Heston
COMMUNITY
SCHOOL

GENERAL DATA PROTECTION REGULATION POLICY

Date reviewed: May 2018
Next review: May 2019

This Policy is founded within the School's ethos which provides a caring, friendly and safe environment for all members of our community.

CONTENTS

DATA PROTECTION POLICY

INTRODUCTION

The General Data Protection Regulation [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 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.

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.

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 adheres to the principles relating to the processing of personal data as set out in the GDPR.

The Principles the School must adhere to are:

1. Personal data must be processed lawfully, fairly and in a transparent manner
2. Personal data must be collected only for specified, explicit and legitimate purposes
3. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
4. Personal data must be accurate and, where necessary, kept up to date
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
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

Further details on each of the above principles is 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 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 in necessary for archiving, statistical or research purposes

The School will identify and document 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 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 required, 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 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 shall 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 also 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 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.

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. These include if the third party:

- 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 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 shall 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 GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the 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 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.

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 will handle 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 hold
(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.

Subject Access Requests

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

Any Data Subject who wishes to obtain the above information must notify the School in writing of his or her request. This is known as a Data Subject Access Request.

The request should in the first instance be sent to the PA to the Headteacher.

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
- 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 GDPR principles.

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

Data Protection Officer [DPO]

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

Data Protection Officer: Craig Stilwell
Address: Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Telephone: 0203 326 9174

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 GDPR or if you have any concerns that this policy is not being or has not been followed. 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 Retention 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
(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 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 [who 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 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 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.

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 GDPR.

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

Privacy by Design

The School has adopted a privacy by design approach to data protection to ensure that the School adhere 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 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 stored
- 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
- Security Policy

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

The School's 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 BREACH POLICY

The General Data Protection Regulation [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 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 possess 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 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: Craig Stilwell
Address: Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Telephone: 0203 326 9174

SECURITY AND DATA-RELATED POLICIES

Staff should refer to the following policies that are related to this data protection policy: - 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 GDPR about how they process personal data.

These policies are also designed to protect personal data and can be found at GDPR tab on the School website.

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 SIMS and Data Manager
- Email the completed form to voneil@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 their Line Manager or the DPO.

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. SIMS and Data Manager will acknowledge receipt of the data breach report form 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, 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
- Notify data subjects affected by the breach
- Notify other appropriate parties to the breach
- Take steps to prevent future breaches

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. If the School is 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 intended] 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].

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 don't 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

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

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 General Data Protection Regulation [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 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; and
- Name of the authorising officer.

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.

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.

RETENTION SCHEDULE

FILE DESCRIPTION	RETENTION PERIOD	RESPONSIBILITY
Employment Records		
Job applications and interview records of unsuccessful candidates	Six 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 Officer
Job applications and interview records of successful candidates	7 years after employment ceases	HR Officer
Written particulars of employment, contracts of employment and changes to terms and conditions	7 years after employment ceases	HR Officer
Right to work documentation including identification documents	7 years after employment ceases	HR Officer
Immigration checks	7 years after the termination of employment	HR Officer
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 Officer
Change of personal details notifications	No longer than 6 months after receiving this notification	HR Officer
Emergency contact details	Destroyed on termination	HR Officer
Personnel and training records	While employment continues and up to seven years after employment ceases	HR Officer
Annual leave records	Seven years after the end of tax year they relate to or possibly longer if leave can be carried over from year to year	HR Officer
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 Officer
Working Time Regulations: • Opt out forms • Records of compliance with WTR	• Two years from the date on which they were entered into • Two years after the relevant period	HR Officer
Disciplinary and training records	7 years after employment ceases	HR Officer

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.	Designate Safeguarding Lead and HR Officer
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	No longer than necessary	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
Professional Development Plans	3 years from the life of the plan	Academy Business Manager
Visitors Book and Signing In Sheets	3 years	PA to Headteacher
Newsletters and circulars to staff, parents and students	3 year	PA to Headteacher
Health and Safety Records		
Health and Safety consultations	Permanently	Site and Premises Manager
Health and Safety Risk Assessments	3 years from the life of the risk assessment	Site and Premises Manager
Any reportable accident, death or injury in connection with work	For at least twelve years from the date the report was made	Site and Premises Manager
Accident reporting	Adults – 6 years from the date of the incident Children – when the child attains 25 years of age.	Site and Premises Manager
Fire precaution log books	6 years	Site and Premises Manager
Medical records and details of: - • control of lead at work	40 years from the date of the last entry made in the record	Site and Premises Manager

• employees exposed to asbestos dust • records specified by the Control of Substances Hazardous to Health Regulations [COSHH]		
Records of tests and examinations of control systems and protection equipment under COSHH	5 years from the date on which the record was made	Site and Premises Manager
Temporary and Casual Workers		
Records relating to hours worked and payments made to workers	7 years	Finance Manager
Student Records		
Admissions records	1 year from the date of admission	Student Services Manager
Admissions register	3 years from the date of entry	Student Services Manager
School Meals Registers	3 years	Student Services Manager
Free School Meals Registers	6 years	Student Services Manager
Attendance Registers	3 years from the date of entry	Student Services Manager
Student Record	7 years or until the child turns 25	Office Manager
Special Educational Needs files, reviews and individual education plans [this includes any statement and all advice and information shared regarding educational needs]	Until the child turns 25.	SENCo
Emails	No more than three years	All

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 the School 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 General Data Protection Regulation [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 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.

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 Network 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 Network 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 Network 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 Network 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 Network 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 the School's systems without the prior approval of the Network Manager or Senior Leadership Team. This includes, but is not limited to, any PDA or telephone, iPad [or other mobile device tablet], USB device, iPod, 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 Network 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 [incidental/occasional/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, 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.

E-mail 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 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 Line Manager who will usually seek to resolve the matter informally. You should refer to the School 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. [Further information is contained in the School's Equal Opportunities and Diversity Policy, Anti-Harassment and Bullying Policy and Grievance Policy and 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 or sponsorship
- 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

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 Network 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 The School's Core Values and excellence in the educational sector. All members of staff are encaged 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 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 Network Manager who will liaise with the Senior Leadership Team as appropriate and necessary.

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.

The School's 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 reserves the right to withdraw its 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, 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 The School Disciplinary Policy and Procedure. 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

Access is granted to the web, telephones and to other electronic systems, for legitimate work purposes only.

Misuse or abuse of The School 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]:

1. Accessing pornographic material [that is writings, pictures, films, video clips of a sexually explicit or arousing nature], racist or other inappropriate or unlawful materials
2. Transmitting a false and/or defamatory statement about any person or organisation
3. Sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others
4. Transmitting confidential information about the School and any of its staff, students or associated third parties
5. Transmitting any other statement which is likely to create any liability [whether criminal or civil, and whether for the employee or for the School
6. Downloading or disseminating material in breach of copyright
7. Copying, downloading, storing or running any software without the express prior authorisation of the Network Manager
8. Engaging in on line chat rooms, instant messaging, social networking sites and on line gambling
9. Forwarding electronic chain letters and other materials
10. 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 The School's 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

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.

Public Authorities should be clear and proactive about the information they will make public. For this reason, a publication scheme is available on the School website www.hestoncommunityschool.co.uk.

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 Acceptable Usage Protocols and Data Protection Policy.

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]*** 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, and 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 enquirers name and 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 require 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 do 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. There is a time limit of 20 working days excluding school holidays for responding to the request.

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
- 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 with them they hold it, then 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
- 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. This, however, does not provide an excuse for bad records management.

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

FEES

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 with staff costs calculated at a fixed rate of £25 per hour [therefore 18 hours' work is required before the threshold is reached].

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 costs].

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 is going to charge they will send the enquirer a fees notice. The School do 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 working days [excluding school holidays]. Failure to comply could result in a complaint by the requester to the Information Commissioner. The response time starts from the time the request is received.

Where the School has asked the enquirer for more information to enable it to answer, the 20 working 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 need more time to consider the public interest test, the School will reply in 20 working 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
- 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 very 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 is:

- 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.

COMPLAINTS/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

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 the School's compliance with the School's legal obligations.

To minimise these risks, avoid loss of productivity and to ensure that the School's 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 the School's 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, 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 the School's 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 Governing Body 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 Network 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 Network Manager on itsupport@hestoncs.org.

COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS

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

1. Breach the School's Electronic Information And Communications Systems Policy
2. Breach the School's obligations with respect to the rules of relevant regulatory bodies
3. Breach any obligations they may have relating to confidentiality
4. Breach our Disciplinary Policy
5. Defame or disparage the School, its Staff, its students or parents, its affiliates, partners, suppliers, vendors or other stakeholders
6. Harass or bully other staff in any way or breach our Bullying Policy
7. Unlawfully discriminate against other staff or third parties or breach our Equal Opportunities Policy
8. Breach the School's Data Protection Policy [for example, never disclose personal information about a colleague online]

9. 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. 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 the School's 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 Trust [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 the School's 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 the School's electronic information and communications systems.

The School reserves the right to monitor, intercept and review, without further notice, staff activities using the School's IT resources and communications systems, including but not limited to social media postings and activities, to ensure that the School's 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 the School's 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/carers and the Network Manager will have overall responsibility for this. Should you wish for any reminders to be issued you should contact the Network Manager by email to ensure that any post can be issued.
5. The proposed post must be presented to your Line Manager for confirmation that the post can 'go live' before it is posted on any social media site.
6. The Network Manager will post the information, but all staff have responsibility to ensure that the Social Media Policy has been adhered to.

PROTECTING THE SCHOOL'S BUSINESS REPUTATION

Staff must not post disparaging or defamatory statements about:

1 The School
2 Current, past or prospective Staff as defined in this policy
3 Current, past or prospective students
4 Parents, carers or families of [3]
5 The School's suppliers and services providers
6 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/her Line Manager.

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 the School's 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 Network Manager, together with the Headteacher shall be responsible for reviewing this policy from time to time to ensure that it meets legal requirements and reflects best practice. The Governing Body 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 Network Manager in the first instance.

PRIVACY NOTICE FOR HESTON COMMUNITY SCHOOL

Heston Community School is committed to protecting the privacy and security of your personal information. This privacy notice describes how the School collect and use personal information about you during and after your work relationship with us, in accordance with the General Data Protection Regulation [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 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 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 will comply with the data protection principles when gathering and using personal information, as set out in the School's data protection policy.

THE CATEGORIES OF INFORMATION THAT WE COLLECT, PROCESS, HOLD AND SHARE

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 retain 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 the School's 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 give to others

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 engage, 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 the School's 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 will use your information in the following circumstances:

- Where the School need to perform the contract the School has entered into with you
- Where the School need 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 the School's legitimate interests [or those of a third party] and your interests, rights and freedoms do not override those interests

The School need all the categories of information in the list above primarily to allow us to perform the School's 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 will process 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 the School's systems and facilities in order to protect the School's networks, the personal data of the School's employees and for the purposes of safeguarding
- To monitor and protect the security of the School's network and information, including preventing unauthorised access to the School's 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 the School's 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 the School's legal obligations [such as to ensure the health and safety of the School's 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 need to use it for another reason and that reason is compatible with the original purpose. If the School need to use your personal information for an unrelated purpose, the School will notify you and the School 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 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 need to carry out the School's legal obligations in line with the School's data protection policy
- Where it is needed in the public interest, such as for equal opportunities monitoring [or in relation to the School's 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 will use 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 the School's 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 will collect 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
- Prospective Employers
- Welfare services [such as social services]
- Law enforcement officials such as police, HMRC
- LA Designated Officer
- 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

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 require 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 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 the School's 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 has put in place measures to limit 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 the School's 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 hold 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 hold 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 hold about you. This enables you to have any inaccurate information the School hold 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

Your Line Manager can resolve any query you raise about the School's 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 resolve by the HR Officer, then you can contact the DPO on the details below:

Data Controller Name: Craig Stilwell

Data Controller Details:
Judicium Consulting Ltd
72 Cannon Street
London,
EC4N 6AE
Data Controller Email: dataservices@judicium.com

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

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

General Data Protection Regulations [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 [CTRL+ALT+DEL -> lock computer].
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.
3. **Secure Your Documents, Planners and Mobile Devices**
   - Encrypt/password protect documents where possible.
   - Limit access to shared drives which 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.
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 Network Manager if unsure.
   - Do not connect devices, for example, mobile phones, directly to Heston School's PCs.
   - USBs, portable storage drives and mobile storage devices will no longer be permissible from the end of June 2018.
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.
   - Ensure machines have anti-virus software that is updated regularly.
   - Do not download any un-authorised software without permission from the Network 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**
   - Send confidential information by encrypted email by adding the word 'Confidential' in to the email title or body.
   - 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 Data Retention Schedule.
    - Keep file back-ups in case of data loss.

GUIDANCE DATA SHARING AGREEMENT [INDIVIDUALS AND SMALL ORGANISATIOINS]

This wording is for Schools to send smaller third party organisations [for example those organisations who have one/two employees working for it, such as sports coaches, photographers]. This wording is given to summarise responsibilities of those organisations/individuals with complying with data protection when it would not be suitable/they would be unwilling 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 we are sharing, who with and reasons why].

Do 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.

It will be the responsibility of the Curriculum Areas or support staff to ensure that this agreement has been completed prior to any personal information of students or staff being shared with external organisations or individuals.

Please forward a copy of this agreement to the SIMS and Data Manager in order to monitor our internal processing activities.

For larger scale projects, where considerable data will be shared or given access to by a third party software provider, please see the SIMS and Data Manager prior to any agreement being placed with the provider.

Guidance Data Sharing Agreement [Individuals and Small Organisations]

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 eg staff, parents, students]: -

- To comply with the data protection principles and laws in force in connection with the processing of personal data;
- You shall 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. This must be notified to the SIMS and Data Manager at Heston Community School by email at info@hestoncs.org **and** by telephone at 0208 572 1931;
- 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 shall 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] shall provide the School with any information and assistance required in order to comply with data protection laws. This includes 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.

It will be the responsibility of the Curriculum Areas or support staff to ensure that this agreement has been completed prior to any personal information of students or staff being shared with external organisations or individuals.

Please forward a copy of this agreement to the SIMS and Data Manager in order to monitor our internal processing activities.

Printed Name: _____

Position Held: _____

Name of Organisation: _____

Date: _____

Signature: _____