updates etc.] that the IT team have installed on their computer, phone or network or the School IT systems
- Report any security breach, suspicious activity or mistake made that may cause a cyber-security breach, to Facilities, Premises and Compliance Manager as soon as practicable from the time of the discovery or occurrence. If your concern relates to a data protection breach you must follow our Data Breach Policy
- Only access work systems using computers or phones that the School owns. Staff may only connect personal devices to the Wi-Fi provided
- Not install software onto your School computer or phone. All software requests should be made to Facilities, Premises and Compliance Manager; and
- Avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using School equipment and/or networks.

The School considers the following actions to be a misuse of its IT systems or resources:

- Any malicious or illegal action carried out against the School or using the School's systems
- Accessing inappropriate, adult or illegal content within School premises or using School equipment

- Excessive personal use of School's IT systems during working hours
- Removing data or equipment from School premises or systems without permission, or in circumstances prohibited by this policy
- Using School equipment in a way prohibited by this policy
- Circumventing technical cyber security measures implemented by the School's IT team; and
- Failing to report a mistake or cyber security breach.

CYBER-CRIME INCIDENT MANAGEMENT PLAN

The incident management plan consists of four main stages:

i) Containment and recovery: To include investigating the breach, utilising appropriate staff to mitigate damage and where possible, to recover any data lost
ii) Assessment of the ongoing risk: To include confirming what happened, what data has been affected and whether the relevant data was protected. The nature and sensitivity of the data should also be confirmed and any consequences of the breach/attack identified
iii) Notification: To consider whether the cyber-attack needs to be reported to regulators [for example, the ICO and National Crime Agency] and/or colleagues/parents as appropriate
iv) Evaluation and response: To evaluate future threats to data security and to consider any improvements that can be made
v) Where it is apparent that a cyber-security incident involves a personal data breach, the School will invoke their Data Breach Policy rather than follow out the process above.

SOCIAL MEDIA POLICY

INTRODUCTION

This policy applies to all School staff regardless of their employment status. It is to be read in conjunction with the School's Electronic Communications Policy. This policy does not form part of the terms and conditions of employee's employment with the School and is not intended to have contractual effect. It does however set out the School's current practices and required standards of conduct and all staff are required to comply with its contents. Breach of the provisions of this policy will be treated as a disciplinary offence which may result in disciplinary action up to and including summary dismissal in accordance with the School's Disciplinary Policy and Procedure.

This Policy may be amended from time to time and staff will be notified of any changes no later than one month from the date those changes are intended to take effect.

PURPOSE OF THIS POLICY

The School recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Twitter, LinkedIn, blogs and Wikipedia. However, staff use of social media can pose risks to the School's confidential and proprietary information, its reputation and it can jeopardise our compliance with our legal obligations.

To minimise these risks, avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate work related purposes, all School staff are required to comply with the provisions in this policy.

WHO IS COVERED BY THIS POLICY?

This policy covers all individuals working at all levels and grades within the School, including senior managers, officers, Governors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers [collectively referred to as **Staff** in this policy].

Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

SCOPE AND PURPOSE OF THIS POLICY

This policy deals with the use of all forms of social media including Facebook, LinkedIn, Twitter, Wikipedia, Instagram, TikTok, WhatsApp all other social networking sites, and all other internet postings, including blogs.

It applies to the use of social media for both work and personal purposes, whether during work hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff.

Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours and regardless of whether the School's equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

PERSONNEL RESPONSIBLE FOR IMPLEMENTING THE POLICY

The Board of Governors have overall responsibility for the effective operation of this policy, but have delegated day-to-day responsibility for its operation to the Headteacher.

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the Headteacher in liaison with the IT Manager.

All senior School Staff have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

All School Staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the Headteacher in the first instance. Questions regarding the content or application of this policy should be directed by email to School Office at info@hestoncs.org

COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS

Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

a) Breach our Electronic Information and Communications Systems Policy
b) Breach our obligations with respect to the rules of relevant regulatory bodies
c) Breach any obligations they may have relating to confidentiality
d) Breach our Disciplinary Rules
e) Defame or disparage the School, its Staff, its students or parents, its affiliates, partners, suppliers, vendors or other stakeholders
f) Harass or bully other Staff in any way or breach our Anti-harassment and bullying policy
g) Unlawfully discriminate against other Staff or third parties or breach our Equal opportunities policy
h) Breach our Data Protection Policy [for example, never disclose personal information about a colleague online]
i) Breach any other laws or ethical standards [for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements].

Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the School and create legal liability for both the author of the reference and the organisation.

Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

PERSONAL USE OF SOCIAL MEDIA

Personal use of social media is never permitted during working time or by means of our computers, networks and other IT resources and communications systems.

Staff should not use a work email address to sign up to any social media and any personal social media page should not make reference to their employment with the School [excluding LinkedIn, where prior permission is sought from the Headteacher.

Staff must not take photos or posts from social media that belongs to the School for their own personal use.

MONITORING

The contents of our IT resources and communications systems are the School's property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

The School reserves the right to monitor, intercept and review, without further notice, Staff members activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your acknowledgement of this policy and your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

The School may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

All Staff are advised not to use our IT resources and communications systems for any matter that he or she wishes to be kept private or confidential from the School.

EDUCATIONAL OR EXTRA CURRICULAR USE OF SOCIAL MEDIA

If your duties require you to speak on behalf of the School in a social media environment, you must follow the protocol outlined below.

The Headteacher may require you to undergo training before you use social media on behalf of the School and impose certain requirements and restrictions with regard to your activities.

Likewise, if you are contacted for comments about the School for publication anywhere, including in any social media outlet, you must direct the inquiry to the Headteacher and must not respond without advanced written approval.

RECRUITMENT

The School may use internet searches to perform pre-employment checks on candidates in the course of recruitment. Where the School does this, it will act in accordance with its data protection and equal opportunities obligations.

RESPONSIBLE USE OF SOCIAL MEDIA

The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely.

PHOTOGRAPHS FOR USE OF SOCIAL MEDIA

Any photos for social media posts may only be taken using School cameras/devices or devices that have been approved in advance by the Headteacher. Where any device is used that does not belong to the School all photos must be deleted immediately from the device, once the photos have been uploaded to a device belonging to the School.

STAFF PROTOCOL FOR USE OF SOCIAL MEDIA

Where any post is going to be made on the School's own social media the following steps must be taken:

1) Ensure that permission from the child's parent has been sought before information is used on social media via Consent Agreement
2) Ensure that there is no identifying information relating to a child/children in the post for example any certificates in photos are blank/without names or the child's name cannot be seen on the piece of work
3) The post must be a positive and relevant post relating to the children, the good work of staff, the School or any achievements
4) Social Media can also be used to issue updates or reminders to parents/guardians and the Headteacher will have overall responsibility for this. Should you wish for any reminders to be issued you should contact the Headteacher by email to ensure that any post can be issued
5) The proposed post must be presented to the Headteacher for confirmation that the post can 'go live' before it is posted on any social media site
6) The Facilities, Premises and Compliance Manager will post the information, but all staff have responsibility to ensure that the Social Media Policy has been adhered to.

PROTECTING OUR BUSINESS REPUTATION

Staff must not post disparaging or defamatory statements about:

i) The School
ii) Current, past or prospective Staff as defined in this policy
iii) Current, past or prospective students
iv) Parents, carers or families
v) The School's suppliers and services providers
vi) Other affiliates and stakeholders.

Staff should also avoid social media communications that might be misconstrued in a way that could damage the School's reputation, even indirectly.

If Staff are using social media they should make it clear in any social media postings that they are speaking on their own behalf. Staff should write in the first person and use a personal rather than School e-mail address when communicating via social media.

Staff are personally responsible for what they communicate in social media. Staff should remember that what they publish might be available to be read by the masses [including the School itself, future employers and social acquaintances] for a long time. Staff should keep this in mind before they post content.

If Staff disclose whether directly or indirectly their affiliation to the School as a member of Staff whether past, current or prospective, they must also state that their views do not represent those of the School.

Staff must ensure that their profile and any content posted are consistent with the professional image they are required to present to colleagues, students and parents.

Staff must avoid posting comments about confidential or sensitive School related topics. Even if Staff make it clear that their views on such topics do not represent those of the School, such comments could still damage the School's reputation and incur potential liability.

If a member of Staff is uncertain or concerned about the appropriateness of any statement or posting, he or she should refrain from making the communication until he or she has discussed it with his or her Line Manager or Head of Department.

If a member of Staff sees content in social media that disparages or reflects poorly on the School, it's Staff, students, parents, service providers or stakeholders, he or she is required to report this in the first instance to the Headteacher without unreasonable delay. All staff are responsible for protecting the School's reputation.

RESPECTING INTELLECTUAL PROPERTY AND CONFIDENTIAL INFORMATION

Staff should not do anything to jeopardise School confidential information and intellectual property through the use of social media.

In addition, Staff should avoid misappropriating or infringing the intellectual property of other schools, organisations, companies and individuals, which can create liability for the School, as well as the individual author.

Staff must not use the School's logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without express prior written permission from the Headteacher.

To protect yourself and the School against liability for copyright infringement, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask the Headteacher in the first instance before making the communication.

RESPECTING COLLEAGUES, STUDENTS, PARENTS, CLIENTS, SERVICE PROVIDERS AND STAKEHOLDERS

Staff must not post anything that their colleagues, the School's past, current or prospective students, parents, service providers or stakeholders may find offensive, including discriminatory comments, insults or obscenity.

Staff must not post anything related to colleagues, the School's past, current or prospective students, parents, service providers or stakeholders without their advanced written permission.

MONITORING AND REVIEW OF THIS POLICY

The Facilities, Premises and Compliance Manager together with the Headteacher, will be responsible for reviewing this policy annually to ensure that it meets legal requirements and reflects best practice. The Board of Governors has responsibility for approving any amendments prior to implementation.

The Headteacher has responsibility for ensuring that any person who may be involved with administration or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.

If Staff have any questions about this policy or suggestions for additions that they would like to be considered on review, they may do so by emailing the Facilities, Premises and Compliance Manager in the first instance.

RECORD OF PROCESSING ACTIVITIES

Created: March 2020
Last Reviewed: Dec 2024

This Record of Processing Activities describes how Heston Community School, the Data Controller, processes personal data.

The School recognises that Article 30 of the General Data Protection Regulation [GDPR] imposes documentation requirements on controllers and processors of data. This record is information that is confidential to the School but will be provided to supervisory authorities [such as the Information Commissioner's Office] on request and as required by the GDPR.

SCHOOL DETAILS

Name:	Heston Community School
Address:	Heston Road Heston Hounslow TW5 0QR
Telephone:	020 8572 1931
Website:	www.hestoncommunitySchool.co.uk
Data Protection Officer's name:	Judicium Consulting Limited
Lead Contact:	Craig Stilwell
Data Protection Officer's details:	72 Cannon Street London EC4N 6AE
Data Protection Officer's email:	dataservices@judicium.com

CATEGORIES OF DATA SUBJECTS

The School collects personal data from the following categories of Data Subjects:

- Heston Community School employees and job applicants
- Heston Community School students and parents
- Heston Community School vendors or suppliers.

CATEGORIES OF PERSONAL DATA

The School collects the following categories of personal data about employees and job applicants

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses
- Emergency contact information such as names, relationship, phone numbers and email addresses
- Information collected during the recruitment process that the School retains during your employment including references, proof of right to work in the UK, application form, CV, qualifications
- Employment contract information such as start dates, hours worked, post, roles
- Education and training details

- Details of salary and benefits including payment details, payroll records, tax status information, national insurance number, pension and benefits information
- Details of any dependants
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information
- Information in your sickness and absence records such as number of absences and reasons[including sensitive personal information regarding your physical and/or mental health]
- Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs
- Criminal records information as required by law to enable you to work with children
- Your trade union membership
- Information on grievances raised by or involving you
- Information on conduct and/or other disciplinary issues involving you
- Details of your appraisals, performance reviews and capability issues
- Details of your time and attendance records
- Information about the use of our IT, communications and other systems, and other monitoring information
- Details of your use of business-related social media
- Images of staff captured by the School's CCTV system
- Your use of public social media [only in very limited circumstances, to check specific risks for specific functions within the School, you will be notified separately if this is to occur]
- Details in references about you that the School gives to others.

The School collects the following categories of personal data about students and parents:

- Personal information such as name, student number, date of birth, gender and contact information
- Emergency contact and family lifestyle information such as names, relationship, phone numbers and email addresses
- Characteristics [such as ethnicity, first language, country of birth and Free School Meal eligibility]
- Attendance details [such as sessions attended, number of absences and reasons for absence]
- Financial details
- Performance and assessment information
- Behavioural information [including exclusions]
- Special educational needs information
- Relevant medical information
- Special categories of personal data [including [biometric data, ethnicity, relevant medical information, special educational needs information]]
- Images of students engaging in School activities, and images captured by the School's CCTV system.

The School collects the following categories of personal data about Governors:

- Personal information such as name, date of birth, gender and contact information
- Nationality and immigration status and information from related documents, such as passport or other identification and immigration information.

The School collects the following categories of personal data about vendors and suppliers:

- Name and contact information
- Financial and payment details.

PURPOSES OF DATA PROCESSING

The School collects and processes personal data about employees and job applicants for the following purposes:

- To determine recruitment and selection decisions on prospective employees
- In order to carry out effective performance of the employees contract of employment and to maintain employment records
- To comply with regulatory requirements and good employment practice
- To carry out vetting and screening of applicants and current staff in accordance with regulatory and legislative requirements
- Enable the development of a comprehensive picture of the workforce and how it is deployed and managed
- To enable management and planning of the workforce, including accounting and auditing
- Personnel management including retention, sickness and attendance
- Performance reviews, managing, performance and determining performance requirements
- In order to manage internal policy and procedure
- Human resources administration including pensions, payroll and benefits
- To determine qualifications for a particular job or task, including decisions about promotions
- Evidence for possible disciplinary or grievance processes
- Complying with legal obligations
- To monitor and manage staff access to our systems and facilities in order to protect our networks, the personal data of our employees and for the purposes of safeguarding
- Network and information security, including preventing unauthorised access to our computer network and communications systems and preventing malicious software distribution
- Education, training and development activities
- To monitor compliance with equal opportunities legislation
- Determinations about continued employment or engagement
- Arrangements for the termination of the working relationship
- Dealing with post-termination arrangements
- Health and safety obligations
- Fraud.

The School collects and processes personal data [including Special Category Data] about students and parents for the following purposes:

- For the purposes of student selection [and to confirm the identity of prospective students and their parents]
- To provide education services and extra-curricular activities to students, and monitoring students' progress and educational needs
- To derive statistics which inform decisions such as the funding of Schools
- To assess performance and to set targets for Schools
- To safeguard students' welfare and provide appropriate pastoral [and where necessary medical] care
- To give and receive information and references about past, current and prospective students, and to provide references to potential employers of past students
- In order to manage internal policy and procedure
- To enable students to take part in national or other assessments, and to publish the results of public examinations or other achievements of students of the School

- For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law [such as diversity or gender pay gap analysis]
- For legal and regulatory purposes [for example child protection, diversity monitoring and health and safety] and to comply with its legal obligations and duties of care
- To enable relevant authorities to monitor the School's performance and to intervene or assist with incidents as appropriate
- To monitor [as appropriate] use of the School's IT and communications systems in accordance with the School's Information Security Policy
- To make use of photographic images of students in School publications, on the School's website and [where appropriate] on the School's social media channels
- For security purposes, including CCTV in accordance with the School's CCTV Policy
- Where otherwise reasonably necessary for the School's purposes, including to obtain appropriate professional advice and insurance for the School.

The School collects and processes personal data [including Special Category Data] about students and parents for the following purposes:

- To enable us to comply with legal obligation and our public task to ensure appropriate governance of the School
- To ensure that those Governors appointed are done so in accordance with legal requirements
- To ensure that Governors contact details are available as required to enable them to carry out their public duty

The School collects and processes personal data about vendors and suppliers for the following purposes:

- To obtain products and services
- To enable those suppliers to provide services to the School to enable them to carry out employment and education based functions
- For supplier administration and management including evaluation potential suppliers and accounts management

CATEGORIES OF PERSONAL DATA RECIPIENTS

The School discloses personal data to the following categories of recipients:

- the Department for Education [DfE] - on a statutory basis under section 3 of The Education [Information About Individual Students] [England] Regulations 2013
- Ofsted
- Youth Support Services – under section 507B of the Education Act 1996, to enable them to provide information regarding training and careers as part of the education or training of 13-19 year olds
- Other Schools that students have attended/will attend
- NHS
- Welfare services [such as social services]
- Law enforcement officials such as police, HMRC
- LADO
- Training providers
- Professional advisors such as lawyers and consultants
- Support services [including HR support, insurance, IT support, information security, pensions and payroll]
- The Local Authority
- Occupational Health
- DBS
- Recruitment and supply agencies

The School ensures that reasons for sharing data with those organisations are in accordance with the GDPR and put in place appropriate safeguards for any personal data transfers.

PERSONAL DATA RETENTION PERIODS

Except as otherwise permitted or required by applicable law or regulation, the School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

To determine the appropriate retention period for personal data, the School considers the amount, nature, and sensitivity of personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for processing the personal data, whether the School can fulfil the purposes of processing by other means and any applicable legal requirements. The School has a Retention Policy which it abides by which contains further details about how it retains data.

The School typically retains personal data for 6 years subject to any exceptional circumstances or to comply with laws or regulations that require a specific retention period.

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

The School has implemented the following technical and organisational security measures to protect personal data:

- Encryption of personal data [including the use of secure passwords]
- Segregation of personal data from other networks
- Access control and user authentication
- Employee training on data protection and information security
- Written information security policies and procedures
- Impact assessments and evaluation of risks to personal data.

CHANGES TO THIS RECORD OF PROCESSING ACTIVITIES

The School reserves the right to amend this Record of Processing Activities from time to time consistent with the GDPR and other applicable data protection requirements including ICO guidance.

DATA SHARING AGREEMENT [INDIVIDUALS AND SMALL ORGANISATIONS]

Use this Data Sharing Agreement for smaller third party organisations [e.g. those organisations who have one / two employees working for it, such as sports coaches, photographers]. The wording given summarises the responsibilities of the organization / individual with complying with Data Protection when it would not be suitable to agree to a lengthier formal agreement. The wording below sets out their responsibilities generally regarding Data Protection.
Before setting out those responsibilities, it would be best to detail at the outset what information you are sharing, who with and reasons why.
Complete the fields highlighted below before sending to the third party.
This does not have to be sent as a formal agreement and can be sent as part of an email to clarify data protection obligations

Heston Community School will be required to share a small amount of data with [NAME OF INDIVIDUAL/COMPANY] as set out below:

[DETAILS including details of the information you will be sharing, specifically the personal data and how it will be sent to them]

In order to achieve [REASONS FOR PROCESSING DATA], [NAME] will require access to some of the School's personal data.

The parties agree to comply with data protection laws and principles. Namely [NAME] will ensure the following when handling personal data of [DETAILS e.g. staff, parents, students]:

- ❑ To comply with the data protection principles and laws from time to time in force in connection with the processing of personal data
- ❑ You will not, by any act or omission, cause a breach of data protection laws. Should any breach be caused by [NAME] then you must immediately notify the School [no later than 24 hours of becoming aware of the breach] with full details of the breach and this must be notified to the SIMS and Data Manager
- ❑ All personal data retained by [NAME] must be kept secure using appropriate measures to prevent unauthorised individuals from accessing that data accidentally or deliberately. These measures need to be implemented, maintained and monitored to ensure ongoing security
- ❑ Personal data will be kept for no longer than is necessary and destroyed securely
- ❑ Personal data should be limited to authorised personnel only and should not be shared with third parties unless you have a reason to do so [as set by data protection laws]
- ❑ Processing of personal data should not be sub-contracted to another third party without consent from the School
- ❑ [NAME] will provide the School with any information and assistance required in order to comply with data protection laws. Including providing information in order to fulfil requests for information under the General Data Protection Regulation and in order for the School to satisfy itself that [NAME] are meeting General Data Protection Regulation requirements
- ❑ [Add to this list as necessary [e.g. Use of Photography, Names etc]

It will be the responsibility of the Curriculum Areas or Support Staff to ensure that this agreement has been completed/sent prior to any personal information of students or staff being shared with external organisations or individuals.
In order for the School to monitor our processing activities, please retain a copy of the agreement or email, for your records and forward a copy to the SIMS and Data Manager.

Contact at Heston Community School _____

Third Party Organisation _____

Print Name _____ Position Held _____

Date _____ Signature _____

DATA PROTECTION IMPACT ASSESSMENT [PART 1]

Under the GDPR, DPIAs need to be used in certain circumstances including:

- New technologies and software
- School trips outside the EEA [EU countries and Norway, Lichtenstein and Iceland]
- Large scale use of sensitive data [such as medical or criminal record information]
- Change of the way personal data is processed
- Public Monitoring

This template should be used to determine whether your proposed project/activity will meet the threshold at which a DPIA is required to be completed.

This is a preliminary assessment and will not be valid until suggested edits and has been signed off by both the School and Judicium.

DATA PROTECTION IMPACT ASSESSMENT [PART 2]

This template needs to be completed and the School must accept the advice/for the DPIA to be signed off by the DPO. Once completed and signed, ensure that you retain this DPIA to evidence GDPR compliance to the ICO [and to Governors]. DPIAs need to be **reviewed annually** to ensure that the DPIA is being followed and doesn't impose any risks to individual data.

Data Protection Impact Assessment [DPIA]

Introduction

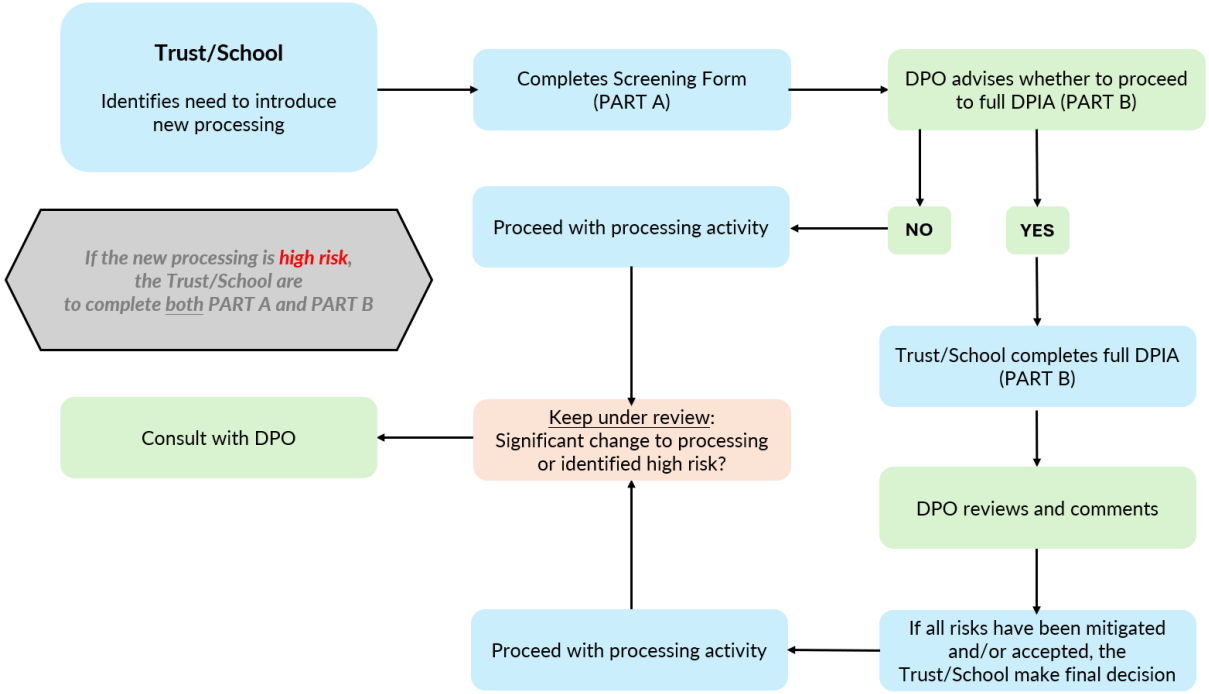
The purpose of a DPIA is to assess risk to personal data in relation to a particular processing activity.
We have created the below two-part form to help you with this process.

PART A – This is a **screening assessment**. Please complete this and follow the instructions to determine whether you are required to proceed with Part B [full DPIA]. Once Part A is completed, please return it to Judicium for checking and any preliminary information regarding the processing.

PART B – You only need to complete Part B if the screening assessment determines the processing is likely to result in a high risk. This part of the form gives opportunity to detail mitigating steps the Trust/School can take to reduce the risk involved.

REVIEW PROCESS – Once the DPIA has been completed, it must be reviewed periodically by the Trust/School to ensure ongoing compliance with data protection requirements and effectiveness of mitigation measures. It is particularly necessary to complete a review exercise when there are significant processing changes to the activity which may affect risk to personal data involved.
*Note: If there are **no** significant changes, a review can be completed but a DPO review is not required.*

Process Flowchart



This form helps ensure that the School remains compliant with data protection laws and safeguards the personal data of individuals effectively. If you are unsure on how to complete any part of this form, please contact Judicium and we can happily guide you.

The School is to complete the relevant PART[s] as far as possible. Please note that your DPO will assist you with filling out the boxes colour coded in green. Your DPO can also review the full form.

The following documents should assist you in completing this form: third party provider privacy notice, data protection policy, data sharing agreement, service level agreement, proposed contract [not an exhaustive list].

PART A – SCREENING ASSESSMENT

Name of Trust/School	Detail name of Trust/School
Date of DPIA [commencement date]	Insert date
Is this a retrospective exercise? [i.e., if this processing activity has been in place for some time already and you are carrying out a retrospective risk assessment check]	Yes/No If yes, detail here when the technology was first introduced and what prompted this review [i.e., significant change in processing or potential high risk].

Question	Answer
1. Name of third party involved in the processing activity [if applicable]	Detail here

DATA PROTECTION IMPACT ASSESSMENT
Client copy

2. Describe the processing activity • What data is being processed, why, and how? Is a third-party processor being used or is this an in-house activity? • What is the objective of this activity? • What is the intended outcome of this exercise? • Clarify the rationale behind this activity.	Detail here
3. Why and how is this the least intrusive method for achieving your intended purpose? i.e., How does this approach minimise intrusion while effectively fulfilling its intended purpose, and what factors were considered in making this determination?	Detail here
4. What personal data will you be sharing? **4a. Consider whether a Data Sharing/Processing Agreement is required.**	Set out personal data relating to all data subjects such as student, parent, staff, governors, etc.
5. Does the processing involve special category data? Note: special category data is defined as personal data revealing: • racial or ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • genetic data; • biometric data [where used for identification purposes]; • data concerning health; • data concerning a person's sex life; and • data concerning a person's sexual orientation.	Detail here
5a. Does the processing involve criminal offence data?	Yes/No Set out reasons clearly
6. Lawful Basis	Detail here: - Is this activity a necessary part of the school's functions [e.g., is it for the purpose of delivering the curriculum, ensuring good behaviour or safeguarding]? - Is this activity necessary for the performance of an employment contract? - Is the school legally obliged to carry out this activity? - Do you intend to seek consent for this activity?
6a. Lawful Basis [mandatory]	
6b. Special Category Condition [where applicable]	
6c. Criminal Offence Condition [where applicable]	

If there is no appropriate lawful basis and special category condition [where applicable] identified for the processing activity, the Trust/School cannot proceed under data protection laws.	
7. Will the processing involve automated decision-making or profiling? Note: Automated decision-making is the process of making a decision by automated means without any human involvement. Profiling analyses aspects of an individual's personality, behaviour, interests and habits to make predictions or decisions about them.	Yes/No Set out reasons clearly
8. Will the processing involve systematic monitoring of individuals [e.g., CCTV, tracking, or monitoring online behaviour]?	Yes/No
9. Will the processing involve large-scale processing of personal data? Detail also the approximate number of data subjects: 1-100 100-500 500-1000 1000+	Yes/No
10. Will the data be transferred outside the EEA?	Yes/No
11. Does the processing involve innovative technology or novel use of data? Example of innovative tech: Artificial Intelligence [AI]	Yes/No [please provide details]
12. Are there any other factors or risks you wish the DPO to consider?	Please detail
If YES to 7-12, proceed to Annex 1 and 2. If NO, please complete Annex 1 by confirming "Non-Applicable" and Annex 2.	

ANNEX 1
MITIGATIONS

Can the identified risks be mitigated/resolved sufficiently at this stage?		
International Transfers	**Response**	**Details** Specify where you read this information
Is the data being transferred internationally? Outside of the EEA.	Yes/ No	If Yes, specify the country: _____
Special Category Data	**Response**	**Details**
Referring to point 5 above, is special category data being shared as part of this processing?	Yes/ No	If Yes, specify any further detail other than under point 5: _____
Are there any other risks you need to consider at this stage?	Yes/ No	If Yes, detail here.

ANNEX 2

TRUST/SCHOOL RISK ASSESSMENT [PART A]

Is the processing likely to result in a high risk to individuals involved? **Consider**: Will the processing result in a risk of significant harm, discrimination, identity theft, financial loss, or other serious consequences for individuals?	
No – it is **not** likely to result in a high risk IF **NO** – Please complete until the end of **PART A** and then submit to Judicium for review.	Include a summary of how this risk has been mitigated
Yes – it **is likely** to result in a high risk IF **YES** - Please continue to **PART B** and then submit to Judicium for review.	Include a summary of why this processing activity requires a DPIA. Identify any risks that need to be mitigated and use this as a basis for Part B.
Trust/School Decision	
Proceed with processing as planned	Yes/No Detail reasoning
Trust / School Sign and Date	Insert name and date

ANNEX 3
DPO REVIEW/COMMENTS

DPO Review and Comments	
Lawful Basis, Special Category Condition and Criminal Offence Data	Note: If relying on Legitimate Interests, advise on Legitimate Interests Assessment.
Has the Trust/School identified risks and mitigated/resolved them sufficiently at this stage?	
Review Trust/School's risk assessment	
Conclusion	Add rationale Advise whether to proceed to PART B, unless high risk has already been identified in which case the Trust/School complete **both** PART A and B.

END OF PART A

Legitimate Interest Assessment [LIA]

There are six lawful bases under the data protection law. You must identify at least one lawful basis in order to process personal data.
Legitimate interest is arguably the most flexible basis for processing.
It is applicable to Independent Schools and other schools. If you are a publicly funded school, legitimate interest will unlikely be applicable, and you should consider an alternative.
Legitimate interest applies when you use personal data in a way that would be reasonably expected by individuals, and it would not be a privacy intrusive way of processing their data.
Be mindful that you may need to complete a Data Protection Impact Assessment [DPIA] where the risk to individuals in this processing is considered high. Ask your DPO for guidance on this.
This LIA should be completed alongside the guidance given by the Information Commissioner's Office [ICO] and can be accessed here: legitimate interests guidance.

Step 1. Purpose test
You need to assess whether you have a legitimate interest for processing this data.

Detail what data you are intending to process and why you want to process this data.	
Detail the benefit/s you expect to get from this processing.	
Do any third parties or any wider public benefit from this processing?	
How important are the benefits that you have identified?	
Supposing that you cannot proceed with this processing, what are the impacts?	
Are you complying with any specific data protection rules that apply to your processing?	
Do you need to comply with any other relevant laws or guidance?	
Are you complying with industry guidelines or codes of practice?	
Are there any ethical issues with your processing?	

Step 2. Necessity test
You need to assess whether it is necessary for the purpose you have identified.

Will the processing help you achieve your purpose? I.e., is it necessary?	
Does the processing achieve the purpose in a proportionate way?	
Can you achieve the same purpose without the processing?	
Can you achieve the same purpose in another, less intrusive way?	

Step 3. Balancing test

Consider the impact on individuals' interests, rights and freedoms. Assess whether this overrides your legitimate interests.

Are you processing special category data or criminal offence data?	Yes/No
Are you processing data which is considered as 'private'?	Yes/No
Are you processing children's data? Or the data of vulnerable individuals?	Yes/No
Is the data relating to personal or professional capacity?	Yes/No

Step 4. Reasonable expectations and likely impacts

Do you have an existing relationship with the individual?	
What's the nature of the relationship and how have you used data in the past?	
Did you collect the data directly from the individual? What did you tell them at the time?	
If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?	
How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?	
Is your intended purpose and method widely understood?	
Are you intending to do anything new or innovative?	
Do you have any evidence about expectations – e.g. from market research, focus groups or other forms of consultation?	
Are there any other factors in the particular circumstances that mean they would or would not expect the processing?	
What are the possible impacts of the processing on people?	
Will individuals lose any control over the use of their personal data?	
What is the likelihood and severity of any potential impact?	
Are some people likely to object to the processing or find it intrusive?	
Would you be happy to explain the processing to individuals?	
Can you adopt any safeguards to minimise the impact?	

Step 5. Making the decision

Can you offer individuals an opt-out?	Yes/No
Can you rely on your legitimate interests to conduct the processing?	
Do you have any comments to justify this outcome?	

LIA completed by	
Date	
Reviewed/Discussed with DPO	Yes/No

Please note that this document has been adapted from the template provided by the ICO.

PART B – FULL DPIA [Conditional]

Processing Activity: **Security measures and mitigating factors the system itself has in place**	
*Please note this needs to be completed for the **processing activity itself**.* *If there are multiple controllers or processors involved, this needs to be made clear in this section of your DPIA.*	
Questions *Please note these questions are prompts and not intended to be definitive as there may be other factors which need to be considered.*	**Answers** *In this column, please detail as far as possible the answers to the questions for each section. Should you have any questions, please send them to Judicium.*
Security Measures 1. What security measures are in place to protect personal data [e.g., encryption, firewalls, access controls]? 2. How is access to personal data restricted and monitored? 3. Is system access and activity logged, and how long are these logs retained? 4. Has the processor been independently audited or certified for security [e.g., ISO 27001, Cyber Essentials]? 5. How is personal data protected against unauthorised access, loss, or tampering? 6. What incident response plans are in place for security breaches?	
Data Retention 1. Does the processor have a data retention policy, and does it align with the school's retention schedule? 2. Can the school request early deletion or anonymisation of data? 3. How does the processor ensure that deleted data is permanently erased from all systems, including backups? 4. How often is retention compliance reviewed?	
Data Transfer 1. What security measures [e.g., encryption] are in place when transferring data? 2. If data is shared with third parties - what safeguards are in place? 3. Is there a record of all third parties who receive shared data? 4. Does the provider allow the school to control or restrict data sharing?	

Offsite Storage & Cloud Computing 1. Is the personal data held on a third party server? [i.e., leaves the school server]. 2. Where is the data physically stored, and does it remain in UK GDPR-compliant jurisdictions? 3. If data is transferred outside the EEA, what safeguards [e.g., Standard Contractual Clauses] are in place? 4. What happens if the provider needs to move data to a different jurisdiction? [i.e., does their documentation state that they will consult the Trust/school?] 5. What contingency plans are in place if the school needs to retrieve or migrate data?	
Data Subject Rights 1. How quickly can the provider support the school with a Subject Access Request [SAR]? Do they provide this assistance? 2. What procedures are in place for handling requests for data rectification, erasure, or restriction? 3. How does the provider notify the school of a data breach, and within what timeframe?	

Considerations: **Steps taken by the Trust/School to protect personal data**	
Data Access & Security Measures 1. Does the school have a clear access control policy that defines user roles and data permissions? 2. How often are access permissions reviewed and updated? 3. Are login credentials unique for each user, and is multi-factor authentication [MFA] enforced? 4. What process is in place for securely offboarding staff and revoking their access to systems and data?	
Purpose of Processing 1. Is the data processing necessary to achieve the school's objectives? 2. Are data subjects [e.g., students, parents, staff] clearly informed about why and how their data is processed? 3. Are data processing activities regularly reviewed to ensure they align with legal and educational requirements?	
Data Deletion & Retention 1. Does the school have an automated or documented process for identifying and deleting outdated data? 2. How does the school ensure that old user accounts [students, staff, parents] are removed when no longer needed? 3. Are backups securely stored and deleted in line with the school's data retention policy? 4. How does the school verify that data deletion is carried out effectively, including in third-party systems?	

Data Sharing 1. Does the school have written agreements [e.g., Data Processing Agreements or Data Sharing Agreements] with all relevant third parties? 2. How does the school ensure that shared data remains secure during and after transfer? 3. Does the school maintain an up-to-date register of all data-sharing arrangements?	
Practical Steps 1. Are staff regularly trained on their data protection responsibilities? 2. Are data protection policies and procedures easily accessible and reviewed regularly? 3. Is there a clear procedure for identifying, reporting, and responding to data protection incidents?	
Data Rights Compliance 1. In the event of a SAR, does the Trust/school have a clear understanding of how to retrieve and collate data which resides in this system [when it falls in the scope of the request]? 2. In the event of a request for erasure, does the Trust/school have the facility to delete the data off this system and know how to do it? 3. Does the Trust/school use a log where this can be reflected?	
Transparency & Consultation 1. Has the school consulted and/or communicated with stakeholders [e.g., parents, staff, students] about how their data is collected and used? 2. Are privacy notices written in clear, accessible language, and are they regularly reviewed? 3. Is there a mechanism for individuals to raise concerns or objections regarding their data?	

TRUST/SCHOOL RISK ASSESSMENT AND MITIGATIONS [PART B]

Each identified risk should be assessed based on [Low, Medium, High]:

- **Likelihood:** How likely is the risk to occur?
- **Severity:** What impact would it have if it did occur?
- **Overall Risk Level:** A combination of likelihood and severity

For each risk, consider measures to reduce its likelihood or impact.

These *may* include the following measures:

- **Technical** [e.g., encryption, access controls, secure authentication]
- **Organisational** [e.g., policies, staff training, DPIA reviews]
- **Procedural** [e.g., data minimisation, pseudonymisation]
- **Legal** [e.g., contracts, DPIAs, privacy notices]

Risk Description	Likelihood & Severity	Overall Risk Level: When assessing this, consider the mitigating measures set out above and set out the residual risk level
Detail here risk 1 identified above	L: Low/Medium/High S: Low/Medium/High	Low/Medium/High
Detail here risk 2 identified above	L: Low/Medium/High S: Low/Medium/High	Low/Medium/High
Detail here risk 3 identified above	L: Low/Medium/High S: Low/Medium/High	Low/Medium/High

Trust/School Final Decision	
Consider and detail Trust/School Final Decision: • Are the remaining risks acceptable given the safeguards? • Does the organisation accept any residual risk, or are additional measures needed? A - Proceed with processing as planned [with mitigations in place] B - Modify processing activity to reduce risk C - Do not proceed with processing	A - Provide summary B - Explain changes C - Due to high risk which cannot be mitigated
Risk Status	☐ **Mitigated** [safeguards in place] ☐ **Accepted** [residual risk deemed acceptable] ☐ **Avoided** [processing will not proceed]
Trust / School Sign and Date	Insert name and date

Accountability Checklist!

Accountability means organisations must prove they handle data properly. Processes such as DPIAs, data maps, and privacy notices help with this by documenting and demonstrating compliance.

Consider whether the following areas need to be updated with this new processing in mind. Note, this will not always be necessary. If you are unsure, please raise this with Judicium and we can assist.

	Indicate whether the following have been updated:
Record of Processing Activities	Yes/No
Data Map	Yes/No
Privacy Notice	Yes/No
Third parties register	Yes/No
Do any other departments need to be contacted such as your IT, cyber team or MIS team?	Detail here

Please also ensure to keep all your completed DPIAs on JEDU and/or secure internal folder.

DPO Review and Comments	
Mitigating measures	Detail advice
Review Risk Assessment	Detail advice/reasoning
Conclusion	Detail and add date of check

END OF PART B

REVIEW PROCESS – DPIA REVIEW AND MONITORING

A DPIA is a living document and should be reviewed periodically to ensure it remains effective and relevant.

1. **Review Triggers:**
    - Significant changes to the processing activity
    - Introduction of new technologies or processes
    - Updates to legal or regulatory requirements
    - Reports of data breaches or security incidents
    - Complaints or concerns raised by data subjects.
2. **Periodic Review Schedule:**
    - Set a timeframe for periodic reviews [e.g., annually]
    - Assign responsibility for conducting reviews.
3. **Consultation and Documentation:**
    - Engage relevant stakeholders [staff, IT, legal etc] during the review process
    - Consult with DPO where the processing has **significantly changed** or the **risk increased** [otherwise, you do not need to contact the DPO]
    - Update the DPIA as needed reflecting clearly the changes made.

Effectiveness and Mitigations	
Are the implemented measures still effective in mitigating risks?	Yes/No If No, detail here
Have new risks emerged which need assessing?	Yes/No If Yes, detail here
Are further changes or additional safeguards required?	Yes/No If Yes, detail here

Is further action required?	
No further action required	Yes/No
Further action is required	Yes/No
PART B updated	N/A **or** Detail here the changes made to PART B
Trust / School Sign and Date	Insert name and date

END OF REVIEW PROCESS

GENERAL DATA PROTECTION REGULATIONS [UK GDPR] - 10 STEPS WE CAN TAKE NOW

1. **Secure Your Machine from Unauthorised Access**
   - Access to your desktop/laptop is password protected
   - Passwords are changed regularly
   - Ensure that you log-out, or lock unattended machines when not in use
2. **Don't Give Out Sensitive Information**
   - Don't give out confidential information over the phone
   - Always ask the individual to put their request in writing to the School at info@hestoncs.org
   - Send information securely via encrypted email or recorded delivery
   - Don't upload/share any personal data of students and/or staff with external websites, providers, suppliers etc without a General Data Protection Impact Assessment and Data Sharing Agreement being completed; if unsure, I will always check with the SIMS and Data Manager
3. **Secure Your Documents, Planners and Mobile Devices**
   - Encrypt/password protect documents where possible
   - Limit access to shared drives that contain confidential information
4. **Keep Paper Documents and Personal Data Safe and Secure**
   - Adopt a Clear Desk Policy
   - Keep sensitive paper documents off your desk and off wall displays
   - Shred and/or file papers as a matter of course; do not leave them sitting on top of desks
   - Lock sensitive documents in a draw/filing cabinet
   - Who has access to keys? Don't leave them in the door
   - Store passwords safely – not on post-it notes or within note books or planners
   - Keep doors locked when not in use if rooms contain sensitive/personal data
   - Do not give out your pass or keys to other members of staff, students or visitors
5. **Be Careful with Remote Access and Storage Devices**
   - Accessing confidential documents remotely: ensure adequate security, for example, mobile devices are password protected; always obtain the approval from the Facilities, Premises and Compliance Manager if unsure
   - Do not connect devices, for example, mobile phones, cameras etc directly to Heston School's PCs
   - USBs, portable storage drives and mobile storage devices are no longer be permissible unless specific approval has been given by SIMS & Data Manager and the correct safeguards put in place
   - Do not save files/images on to my personal computers or hardware
   - Always access your email through RMUnify to ensure the correct level of security
   - When working off-site, use CC4 to access your Heston Desktop remotely
   - Only use the School's equipment for recording student activities or images, for example: School Trips, Activities, clubs and only if the students/parents have given their explicit consent to do so in writing; check with the SIMS & Data Manager if unsure
   - Do not record, share, or publish and personal information or images of students, staff and contractors without their explicit consent being recorded in SIMS
6. **Act Fast to Report a Data Breach [72 Hours to Report and Investigate]**
   - Time frames under the regulations are shortening
   - Report any data breach immediately to the SIMS & Data Manager
   - 72 hours to report and investigate a Data Breach before referring on to the DPO / ICO
   - Provide evidence as necessary
   - Do not carry out an investigation yourself; always refer to your Line Manager or SIMS & Data Manager
7. **Beware of Viruses and Hacking**
   - Don't open emails from recipients you are unsure of; always alert the Facilities, Premises and Compliance Manager of suspicious emails immediately
   - Ensure machines have anti-virus software are updated regularly
   - Do not download any un-authorised software without permission from the Facilities, Premises and Compliance Manager
8. **Better Safe Than Sorry – Always Report if Unsure**
   - Obligation to notify breaches applies to everyone
   - If you are unsure of the potential risk, always report it to the SIMS & Data Manager
   - Don't assume everything will be okay; it's better to be safe than sorry
9. **Email Etiquette and Encryption**
   - All emails should be sent via the School's encrypted email
   - Only send an email unencrypted if there is no other secure method
   - Do not put personal/sensitive information about student/staff etc in the body of an email
   - Personal/sensitive information sent via email, should be sent as a password protected document; with a non-generic password forwarded via the telephone
   - Proof read all communications carefully before sending, including that the email is addressed to the correct recipient[s]
10. **Data** Back Up, Retention and Destruction
    - Does data need to be retained
    - Can it be archived/destroyed
    - Ensure that it is done securely [shredding, confidential waste bins] and that it follows the School's GDPR Policy and Retention Guidelines

PRIVACY NOTICE FOR GOVERNORS AND VOLUNTEERS

Heston Community School is committed to protecting the privacy and security of your personal information. This privacy notice describes how the School collects and use personal information about you during and after your work relationship with us, in accordance with the UK General Data Protection Regulation [UK GDPR].

Following Brexit, Regulation [EU] 2016/679, General Data Protection Regulation [GDPR] is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR. It applies to Governors and volunteers.

WHO COLLECTS THIS INFORMATION

Heston Community School is a 'Data Controller.' This means that the School is responsible for deciding how the School holds and use personal information about you.

The School is required under data protection legislation to notify you of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and the School may update this notice at any time.

It is important that you read this notice, together with any other privacy notice the School may provide on specific occasions when the School is collecting or processing personal information about you, so that you are aware of how and why the School is using such information.

DATA PROTECTION PRINCIPLES

The School complies with the data protection principles when gathering and using personal information, as set out in our Data Protection Policy.

THE CATEGORIES OF INFORMATION THAT THE SCHOOL COLLECTS, PROCESSES, HOLDS AND SHARES

The School may collect, store and use the following categories of personal information about you:

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses
- Emergency contact information such as names, relationship, phone numbers and email addresses
- Education details
- DBS details
- Employment details
- Information about business and pecuniary interests
- Information acquired as part of your application to become a Governor
- Criminal records information as required by law to enable you to work with children
- Information about your use of our IT, communications and other systems, and other monitoring information
- Photographs
- Images captured by the School's CCTV system
- Video recordings captured by the School's video conferencing platform
- Your racial or ethnic origin, sex or sexual orientation, religious or similar beliefs
- Details in references about you that we give to others.

HOW THE SCHOOL COLLECTS THIS INFORMATION

The School may collect this information from you directly, from the DBS, other employees and professionals the School may engage, automated monitoring of our websites and other technical systems such as our computer networks and connects, CCTV and access control systems, remote access systems, email and instant messaging systems, intranet and internet facilities.

A majority of the information that the School collects from you is mandatory, however there is some information that you can choose whether or not to provide it to us. Whenever the School seeks to collect information from you, the School makes it clear whether you must provide this information [and if so, what the possible consequences are of not complying], or whether you have a choice.

HOW THE SCHOOL USES YOUR INFORMATION

The School only uses your personal information when the law allows us to. Most commonly, the School uses your information in the following circumstances:

- Where you have provided your consent
- Where the School needs to perform the contract the School has entered into with you
- Where the School needs to comply with a legal obligation [such as health and safety legislation and under statutory codes of practice]
- Where it is needed in the public interest or for official purposes
- Where it is necessary for our legitimate interests [or those of a third party] and your interests, rights and freedoms do not override those interests.

The School needs all the categories of information in the list above primarily to allow us to comply with our legal obligations and to enable us as a School to perform our public task. Please note that the School may process your information without your knowledge or consent, where this is require or permitted by law.

The situations in which the School processes your personal information are listed below:

- To determine appointment and suitability as a Governor
- To deal with election of Governors
- To comply with safeguarding obligations
- To provide details on our website or online databases about Governors
- To communicate with third parties and other stakeholders to the School
- For business management and planning purposes [including accounting, budgetary and health and safety purposes
- For financial purposes [such as expenses]
- To deal with any complaints/investigations as required
- When you sit on a panel or committee, name and comments as well as decisions made
- To send communications in your role as Governor
- For education, training and development requirements
- In order to review governance of the School
- In order to comply with any legal dispute or any legal obligations
- In order to comply with regulatory requirements or health and safety obligations
- To ensure system security, including preventing unauthorised access to our networks
- To monitor use of our systems to ensure compliance with our IT processes
- To receive advice from external advisors and consultants
- To liaise with regulatory bodies [such as the DfE, DBS]
- Dealing with termination of your appointment.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide certain information when requested, the School may be prevented from complying with our legal obligations [such as to ensure health and safety]. Where you have provided us with consent to use your data, you may withdraw this consent at any time.

The School only uses your personal information for the purposes for which the School collected it, unless the School reasonably considers that the School needs to use it for another reason and that reason is compatible with the original purpose. If the School needs to use your personal information for an unrelated purpose, the School will notify you and will explain the legal basis which allows us to do so.

HOW THE SCHOOL USES PARTICULARLY SENSITIVE INFORMATION

Sensitive personal information [as defined under the UK GDPR as 'Special Category Data'] require higher levels of protection and further justification for collecting, storing and using this type of personal information. The School may process this data in the following circumstances:

- In limited circumstances, with your explicit written consent
- Where the School needs to carry out our legal obligations in line with our Data Protection Policy
- Where it is needed in the public interest, such as for equal opportunities monitoring [or in relation to our pension scheme]
- Where it is needed in relation to legal claims or where it is necessary to protect your interests [or someone else's interests] and you are not capable of giving your consent.

CRIMINAL CONVICTIONS

The School may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. The School only collects information about criminal convictions if it is appropriate given the nature of the role and where the School is legally able to do so.

Where appropriate the School collects information about criminal convictions as part of the recruitment process or the School may be notified of such information directly by you in the course of working for us.

AUTOMATED DECISION MAKING

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. The School are allowed to use automated decision making in the following circumstances: -

- Where the School have notified you of the decision and given you 21 days to request a reconsideration
- Where it is necessary to perform the contract with you and appropriate measures are put in place to safeguard your rights; or
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless the School has a lawful basis for doing so and the School has notified you.

SHARING DATA

The School may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where the School has another legitimate interest in doing so. These include the following:

- Government departments or agencies
- The Local Authority
- Suppliers and Service providers
- Professional advisors and consultants
- The Department for Education
- Law enforcement
- Support services
- DBS

Information will be provided to those agencies securely or anonymised where possible.

The recipient of the information will be bound by confidentiality obligations, the School requires them to respect the security of your data and to treat it in accordance with the law.

The School may transfer your personal information outside the UK and the EU. If the School does, you can expect a similar degree of protection in respect of your personal information.

RETENTION PERIODS

Except as otherwise permitted or required by applicable law or regulation, the School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

To determine the appropriate retention period for personal data, the School considers the amount, nature, and sensitivity of personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for processing the personal data, whether the School can fulfil the purposes of processing by other means and any applicable legal requirements.

Once you are no longer a Governor or volunteer of the School, the School will retain and securely destroy your personal information in accordance with our Data Retention Policy.

SECURITY

The School has put in place measures to protect the security of your information i.e. against it being accidentally lost, used or accessed in an unauthorised way]. In addition, the School limits access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

Third parties will only process your personal information on our instructions and where they have agreed to treat information confidentially and to keep it secure.

The School has put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where the School is legally required to do so.

Automated Decision Making
Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision making in limited circumstances.
Governors/volunteers will not be subject to automated decision-making, unless we have a lawful basis for doing so and we have notified you.

Biometric Data
At [name of school] we would like to use your information as part of an automated [i.e., electronically operated] recognition system. This is for the purposes of [specify what purpose is – e.g., catering, library access]. The information that we wish to use is referred to as 'biometric information'. This data will only be processed once we have obtained appropriate consent. For further information in relation to this, please see our Biometrics policy.

YOUR RIGHTS OF ACCESS, CORRECTION, ERASURE AND RESTRICTION

It is important that the personal information the School holds about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Under certain circumstances by law you have the right to:

- Access your personal information [commonly known as a 'Subject Access Request']. This allows you to receive a copy of the personal information the School holds about you and to check the School is lawfully processing it. You will not have to pay a fee to access your personal information. However the School may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively the School may refuse to comply with the request in such circumstances
- Correction of the personal information the School holds about you. This enables you to have any inaccurate information the School holds about you corrected
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it
- To object to processing in certain circumstances [for example for direct marketing purposes]
- To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact the PA to the Headteacher in writing.

The School may need to request specific information from you to help us confirm your identity and ensure your right to access the information [or to exercise any of your other rights]. This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the PA to the Headteacher. Once the School has received notification that you have withdrawn your consent, the School no longer processes your information for the purpose or purposes you originally agreed to, unless the School has another legitimate basis for doing so in law.

HOW TO RAISE A CONCERN

The School hopes that the PA to the Headteacher can resolve any query you raise about our use of your information in the first instance. The School has appointed a Data Protection Officer [DPO] to oversee compliance with data protection and this privacy notice. If you have any questions about how the School handles your personal information which cannot be resolved by the PA to the Headteacher then you can contact the DPO on the details below:

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Lead Contact: Craig Stilwell

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues.

CHANGES TO THIS PRIVACY NOTICE

The School reserves the right to update this privacy notice at any time, and the School provides you with a new privacy notice when the School makes any substantial updates. The School may also notify you in other ways from time to time about the processing of your personal information.

PRIVACY NOTICE FOR STAFF

Heston Community School is committed to protecting the privacy and security of your personal information. This privacy notice describes how the School collects and use personal information about you during and after your work relationship with us, in accordance with the UK General Data Protection Regulation [UK GDPR].

Following Brexit, Regulation [EU] 2016/679, General Data Protection Regulation [GDPR] is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.

It applies to all current and former employees, workers and contractors.

WHO COLLECTS THIS INFORMATION

Heston Community School is a 'Data Controller.' This means that the School is responsible for deciding how the School holds and use personal information about you.

The School is required under data protection legislation to notify you of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and the School may update this notice at any time.

It is important that you read this notice, together with any other privacy notice the School may provide on specific occasions when the School is collecting or processing personal information about you, so that you are aware of how and why the School is using such information.

DATA PROTECTION PRINCIPLES

The School complies with the data protection principles when gathering and using personal information, as set out in our Data Protection Policy.

THE CATEGORIES OF INFORMATION THAT THE SCHOOL COLLECTS, PROCESSES, HOLDS AND SHARES

The School may collect, store and use the following categories of personal information about you:

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses
- Emergency contact information such as names, relationship, phone numbers and email addresses
- Information collected during the recruitment process that the School retains during your employment including references, proof of right to work in the UK, application form, CV, qualifications
- Employment contract information such as start dates, hours worked, post, roles
- Education and training details
- Details of salary and benefits including payment details, payroll records, tax status information, national insurance number, pension and benefits information
- Details of any dependants
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information

- Information in your sickness and absence records such as number of absences and reasons[including sensitive personal information regarding your physical and/or mental health]
- Criminal records information as required by law to enable you to work with children
- Your trade union membership
- Information on grievances raised by or involving you
- Information on conduct and/or other disciplinary issues involving you
- Details of your appraisals, performance reviews and capability issues
- Details of your time and attendance records
- Information about the use of our IT, communications and other systems, and other monitoring information
- Details of your use of business-related social media
- Images of staff captured by the School's CCTV system
- Recordings of staff from the School's video conferencing platform
- Your use of public social media [only in very limited circumstances, to check specific risks for specific functions within the School, you will be notified separately if this is to occur]
- Details in references about you that the School gives to others
- Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs.

HOW THE SCHOOL COLLECTS THIS INFORMATION

The School may collect this information from you, your personnel records, the Home Office, pension administrators, your doctors, from medical and occupational health professionals the School engages, the DBS, your trade union, other employees, other professionals the School may engage [e.g. to advise us generally], automated monitoring of the School's websites and other technical systems such as our computer networks and connections, CCTV and access control systems, remote access systems, email and instant messaging systems, intranet and internet facilities

HOW THE SCHOOL USES YOUR INFORMATION

The School only uses your personal information when the law allows us to. Most commonly, the School uses your information in the following circumstances:

- Where the School needs to perform the contract the School has entered into with you
- Where the School needs to comply with a legal obligation [such as health and safety legislation, under statutory codes of practice and employment protection legislation]
- Where it is needed in the public interest or for official purposes
- Where it is necessary for our legitimate interests [or those of a third party] and your interests, rights and freedoms do not override those interests
- When you have provided us with consent to process your personal data.

The School needs all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. Please note that the School may process your information without your knowledge or consent, where this is require or permitted by law.

The situations in which the School processes your personal information are listed below:

- To determine recruitment and selection decisions on prospective employees
- In order to carry out effective performance of the employees contract of employment and to maintain employment records
- To comply with regulatory requirements and good employment practice
- To carry out vetting and screening of applicants and current staff in accordance with regulatory and legislative requirements
- Enable the development of a comprehensive picture of the workforce and how it is deployed and managed
- To enable management and planning of the workforce, including accounting and auditing
- Personnel management including retention, sickness and attendance
- Performance reviews, managing performance and determining performance requirements
- In order to manage internal policy and procedure
- Human resources administration including pensions, payroll and benefits
- To determine qualifications for a particular job or task, including decisions about promotions
- Evidence for possible disciplinary or grievance processes
- Complying with legal obligations
- To monitor and manage staff access to our systems and facilities in order to protect our networks, the personal data of our employees and for the purposes of safeguarding
- To monitor and protect the security of our network and information, including preventing unauthorised access to our computer network and communications systems and preventing malicious software distribution
- Education, training and development activities
- To monitor compliance with equal opportunities legislation
- To answer questions from insurers in respect of any insurance policies which relate to you
- Determinations about continued employment or engagement
- Arrangements for the termination of the working relationship
- Dealing with post-termination arrangements
- Health and safety obligations
- Prevention and detection of fraud or other criminal offences
- To defend the School in respect of any investigation or court proceedings and to comply with any court or tribunal order for disclosure.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide certain information when requested, the School may not be able to perform the contract the School has entered into with you [such as paying you or providing a benefit], or the School may be prevented from complying with our legal obligations [such as to ensure the health and safety of our workers].

The School will only use your personal information for the purposes for which the School collected it, unless the School reasonably consider that the School needs to use it for another reason and that reason is compatible with the original purpose. If the School needs to use your personal information for an unrelated purpose, the School will notify you and will explain the legal basis which allows us to do so.

HOW THE SCHOOL USES PARTICULARLY SENSITIVE INFORMATION

Sensitive personal information [as defined under the UK GDPR as 'Special Category Data'] require higher levels of protection and further justification for collecting, storing and using this type of personal information. The School may process this data in the following circumstances:

- In limited circumstances, with your explicit written consent
- Where the School needs to carry out our legal obligations in line with our Data Protection Policy
- Where it is needed in the public interest, such as for equal opportunities monitoring [or in relation to our pension scheme]
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards. Less commonly, the School may process this type of information where it is needed in relation to legal claims or where it is necessary to protect your interests [or someone else's interests] and you are not capable of giving your consent

THE SCHOOL USES THIS INFORMATION IN THE FOLLOWING WAYS:

- Collecting information relating to leave of absence, which may include sickness absence or family related leave
- To comply with employment and other laws
- Collecting information about your physical or mental health, or disability status, to ensure your health and welfare in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to manage sickness absence and to administer benefits
- Collecting information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting
- To record trade union membership information to pay trade union premiums and to comply with employment law obligations.

CRIMINAL CONVICTIONS

The School may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. The School will only collect information about criminal convictions if it is appropriate given the nature of the role and where the School is legally able to do so.

Where appropriate the School collects information about criminal convictions as part of the recruitment process or the School may be notified of such information directly by you in the course of working for us.

SHARING DATA

The School may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where the School has another legitimate interest in doing so. These include the following:

- the Department for Education [DfE]
- Ofsted
- The Local Authority

- Prospective Employers
- Welfare services [such as social services]
- Law enforcement officials such as police, HMRC
- LADO
- Training providers
- Professional advisors such as lawyers and consultants
- Support services [including HR support, insurance, IT support, information security, pensions and payroll]
- Occupational Health
- DBS
- Recruitment and supply agencies.

Information will be provided to those agencies securely or anonymised where possible.

The recipient of the information will be bound by confidentiality obligations, the School requires them to respect the security of your data and to treat it in accordance with the law.

The School may transfer your personal information outside the UK and the EU. If the School do, you can expect a similar degree of protection in respect of your personal information.

RETENTION PERIODS

Except as otherwise permitted or required by applicable law or regulation, the School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

To determine the appropriate retention period for personal data, the School considers the amount, nature, and sensitivity of personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for processing the personal data, whether the School can fulfil the purposes of processing by other means and any applicable legal requirements.

Once you are no longer an employee, worker or contractor of the company the School will retain and securely destroy your personal information in accordance with our Data Retention Policy.

The School typically retains personal data for 6 years subject to any exceptional circumstances or to comply with laws or regulations that require a specific retention period.

SECURITY

The School has put in place measures to protect the security of your information i.e. against it being accidentally lost, used or accessed in an unauthorised way]. In addition, the School limits access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

Third parties will only process your personal information on our instructions and where they have agreed to treat information confidentially and to keep it secure.

The School has put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where the School is legally required to do so.

AUTOMATED DECISION MAKING

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision making in the following circumstances: -

- Where we have notified you of the decision and given you 21 days to request a reconsideration
- Where it is necessary to perform the contract with you and appropriate measures are put in place to safeguard your rights or
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

BIOMETRIC DATA

At the School we would like to use your information as part of an automated [i.e. electronically operated] recognition system. This is for the purpose of catering. The information that we wish to use is referred to as Biometric Information. This data will only be processed once we have obtained the appropriate consent. For further information in relation to this, please see our Biometrics Policy.

YOUR RIGHTS OF ACCESS, CORRECTION, ERASURE AND RESTRICTION

It is important that the personal information the School holds about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Under certain circumstances by law you have the right to:

- Access your personal information [commonly known as a 'Subject Access Request']. This allows you to receive a copy of the personal information the School holds about you and to check the School is lawfully processing it. You will not have to pay a fee to access your personal information. However the School may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively the School may refuse to comply with the request in such circumstances
- Correction of the personal information the School holds about you. This enables you to have any inaccurate information the School holds about you corrected
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it
- To object to processing in certain circumstances [for example for direct marketing purposes]
- To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact the PA to the Headteacher in writing.

The School may need to request specific information from you to help us confirm your identity and ensure your right to access the information [or to exercise any of your other rights]. This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the PA to the Headteacher. Once the School has received notification that you have withdrawn your consent, the School will no longer process your information for the purpose or purposes you originally agreed to, unless the School has another legitimate basis for doing so in law.

HOW TO RAISE A CONCERN

The School hopes that the PA to the Headteacher can resolve any query you raise about our use of your information in the first instance.

The School has appointed a data protection officer [DPO] to oversee compliance with data protection and this privacy notice. If you have any questions about how the School handle your personal information which cannot be resolved by the PA to the Headteacher, then you can contact the DPO on the details below:

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Lead Contact: Craig Stilwell

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues.

CHANGES TO THIS PRIVACY NOTICE

The School reserves the right to update this privacy notice at any time, and the School provides you with a new privacy notice when the School makes any substantial updates. The School may also notify you in other ways from time to time about the processing of your personal information.

PRIVACY NOTICE FOR JOB APPLICANTS

Heston Community School is committed to protecting the privacy and security of your personal information. This privacy notice describes how the School collects and use personal information about you during and after your work relationship with us, in accordance with the UK General Data Protection Regulation [UK GDPR].

Following Brexit, Regulation [EU] 2016/679, General Data Protection Regulation [GDPR] is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.

Successful candidates should refer to our Privacy Notice for Staff for information about how their personal data is stored and collected.

WHO COLLECTS THIS INFORMATION

Heston Community School is a 'Data Controller.' This means that the School is responsible for deciding how the School holds and use personal information about you.

The School is required under data protection legislation to notify you of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and the School may update this notice at any time.

It is important that you read this notice, together with any other privacy notice the School may provide on specific occasions when the School is collecting or processing personal information about you, so that you are aware of how and why the School is using such information.

DATA PROTECTION PRINCIPLES

The School complies with the data protection principles when gathering and using personal information, as set out in our Data Protection Policy.

THE CATEGORIES OF INFORMATION THAT THE SCHOOL COLLECTS, PROCESSES, HOLDS AND SHARES

The School may collect, store and use the following categories of personal information about you up to the shortlisting stage of the recruitment process:

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses
- Emergency contact information such as names, relationship, phone numbers and email addresses
- Information collected during the recruitment process that the School retains during your employment including proof of right to work in the UK, information entered on the application form, CV, qualifications
- Details of your employment history including job titles, salary and working hours
- Information regarding your criminal record as required by law to enable you to work with children
- Details of your referees and references
- Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs.

The School may also collect information after the shortlisting and interview stage in order to make a final decision on where to recruit, including criminal record information, references, information regarding qualifications. The School may also ask about details of any conduct, grievance or performance issues, appraisals, time and attendance from references provided by you.

HOW THE SCHOOL COLLECTS THIS INFORMATION

The School may collect this information from you, your referees, your education provider, relevant professional bodies, the Home Office and from the DBS.

HOW THE SCHOOL USES YOUR INFORMATION

The School only uses your personal information when the law allows us to. Most commonly, the School uses your information in the following circumstances:

- Where the School needs to take steps to enter into a contract with you
- Where the School needs to comply with a legal obligation [such as health and safety legislation, under statutory codes of practice and employment protection legislation]
- Where it is needed in the public interest or for official purposes
- Where it is necessary for our legitimate interests [or those of a third party] and your interests, rights and freedoms do not override those interests
- Where you have provided your consent for us to process your personal data.

Generally the purpose of us collecting your data is to enable us to facilitate safe recruitment and determine suitability for the role. The School also collects data in order to carry out equal opportunities monitoring and to ensure appropriate access arrangements are put in place if required.

If you fail to provide certain information when requested, the School may not be able to take the steps to enter into a contract with you [for example if incorrect references are provided], or the School may be prevented from complying with our legal obligations [such as to determine suitability to work with children].

The School only uses your personal information for the purposes for which the School collected it, unless the School reasonably considers that the School needs to use it for another reason and that reason is compatible with the original purpose. If the School needs to use your personal information for an unrelated purpose, the School will notify you and explain the legal basis which allows us to do so.

HOW THE SCHOOL USES PARTICULARLY SENSITIVE INFORMATION

Sensitive personal information [as defined under the UK GDPR as 'Special Category Data'] require higher levels of protection and further justification for collecting, storing and using this type of personal information. The School may process this data in the following circumstances:

- In limited circumstances, with your explicit written consent
- Where the School needs to carry out our legal obligations in line with our Data Protection Policy
- Where it is needed in the public interest, such as for equal opportunities monitoring

- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards. Less commonly, the School may process this type of information where it is needed in relation to legal claims or where it is necessary to protect your interests [or someone else's interests] and you are not capable of giving your consent

CRIMINAL CONVICTIONS

The School may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. The School will only collect information about criminal convictions if it is appropriate given the nature of the role and where the School is legally able to do so.

Where appropriate the School collects information about criminal convictions as part of the recruitment process or the School may be notified of such information directly by you in the course of working for us.

SHARING DATA

The School may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where the School has another legitimate interest in doing so.

These include the following:

- Academic or regulatory bodies to validate qualifications/experience [for example the teaching agency]
- Referees
- The Local Authority in order to meet our legal obligations for sharing data with it
- Other schools
- DBS
- Recruitment and supply agencies.

The School may also need to share some of the above categories of personal information with other parties, such as HR consultants and professional advisers. Usually information will be anonymised but this may not always be possible. The recipients of the information will be bound by confidentiality obligations. The School may also be required to share some personal information with our regulators or as required to comply with the law.

RETENTION PERIODS

Except as otherwise permitted or required by applicable law or regulation, the School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

How long the School keeps your information will depend on whether your application is successful and you become employed by us, the nature of the information concerned and the purposes for which it is processed. Full details on how long the School keeps personal data for is set out in our Data Retention Policy Retention Policy.

SECURITY

The School has put in place measures to protect the security of your information i.e. against it being accidentally lost, used or accessed in an unauthorised way]. In addition, the School limits access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

Third parties will only process your personal information on our instructions and where they have agreed to treat information confidentially and to keep it secure.

The School has put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where the School is legally required to do so.

YOUR RIGHTS OF ACCESS, CORRECTION, ERASURE AND RESTRICTION

It is important that the personal information the School holds about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Under certain circumstances by law you have the right to:

- Access your personal information [commonly known as a 'Subject Access Request']. This allows you to receive a copy of the personal information the School holds about you and to check the School is lawfully processing it. You will not have to pay a fee to access your personal information. However the School may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively the School may refuse to comply with the request in such circumstances
- Correction of the personal information the School holds about you. This enables you to have any inaccurate information the School holds about you corrected
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it
- To object to processing in certain circumstances [for example for direct marketing purposes]
- To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact the PA to the Headteacher in writing.

The School may need to request specific information from you to help us confirm your identity and ensure your right to access the information [or to exercise any of your other rights]. This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the PA to the Headteacher. Once the School has received notification that you have withdrawn your consent, the School no longer processes your information for the purpose or purposes you originally agreed to, unless the School has another legitimate basis for doing so in law.

HOW TO RAISE A CONCERN

The School hopes that the PA to the Headteacher can resolve any query you raise about our use of your information in the first instance.

The School has appointed a Data Protection Officer [DPO] to oversee compliance with data protection and this privacy notice. If you have any questions about how the School handles your personal information which cannot be resolved by the PA to the Headteacher, then you can contact the DPO on the details below:

Data Protection Officer: Judicium Consulting Limited Address: 72 Cannon Street, London, EC4N 6AE Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk Lead Contact: Craig Stilwell

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues.

PRIVACY NOTICE FOR PARENTS AND STUDENTS

Heston Community School is committed to protecting the privacy and security of personal information. This privacy notice describes how the School collects and uses personal information about students, in accordance with the UK General Data Protection Regulation [UK GDPR], section 537A of the Education Act 1996 and section 83 of the Children Act 1989.

Following Brexit, Regulation [EU] 2016/679, General Data Protection Regulation [GDPR] is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.

WHO COLLECTS THIS INFORMATION

Heston Community School is a 'Data Controller.' This means that the School is responsible for deciding how the School holds and uses personal information about students and parents.

THE CATEGORIES OF STUDENT INFORMATION THAT THE SCHOOL COLLECTS, PROCESSES, HOLDS AND SHARES

The School may collect, store and use the following categories of personal information about you:

- Personal information such as name, student number, date of birth, gender and contact information
- Emergency contact and family lifestyle information such as names, relationship, phone numbers and email addresses
- Characteristics [such as ethnicity, language, nationality, country of birth and Free School Meal eligibility]
- Attendance details [such as sessions attended, number of absences and reasons for absence]
- Post 16 learning information
- Performance and assessment information
- Behavioural information [including exclusions]
- Special educational needs information
- Relevant medical information
- Special categories of personal data [including [biometric data, ethnicity, relevant medical information, special educational needs information]
- Images of students engaging in School activities, and images captured by the School's CCTV system
- Recordings of students and/or parents from the School's video conferencing platform
- Information about the use of our IT, communications and other systems, and other monitoring information

COLLECTING THIS INFORMATION

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the UK General Data Protection Regulation, the School informs you whether you are required to provide certain student information to us or if you have a choice in this.

It is important that the personal information the School holds about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

HOW THE SCHOOL USES YOUR PERSONAL INFORMATION

The School holds student data and use it for:

Student selection [and to confirm the identity of prospective students and their parents]

- Providing education services and extra-curricular activities to students, and monitoring students' progress and educational needs
- Informing decisions such as the funding of Schools
- Assessing performance and to set targets for Schools
- Safeguarding students' welfare and providing appropriate pastoral [and where necessary medical] care
- Support teaching and learning
- Giving and receive information and references about past, current and prospective students, and to provide references to potential employers of past students
- Managing internal policy and procedure
- Enabling students to take part in assessments, to publish the results of examinations and to record student achievements
- To carry out statistical analysis for diversity purposes
- Legal and regulatory purposes [for example child protection, diversity monitoring and health and safety] and to comply with legal obligations and duties of care
- Enabling relevant authorities to monitor the School's performance and to intervene or assist with incidents as appropriate
- Monitoring use of the School's IT and communications systems in accordance with the School's Information Security Policy
- Making use of photographic images of students in School publications, on the School website and on social media channels
- Security purposes, including CCTV
- Where otherwise reasonably necessary for the School's purposes, including to obtain appropriate professional advice and insurance for the School
- To provide support to students after they leave the School

THE LAWFUL BASIS ON WHICH THE SCHOOL USES THIS INFORMATION

The School will only use your information when the law allows us to. Most commonly, the School uses your information in the following circumstances:

- Consent: the individual has given clear consent to process their personal data for a specific purpose
- Contract: the processing is necessary for a contract with the individual
- Legal obligation: the processing is necessary to comply with the law [not including contractual obligations]
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law
- The Education Act 1996: for Departmental Censuses 3 times a year. More information can be found at:
- https://www.gov.uk/education/data-collection-and-censuses-for-Schools

The School needs all the categories of information in the list above primarily to allow us to comply with legal obligations. Please note that the School may process information without knowledge or consent, where this is require or permitted by law.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

Special categories of particularly sensitive personal information, such as information about your health, racial or ethnic origin, sexual orientation, or biometrics require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations in line with our data protection policy.
- Where it is needed in the public interest, such as for equal opportunities monitoring.
- Where it is necessary to protect you or another person from harm.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests [or someone else's interests] and you are not capable of giving your consent, or where you have already made the information public.

SHARING DATA

The School may need to share your data with third parties where it is necessary. There are strict controls on who can see your information. The School will not share your data if you have advised us that you do not want it shared unless it's the only way the School can make sure you stay safe and healthy or the School is legally required to do so.

The School shares student information with:

- The Department for Education [DfE] - on a statutory basis under section 3 of The Education [Information About Individual Students] [England] Regulations 2013
- Ofsted
- Youth Support Services – under section 507B of the Education Act 1996, to enable them to provide information regarding training and careers as part of the education or training of 13-19 year olds
- The Local Authority
- Other Schools that students have attended/will attend
- NHS
- Welfare services [such as social services]
- Law enforcement officials such as police, HMRC
- Local Authority Designated Officer
- Professional advisors such as lawyers and consultants
- Support services [including insurance, IT support, information security]
- Providers of learning software such as [e.g. My Maths, Edukey]

Information will be provided to those agencies securely or anonymised where possible.

The recipient of the information will be bound by confidentiality obligations, the School requires them to respect the security of your data and to treat it in accordance with the law.

The School may transfer your personal information outside the UK and the EU. If the School does, you can expect a similar degree of protection in respect of your personal information.

WHY THE SCHOOL SHARES THIS INFORMATION

The School does not share information about our students with anyone without consent unless otherwise required by law.

For example, the School shares students' data with the DfE on a statutory basis which underpins School funding and educational attainment. To find out more about the data collection requirements placed on us by the DfE please go to:

https://www.gov.uk/education/data-collection-and-censuses-for-Schools

STORING STUDENT DATA

The School keeps information about students on computer systems and sometimes on paper.

Except as required by law, the School only retains information about students for as long as necessary in accordance with timeframes imposed by law and our internal policy.

Full details on how long we keep personal data for is set out in our Data Retention Policy. If you require further information about our retention periods, you can request a copy of the School policy by emailing the School on info@hestoncs.org

BIOMETRIC DATA

The School would like to use your information as part of an automated [i.e. electronically operated] recognition system. This is for the purposes of catering, library access. The information that we wish to use is referred to as 'biometric information'. This data will only be processed once we have obtained appropriate consent. For further information in relation to this, please see our Biometrics Policy.

AUTOMATED DECISION MAKING

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. The School are allowed to use automated decision making in limited circumstances.

Students will not be subject to automated decision-making, unless the School has a lawful basis for doing so and the School has notified you.

RETENTION PERIODS

Except as otherwise permitted or required by applicable law or regulation, the School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

Information about how we retain information can be found in our Data Retention policy.

SECURITY

The School has put in place measures to protect the security of your information i.e. against it being accidentally lost, used or accessed in an unauthorised way].

Youth Support Services

Students aged 13+

- Once our students reach the age of 13, the School also passes student information to our Local Authority and / or provider of Youth Support Services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

The School must provide the student's name, the parent's name[s] and any further information relevant to the support services role.

This enables them to provide services as follows:

- Youth Support Services
- Careers Advisers.

A parent or guardian can request that only their child's name, address and date of birth is passed to their Local Authority or provider of Youth Support Services by informing us. This right is transferred to the student once he/she reaches the age 16.

Students aged 16+

The School also share certain information about students aged 16+ with our Local Authority and / or provider of Youth Support Services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- Post-16 Education and Training Providers
- Youth Support Services
- Careers Advisers.

For more information about services for young people, please visit our Local Authority website https://www.hounslow.gov.uk/site/

THE NATIONAL STUDENT DATABASE

The NPD is owned and managed by the Department for Education and contains information about students in Schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including Schools, local authorities and awarding bodies.

The School is required by law, to provide information about our students to the DfE as part of statutory data collections such as the School Census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education [Information about Individual Students] [England] Regulations 2013.

To find out more about the NPD, go to:
https://www.gov.uk/government/publications/national-student-database-user-guide-and-supporting-information

The department may share information about our students from the NPD with third parties who promote the education or well-being of children in England by:

- Conducting research or analysis
- Producing statistics
- Providing information, advice or guidance.

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- Who is requesting the data
- The purpose for which it is required
- The level and sensitivity of data requested: and
- The arrangements in place to store and handle the data.

To be granted access to student information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided student information, [and for which project], please visit the following website: https://www.gov.uk/government/publications/national-student-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

REQUESTING ACCESS TO YOUR PERSONAL DATA

Under Data Protection Legislation, parents and students have the right to request access to information about them that the School holds. To request your personal information, please email the School on info@hestoncs.org.

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for the purposes of direct marketing
- Object to decisions being taken by automated means
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed
- Claim compensation for damages caused by a breach of the data protection regulations.

If you want to exercise any of the above rights, please contact the PA to the Headteacher in writing.

The School may need to request specific information from you to help us confirm your identity and ensure your right to access the information [or to exercise any of your other rights]. This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

RIGHT TO WITHDRAW CONSENT

In circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the PA to Headteacher. Once the School has received notification that you have withdrawn your consent, the School no longer processes your information for the purpose or purposes you originally agreed to, unless the School has another legitimate basis for doing so in law.

CONTACT

If you would like to discuss anything within this privacy notice or have a concern about the way the School is collecting or using your personal data, please raise your concerns with your child's Learning Coordinator in the first instance.

The School has appointed a Data Protection Officer [DPO] to oversee compliance with data protection and this privacy notice. If you have any questions about how the School handles your personal information which cannot be resolved by the School, then you can contact the DPO on the details below:

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Lead Contact: Craig Stilwell

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues at:
https://ico.org.uk/concerns

CHANGES TO THIS PRIVACY NOTICE

The School reserves the right to update this privacy notice at any time, and will provide you with a new privacy notice when the School makes any substantial updates. The School may also notify you in other ways from time to time about the processing of your personal information.

PRIVACY NOTICE FOR VISITORS AND CONTRACTORS

Heston Community School is committed to protecting the privacy and security of your personal information. This privacy notice describes how the School collects and uses personal information about you during and after your visit with us, in accordance with the UK General Data Protection Regulation [UK GDPR].

Following Brexit, Regulation [EU] 2016/679, General Data Protection Regulation [GDPR] is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.

It applies to all current and former visitors and contractors.

WHO COLLECTS THIS INFORMATION

Heston Community School is a 'Data Controller' This means that the School is responsible for deciding how the School hold and use personal information about you.

The School is required under data protection legislation to notify you of the information contained in this privacy notice. This notice does not form part of a contract to provide services and the School may update this notice at any time.

It is important that you read this notice, together with any other privacy notice the School may provide on specific occasions when the School is collecting or processing personal information about you, so that you are aware of how and why the School is using such information.

DATA PROTECTION PRINCIPLES

The School will comply with the data protection principles when gathering and using personal information, as set out in our Data Protection Policy.

THE CATEGORIES OF VISITOR INFORMATION THAT THE SCHOOL COLLECTS, PROCESSES, HOLDS AND SHARES

The School processes data relating to those visiting our School [including contractors]. Personal data that the School may collect, process, hold and share [where appropriate] about you includes, but not restricted to:

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses
- Criminal records information as required by law to enable you to work with children
- e.g. DBS checks
- Information relating to your visit, e.g. your company or organisations name, arrival and departure time, car number plate
- Information about any access arrangements you may need
- Photographs for identification purposes for the duration of your visit
- CCTV footage captured by the School.

We may also collect, store and use the following more sensitive types of personal information:

- Information about your race or ethnicity, religious or philosophical beliefs

- Information about your health, including any medical conditions.
- [Biometric data]

HOW THE SCHOOL COLLECTS THIS INFORMATION

The School may collect this information from you, the Home Office, the DBS, other professionals the School may engage [e.g. to advise us generally], our signing in system, automated monitoring of our websites and other technical systems such as our computer networks and connections, CCTV and access control systems, remote access systems, email and instant messaging systems, intranet and internet facilities.

HOW THE SCHOOL USES YOUR INFORMATION

The School will only use your personal information when the law allows us to. Most commonly, the School uses your information in the following circumstances:

- Where the School needs to perform the contract the School has entered into with you
- Where the School needs to comply with a legal obligation [such as health and safety legislation, under statutory codes of practice and employment protection legislation]
- Where it is needed in the public interest or for official purposes
- Where it is necessary for our legitimate interests [or those of a third party] and your interests, rights and freedoms do not override those interests
- When you have provided us with consent to process your personal data

The School needs all the categories of information in the list above primarily to allow us to perform our contract with you, with your consent and to enable us to comply with legal obligations. Please note that the School may process your information without your knowledge or consent, where this is require or permitted by law.

The situations in which the School processes your personal information are listed below:

- Ensure the safe and orderly running of the School
- To manage our workforce and those deployed on site
- Personnel management including retention
- In order to manage internal policy and procedure
- Complying with legal obligations
- Carry out necessary administration functions to allow visitors and contractors on site
- To monitor and manage access to our systems and facilities in order to protect our networks and for the purposes of safeguarding
- To monitor and protect the security of our network and information, including preventing unauthorised access to our computer network and communications systems and preventing malicious software distribution
- To answer questions from insurers in respect of any insurance policies which relate to you
- Health and safety obligations
- Prevention and detection of fraud or other criminal offences
- To defend the School in respect of any investigation or court proceedings and to comply with any court or tribunal order for disclosure

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.
The School will only use your personal information for the purposes for which the School collected it, unless the School reasonably considers that the School needs to use it for another reason and that reason is compatible with the original purpose. If the School needs to use your personal information for an unrelated purpose, the School notify you and will explain the legal basis which allows us to do so.

HOW THE SCHOOL USES PARTICULARLY SENSITIVE INFORMATION

Sensitive personal information [as defined under the UK GDPR as 'Special Category Data'] require higher levels of protection and further justification for collecting, storing and using this type of personal information. The School may process this data in the following circumstances:

- In limited circumstances, with your explicit written consent
- Where the School needs to carry out our legal obligations in line with our Data Protection Policy
- Where it is needed in the public interest, such as for equal opportunities monitoring
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards. Less commonly, the School may process this type of information where it is needed in relation to legal claims or where it is necessary to protect your interests [or someone else's interests] and you are not capable of giving your consent

CRIMINAL CONVICTIONS

The School may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. The School will only collect information about criminal convictions if it is appropriate given the nature of the role and where the School is legally able to do so.

SHARING DATA

The School may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where the School has another legitimate interest in doing so. These include the following:

- The Department for Education [DfE]
- Ofsted
- Law enforcement officials such as police, HMRC
- Local Authority Designated Officer
- Professional advisors such as lawyers and consultants
- Support services [including HR support, insurance, IT support, information security, pensions and payroll]
- The Local Authority
- DBS

Information will be provided to those agencies securely or anonymised where possible.

The recipient of the information will be bound by confidentiality obligations, the School requires them to respect the security of your data and to treat it in accordance with the law.

RETENTION PERIODS

Except as otherwise permitted or required by applicable law or regulation, the School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

To determine the appropriate retention period for personal data, the School considers the amount, nature, and sensitivity of personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for processing the personal data, whether the School can fulfil the purposes of processing by other means and any applicable legal requirements.

The School typically retains personal data for 6 years or for as long as the data is required subject to any exceptional circumstances or to comply with laws or regulations that require a specific retention period.

SECURITY

The School has put in place measures to protect the security of your information i.e. against it being accidentally lost, used or accessed in an unauthorised way]. In addition, the School limits access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

Third parties will only process your personal information on our instructions and where they have agreed to treat information confidentially and to keep it secure.

The School has put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where the School is legally required to do so.

Automated Decision Making
Automated Decision-Making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision making in limited circumstances.
Visitors/contractors will not be subject to automated decision-making, unless we have a lawful basis for doing so and we have notified you.

Biometric Data
At [name of school] we would like to use your information as part of an automated [i.e., electronically operated] recognition system. This is for the purposes of [specify what purpose is – e.g., catering, library access]. The information that we wish to use is referred to as 'biometric information'. This data will only be processed once we have obtained appropriate consent. For further information in relation to this, please see our Biometrics policy.

YOUR RIGHTS OF ACCESS, CORRECTION, ERASURE AND RESTRICTION

It is important that the personal information the School holds about you is accurate and current. Please keep us informed if your personal information changes during your relationship with us.

Under certain circumstances by law you have the right to:

- Access your personal information [commonly known as a 'Subject Access Request']. This allows you to receive a copy of the personal information the School holds about you and to check the School is lawfully processing it. You will not have to pay a fee to access your personal information. However, the School may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, the School may refuse to comply with the request in such circumstances
- Correction of the personal information the School holds about you. This enables you to have any inaccurate information the School holds about you corrected

- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it
- To object to processing in certain circumstances [for example for direct marketing purposes]
- To transfer your personal information to another party

If you want to exercise any of the above rights, please contact the PA to the Headteacher in writing.

The School may need to request specific information from you to help us confirm your identity and ensure your right to access the information [or to exercise any of your other rights]. This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the PA to the Headteacher. Once the School has received notification that you have withdrawn your consent, the School no longer processes your information for the purpose or purposes you originally agreed to, unless the School has another legitimate basis for doing so in law.

HOW TO RAISE A CONCERN

The School hopes that the PA to the Headteacher can resolve any query you raise about our use of your information in the first instance.

The School has appointed a Data Protection Officer [DPO] to oversee compliance with data protection and this privacy notice. If you have any questions about how the School handles your personal information which cannot be resolved by the PA to the Headteacher, then you can contact the DPO on the details below:

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Lead Contact: Craig Stilwell

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues.

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

ARTIFICIAL INTELLIGENCE POLICY FOR STUDENTS AND PARENTS

Background to the Policy

Although Data Protection law does not specifically define or discuss the guidelines for Artificial Intelligence ['AI'], the guidance from the Information Commissioner's Office and the UK government defines it as using non-human systems to imitate human intelligence. In this time of constant development and increased usage, there is a need to provide students and staff with an awareness of how AI will be used and monitored by the school and the guidelines for usage by students, especially if being used to complete school work.

Acceptable Student Usage of AI

The School permits student usage of AI in the following circumstances: ensuring it is consistent with government and exam board guidelines.

The School permits AI uses in the following circumstances:

a. As a research tool
b. Idea generation for projects
c. For use with student work with the above requirements fulfilled, and in line with JCQ and UCAS Regulations.

For examinations and coursework, AI must only be used when the conditions of the assessment permit its use.

Where AI is permitted, it must not be misused in accordance with this statement. Examples of AI misuse include, but are not limited to, the following:

- Copying or paraphrasing sections of AI-generated content so that the work is no longer the student's own
- Copying or paraphrasing whole responses of AI-generated content
- Using AI to complete parts of the assessment so that the work does not reflect the student's own work, analysis, evaluation or calculations
- Failing to acknowledge use of AI tools when they have been used as a source of information
- Incomplete or poor acknowledgement of AI tools
- Submitting work with intentionally incomplete or misleading references.

Therefore, students must ensure that any information cited within schoolwork found using an AI system or software, must be referenced in the same way any other article or quotation would be, and in line with JCQ and Examination Board Regulations. The Joint Council for Qualifications have confirmed that students must show

Artificial Intelligence Staff Policy

We permit and encourage the informed and responsible use of generative AI applications by staff in carrying out identified business activities. Staff will comply with the terms of the workforce specific policy when using generative AI to carry out business activities.
We permit and encourage the informed and responsible use of authorised AI applications by staff, for the following business purposes:

(a) Drafting internal guidance, training and presentations
(b) Lesson planning
(c) Conducting research

(d) Developing code
(e) Providing summaries
(f) Idea generation
(g) Marking, in line with JCQ and Examination Board Regulations.

Where personal data is used with AI applications, an ICO risk assessment and/or data protection impact assessment ['DPIA'] has been carried out to ensure transparency in how AI will be used and what mitigating steps have been taken to reduce any potential risk of harm to students, staff and any other data subjects whose data might be shared with the authorised systems.

This Policy covers all employees, officers, consultants, contractors, volunteers, interns, casual workers and agency workers.

Authorised AI Applications

The school uses the following AI applications for business purposes;
Turnitin
Gradescope
OlexAI
Pupil Progress
Microsoft Copilot

The listed AI applications may be updated at any time.

Guidelines for Staff on Using Generative AI Tools and Platforms

You should not use generative AI tools other than in accordance with the list above, when sharing personal data. If you wish to use another generative AI tool, you should contact Data Protection Officer to ask whether the AI tool can be added to the list and/or whether you can be given authority to use it.

You must not share your access credentials or allow others to use generative AI tools on your behalf.

You must not use generative AI in any way that could be considered discriminatory or could give rise to defamation, harassment, intimidation or bullying or in any way that could harm the reputation of another.

You must not use generative AI to create illegal content or for illegal purposes.
You must not use offensive, obscene or abusive language, graphics or imagery when inputting content into generative AI and must not attempt to create content which is offensive, obscene or abusive through your use of generative AI tools.

Unless specifically authorised to do so, you must not input into a publicly-accessible generative AI tool:

- The School's trademarks, brands, logos or any other identifying material
- The School's name, email or other contact details [other than where required to input your work email address
- Propriety school information
- School materials or data
- Trade secret, confidential or valuable information
- Usernames, passwords [other than for the AI tool itself] and security tokens

- Personal data, i.e., information or data from which any living individual can be identified—including personal data relating to employees, parents, students, governors, suppliers and unconnected third parties.

When using generative AI in the workplace, you must always use your company email address to create and log in to any generative AI account [do not use your personal email address or login credentials].

You must protect your login credentials and ensure any generative AI accounts that you hold are not accessible to unauthorised third parties. The use of multi-factor authentication is advised in respect of any generative AI tools and technologies used.]

Personal Use of Generative AI

You must not use the company's computers, networks or systems [including via smartphones or tablets] to access generative AI tools for personal use at any time.

Any unauthorised use of generative AI is strictly prohibited. Permission to use the company's systems to access generative AI tools for personal use may be withdrawn at any time at the company's discretion.

Monitoring

We reserve the right to monitor all content on any AI applications used for business purposes. This will only be carried out by the school to comply with a legal obligation or for our legitimate business purposes, in order to:

(a) prevent misuse of the content and protect confidential information [and the confidential information of our students, staff or other stakeholders]
(b) ensure compliance with our rules, standards of conduct and policies in force
(c) ensure that staff do not use AI for any unlawful purposes or activities
(d) comply with legislation for the protection of intellectual property rights.

Breach of this Policy

Breach of this Policy may, where appropriate, result in disciplinary action up to and including dismissal or termination of your employment or engagement with us.

Where disciplinary action is appropriate, it may be taken whether the breach is committed during or outside normal hours of work and whether or not use of AI is on an individual's own device or one of our devices, and whether at home, in the office or from a remote working location.

You are required to assist with any investigation into a suspected breach of this policy. This may involve providing us with access to AI applications and any relevant passwords and login details.

You must report any breach of this policy immediately to the Data Protection Officer.