Heston
COMMUNITY
SCHOOL

E-SAFETY POLICY

Updated: July 2015
Next Review: July 2018

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

Contents

6 Search and Confiscation guidance from DfE https://www.gov.uk/government/publications/searching-screening-and-confiscation

1.0 Introduction and Overview

1.1 Rationale

The purpose of this Policy is to:

- Set out the key principles expected of all members of the school community at Heston Community School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Heston Community School
- Assist School Staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other School Policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games [exposure to violence associated with often racist language], substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: How to check authenticity and accuracy of online content

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft [including 'frape' - hacking Facebook profiles] and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being [amount of time spent online - Internet or gaming]

- Sexting [sending and receiving of personally intimate images] also referred to as SGII [Self-Generated Indecent Images]
- Copyright [little care or consideration for intellectual property and ownership – such as music and film]

[Reference: Ofsted 2013]

1.2 Scope

This Policy applies to all members of Heston Community School's community [including staff, students, volunteers, parents/carers, visitors and community users] who have access to and are users of School ICT systems, both in and out of School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the School/Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this Policy, which may take place outside of the School but is linked to membership of the School. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data [see Appendices]. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The School will deal with such incidents within this Policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

1.3 Roles and Responsibilities

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security [SIRO] • To ensure the School uses an approved, filtered Internet Service, which complies with current statutory requirements, e.g. LGfL • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident • To receive regular monitoring reports from the E-Safety Officer • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures [eg Network Manager]

Role	Key Responsibilities
E-Safety Coordinator/ Designated Child Protection Lead	• To take day to day responsibility for e-safety issues and a leading role in establishing and reviewing the School E-Safety Policies/Documents • To promote an awareness and commitment to e-safeguarding throughout the school community • To ensure that e-safety education is embedded across the curriculum • To liaise with School's ICT technical staff • To communicate regularly with SALT and the designated E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • To ensure that an e-safety incident log is kept up to date • To facilitate training and advice for all staff • To liaise with the Local Authority and relevant agencies • To be regularly updated in e-safety issues and legislation and be aware of the potential for serious child protection issues to arise from: - Sharing of personal data - Access to illegal/inappropriate materials - Inappropriate on-line contact with adults/ strangers - Potential or actual incidents of grooming · Cyber-bullying and use of social media
Governors/ E-Safety Governor	• To ensure that the School follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the Policy. The Governors' Sub-Committee receiving regular information about e-safety incidents and monitoring reports will carry this out. A member of the Governing Body has taken on the role of E-Safety Governor • To support the School in encouraging parents/carers and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include: - Regular review with the E-Safety Officer [including e-safety incident logs, filtering/ change control logs]
Curriculum Leader Business Education and ICT	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise regularly with the E-safety Coordinator

Role	Key Responsibilities
Network Manager	• To report any e-safety related issues that arise, to the E-Safety Coordinator • To ensure that users may only access the School's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack [e.g. keeping virus protection up to date] • To ensure the security of the School's ICT system • To ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices • To ensure the School's Policy on web filtering is applied and updated on a regular basis • To ensure LGfL is informed of issues relating to the filtering applied by the Grid • To ensure that s/he keeps up to date with the School's E-Safety Policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • To ensure that the use of the Network, Virtual Learning Environment [Learning Platform] remote access and email is regularly monitored in order that any misuse or attempted misuse may be reported to the E-Safety Co-ordinator and Headteacher for investigation, action or sanction, as appropriate • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the School's e-security and technical procedures
Data Officer	• To ensure that all data held on students on the Learning Platform and School Administration machines have appropriate access controls in place
LGfL Nominated contact[s]	• To ensure all LGfL services are managed on behalf of the School, including maintaining the LGfL USO database of access accounts
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide students carefully when engaged in learning activities involving online technology [including, extra-curricular and extended school activities, where relevant] • To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

Role	Key Responsibilities
All Staff	• To read, understand and help promote the School's E-Safety policies and guidance • To read, understand, sign and adhere to the School Staff Acceptable Use Agreement and Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current School Policies with regard to these devices • To report any suspected misuse or problem to the E-Safety Coordinator • To maintain an awareness of current e-safety issues and guidance, eg through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with students is on a professional level and only through school based systems and never through personal mechanisms, e.g. email, text, mobile 'phones etc.
Students	• To read, understand, sign and adhere to the Student Acceptable Use Agreement • To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand School Policy on the use of mobile 'phones, digital cameras and handheld devices. • To know and understand School Policy on the taking and use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the School's E-Safety Policy covers students' actions out of school, if related to their membership of the School • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • To help the School in the creation and review of E-Safety Policies

Role	Key Responsibilities
Parents/Carers	• To support the School in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the students' use of the Internet and the School's use of photographic and video images • To read, understand and promote the School's Student Acceptable Use Agreement with their children • To access the School Website, Learning Platform, on-line student records in accordance with the relevant School Acceptable Use Agreement • To consult with the School if they have any concerns about their children's use of technology
External Groups	• Any external individual or organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within the School

1.4 Communication

The Policy will be communicated to staff, students and the community in the following ways:

- Policy to be posted on the School Website
- Policy to be part of School Induction Pack for new staff
- Acceptable Use Agreements discussed with students at the start of each Academic Year
- Acceptable Use Agreements to be issued to whole school community, usually on entry to the School
- Acceptable Use Agreements to be held in Student and Personnel Files

1.5 Complaints

- The School will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The School cannot accept liability for material accessed or any consequences of Internet access.
- Staff and students are given information about infringements in use and possible sanctions. Sanctions available include:
  - Interview and/or counselling by Tutor
  - Interview with Learning Coordinator and E-Safety
  - Interview to inform parents/carers
  - Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework]
  - Referral to Police

- The School's E-Safety Coordinator will act as first point of contact for any complaint. Any complaint about staff misuse will be referred to the Headteacher for information.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to Child Protection are dealt with in accordance with the School's Child Protection procedures.

1.6 Review and Monitoring

The E-Safety Policy may be referenced from within other School Policies and Documentation [eg Child Protection Policy, Anti-Bullying Policy, the School Development Plan and the Behaviour Policy].

The School has an E-Safety Coordinator who will be responsible for document ownership, review and updates.

The E-Safety Policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the School.

At the time of writing, the E-Safety Policy is current and appropriate for its intended audience and purpose.

Widespread ownership of the Policy will be developed and it has been agreed by the SALT and will be approved by Governors. All amendments to the Policy will be discussed in detail with all members of staff.

2.0 Education and Curriculum

2.1 Student E-Safety Curriculum

Heston Community School:

- Has a clear, progressive E-Safety Education Programme as part of the Computer Science and ICT and PSHE curricula. It is built on the LGfL e-safeguarding and e-literacy framework and national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - To STOP and THINK before they CLICK
    - To develop a range of strategies to evaluate and verify information before accepting its accuracy
    - To be aware that the author of a web site and/or page may have a particular bias or purpose and to develop skills to recognise what that may be
    - To know how to narrow down or refine a search
    - To understand how search engines work and to understand that this affects the results they see at the top of the listings
    - To understand acceptable behaviour when using an online environment and email, ie be polite, no bad or abusive language or other inappropriate behaviour and keeping personal information private
    - To understand how photographs can be manipulated and how web content can attract the wrong sort of attention
    - To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
    - To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
    - To understand why they must not post pictures or videos of others without their permission
    - To know not to download any files [such as music files] without permission
    - To have strategies for dealing with receipt of inappropriate materials
    - To understand why and how some people will 'groom' young people for sexual reasons
    - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying
    - To know how to report any abuse including cyberbullying and how to seek help if they experience problems when using the Internet and related technologies, ie parent/carer, teacher or trusted staff member or an organisation such as ChildLine or the CLICK CEOP button.
- Plans internet use carefully to ensure that it is age appropriate and supports the learning objectives for specific Curriculum Areas.

- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign and will be displayed when a student logs on to the School Network.
- Ensures staff model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and students understand issues around plagiarism, how to check copyright and also know that they must respect and acknowledge copyright and intellectual property rights
- Ensures that staff and students understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include, risks in pop-ups, buying on-line, on-line gaming and gambling.

2.2 Staff and Governor Training

Heston Community School:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection
- Makes regular training available to staff on e-safety issues and the School's E-Safety Education Programme annually with updates as appropriate
- As part of the Induction Process, provides all new staff [including those on university/college placement and work experience] with information and guidance on the E-Safeguarding Policy and the School's Acceptable Use Policies and Agreements.

2.3 Parent/Carer Awareness and Training

Heston Community School:

- Runs a rolling programme of advice, guidance and training for parents/carers, including:
  - Introduction of the Acceptable Use Agreements to new parents/carers to ensure that principles of e-safe behaviour are made clear
  - Information leaflet and information in School Newsletters and on the School Website
  - Demonstrations, practical sessions held at school
  - Suggestions for safe Internet use at home
  - Provision of information about national support sites for parents/carers.

3.0 Expected Conduct and Incident Management

3.1 Expected Conduct

At Heston Community School, all users:

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy and Agreement which they will be expected to sign before being given access to school systems.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the School's E-Safety Policy covers their actions out of school, if related to their membership of the School.
- Will be expected to know and understand School Policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand School Policies on the taking and use of images and on cyber-bullying.

Staff

- Are responsible for reading the School's E-Safety Policy and using the School's ICT systems accordingly, including the use of mobile 'phones and handheld devices.

Students

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers

- Should provide consent for students to use the Internet, as well as other technologies, as part of the E-Safety Acceptable Use Agreement Form at time of their child's entry to the School.
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

3.2 Incident Management

At Heston Community School:

- There is strict monitoring and application of the E-Safety Policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
- All members and the School's wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the School's escalation processes.

- Support is actively sought from other agencies as needed [eg LGfL, and the UK Safer Internet Centre helpline] in dealing with e-safety issues.
- Monitoring and reporting of e-safety incidents take place and contribute to developments in policy and practice in e-safety within the School. The records are reviewed and reported to the School's senior leaders and Governors.
- Parents/Carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- The Police will contacted the Police if staff or students receive online communication that is considered to be particularly disturbing or breaks the law.

4.0 Managing the IT Infrastructure

4.1 Internet Access, Security [Virus Protection] and Filtering

Heston Community School:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network
- Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the Filtering Policy is logged and only available to staff with the approved 'web filtering management' status
- Uses USO user-level filtering, where relevant, thereby closing down or opening up options appropriate to the age and stage of the students
- Ensures network healthy through use of Sophos anti-virus software [from LGfL] etc. and network set-up so staff and students cannot download executable files
- Uses DfE and LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site
- Blocks all Chat Rooms and Social Networking Sites except those that are part of an Educational Network or approved Learning Platform
- Only unblocks other external social networking sites for specific purposes or Internet Literacy lessons
- Has blocked student access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network
- Uses security time-outs on internet access where practicable and useful

- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students
- Is vigilant in its supervision of students' use at all times, as far as is reasonable and uses common-sense strategies in learning resource areas where older pupils have more flexible access
- Ensures all staff and students have signed an Acceptable Use Agreement Form and understands that they must report any concerns
- Ensures students only publish within an appropriately secure environment: the School's Learning Environment, the London Learning Platform or LGfL secure platforms such as J2Bloggy, etc
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the School's Learning Platform as a key way to direct students to age and subject appropriate web sites
- Requires staff to plan the curriculum context for internet use to match students' ability, using child-friendly search engines where more open internet searching is required, eg yahoo for kids or ask for kids , Google Safe Search etc.
- Is vigilant when conducting 'raw' image search with students, eg Google image search
- Informs all users that internet use is monitored
- Informs staff and students that that they must report any failure of the filtering systems directly to their Teacher or Network Manager. The System Administrator logs or escalates, as appropriate, to the Technical Service Provider or LGfL Helpdesk
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through Staff Meetings and Teaching Programmes
- Provides advice and information on reporting offensive materials, abuse, bullying etc available for students, staff and parents/carers
- Immediately refers any material it suspects is illegal to the appropriate authorities, eg the Police and the LA.

4.2 Network Management [User Access and Backup]

Heston Community School:

- Uses individual, audited log-ins for all users, the London USO system and RM Unify
- Uses guest accounts occasionally for external or short-term visitors to gain temporary access to appropriate services
- Uses teacher 'remote' management control tools for controlling workstations, viewing users and setting up applications and internet web sites, where useful
- Has additional local network auditing software installed

- Ensures the Network Manager is up to date with LGfL services and policies
- Ensures that storage of all data within the School will conform to the UK data protection requirements
- Ensures that students and staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this School:

- Ensures staff read and sign that they have understood the School's E-safety Policy. Following this, they are set-up with internet, e-mail and network access. Online access to services is through a unique, audited username and password.
- Ensures that staff access to the School's Management Information System is controlled through SCOMIS.
- Provides students with an individual network log in username. From Year 7 students are also expected to use a personal password.
- Provides all students with their own unique username and password which gives them access to the Internet, the Learning Platform and their own school approved email account.
- Uses the London Grid for Learning's Unified Sign-On [USO] system and RM Unify for username and passwords.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.
- Has set up the network with a shared work area for students and one for staff. Staff and students are shown how to save work and access work from these areas.
- Requires all users to always log off when they have finished working or are leaving the computer unattended.
- Where a user finds a logged on machine, requires them to always log off and then log on again as themselves. [Users needing access to secure data are timed out after 10 minutes and have to re-enter their username and password to re-enter the network.]
- Requests that Staff and Students do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. Staff and Students are requested that they DO switch off the computers at the end of the day and computers automatically switch off at 18:00 to save energy.
- Has set up the network so that users cannot download executable files/programmes
- Has blocked access to music/media download and shopping sites, except those approved for educational purposes
- Scans all mobile equipment with anti-virus/spyware before it is connected to the network

- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the School provides them with a solution to do so
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the School is used solely to support their professional responsibilities and that they notify the school of any 'significant personal use' as defined by HM Revenue & Customs.
- *Makes clear that staff accessing LA systems do so in accordance with any Corporate policies, eg Borough email or Intranet, finance systems, Personnel systems etc.*
- Maintains equipment to ensure Health and Safety is followed, eg projector filters cleaned by the Network Manager, equipment installed and checked by approved Suppliers and/or electrical engineers
- Has integrated curriculum and administration networks but access to the Management Information System is set up so as to ensure staff users can only access modules related to their role, eg teachers access the Data Harvest module and only the SENCO may access certain SEN data.
- Ensures that access to the School's network resources from remote locations by staff is restricted and access is only through School approved systems, e.g. staff may access their area, the staff shared area for planning documentation
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems, e.g. technical support or MIS Support, Education Welfare Officers accessing attendance data on specific children, parents/carers using a secure portal to access information on their child.
- Provides students and staff with access to content and resources through the approved Learning Platform which staff and students access using their username and password [their USO username and password].
- Makes clear responsibilities for the daily back up of MIS and Finance Systems and other important files.
- Has a clear Disaster Recovery System in place for critical data that includes a secure, remote back up of critical data that complies with External Audit requirements.
- Uses the broadband network for the CCTV system and has had set up by approved partners.
- Uses the DfE secure s2s website for all CTF files sent to other schools.
- Ensures that all student level data or personal data sent over the internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange [USO FX].

- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network.
- Ensures that the wireless network has been secured to industry standard Enterprise security level and appropriate standards suitable for educational use.
- Ensures that all computer equipment is installed professionally and meets health and safety standards.
- Ensures IT equipment is maintained so that the quality of presentation remains high.
- Reviews the school IT systems regularly with regard to health and safety and security.

4.3 Password Policy

- This School makes it clear that staff and students must always keep their password private and must not share it with others or leave it where others can find it.
- All staff and students have their own unique username and private passwords to access school systems. Staff and students are responsible for keeping their password private.
- The School requires staff and students to use strong access passwords.
- The School requires staff to change their passwords every 90 days.

4.4 E-Mail

General

Heston Community School:

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account.
- Does not publish personal e-mail addresses of students or staff on the School Website. The School may use anonymous or group e-mail addresses, for example, info@hestoncs.org for communication with the wider public.
- Will contact the Police if staff or students receive an e-mail that is considered to be particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date.
- Reports messages relating to or in support of illegal activities to the relevant Authority and, if necessary, to the Police.
- Knows that spam, phishing and virus attachments can make emails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the School, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our Internet access to the Worldwide Web.

Students

Heston Community School:

- Provides students with an email account for their educational and study purposes and makes clear personal email should be through a separate account.
- Students are introduced to, and use e-mail as part of the ICT/ Computing Scheme of Work.
- Pupils can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this.
- Students are taught about the safety and 'netiquette' of using e-mail both in school and at home, i.e. they are taught:
  - Not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer
  - That an e-mail is a form of publishing where the message should be clear, short and concise
  - That any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
  - They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.
  - To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe
  - That they should think carefully before sending any attachments
  - Embedding adverts is not allowed
  - That they must immediately tell a teacher or responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature
  - Not to respond to malicious or threatening messages
  - Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying
  - Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them
  - That forwarding 'chain' e-mail letters are not permitted.
- Students sign the School User Agreement Form to say they have read and understood the e-safety rules, including e-mail and how any inappropriate use will be dealt with.

Staff

- Staff can only use the School's e-mail systems on the school system
- Staff may only use the School e-mail systems for professional purposes
- Access in school to external personal e-mail accounts may be blocked
- Staff may use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information.
- Never use email to transfer staff or student personal data. Use secure, LA/DfE approved system is used, e.g. S2S [for school to school transfer]. Collect; USO-FX.
- Staff know that e-mails sent to an external organisation must be written carefully [and may require authorisation], in the same way as

a letter written on School Headed paper. That it should follow the School's 'house-style':
  - The sending of multiple or large attachments should be limited and may also be restricted by the provider of the service being used
  - The sending of chain letters is not permitted
  - Embedding adverts is not allowed;
- All staff sign the School's User Agreement Form [AUP] to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

4.5 School Website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- Uploading of information is restricted to our website authorisers e.g. Marketing Manager
- The School Website complies with the statutory DfE guidelines for publications
- Most material is the School's own work. Where other's work is published or linked to, the School will credit the sources used and state clearly the author's identity or status
- The point of contact on the Website is the School Address, Telephone Number and we use a general email contact address, e.g. info@hestoncs.org. Home information or individual e-mail identities will not be published
- Photographs published on the website do not have full names attached
- The School does not use students' names when saving images in the file names or in the tags when publishing to the website
- The School does not use embedded geodata in respect of stored images
- The School expects staff using school approved blogs or wikis to password protect them and run from the School Website.

4.6 Virtual Learning Environment

- Uploading of information on the School's Learning Virtual Learning Environment [VLE] is shared between different staff members according to their responsibilities, e.g. all Class Teachers may upload information in their class areas
- Photographs and videos uploaded to the School's VLE will only be accessible by members of the school community
- In school, students are only able to upload and publish within school approved and closed systems, such as the VLE

4.7 Social Networking

- Teachers are instructed not to run Social Network spaces for student use on a personal basis or to open up their own spaces to their

students but to use the School's preferred system for such communications.

- The School's preferred system for social networking will be maintained in adherence with the Communications Policy.

School staff will ensure that in private use:

- No reference is made in social media to students, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the School Community
- Personal opinions should not be attributed to the School
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

4.8 Video Conferencing

Heston Community School:

- Only uses the LGfL/Janet supported services for video conferencing activity
- Only uses approved or checked webcam sites

4.9 CCTV

- The School has CCTV in operation as part of our site surveillance for staff and student safety. The School will not reveal any recordings [retained by the Support Provider for 28 days], without permission except where disclosed to the Police, as part of a criminal investigation.
- The School uses specialist lesson recording equipment [IRIS], on occasions, as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

5.0 Data Security: Management Information System access and Data Transfer

5.1 Strategic and Operational Practices

At this School:

- The Headteacher is the Senior Information Risk Officer [SIRO].
- Staff are clear who are the key contact[s] for key school information [the Information Asset Owners] are. The School will list the information and information asset owners in a spreadsheet which will be available to all staff.
- We ensure staff know to whom to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record in SIMS.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

  - Staff
  - Governors
  - Students
  - Parents/Carers

This makes clear each person's responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services, Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted Material must be encrypted if the material is to be removed from the School and limit such data removal. We also have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

5.2 Technical Solutions

- Staff have secure area[s] on the Network where they may store sensitive documents or photographs.
- We require staff to log out of systems when leaving their computer, but also enforce lock out after 10 minutes idle time.

- Staff should not take any sensitive information off site unless it has been encrypted.
- We use the DfE S2S site to securely transfer CTF student data files to other schools.
- We use the Pan-London Admissions system [based on USO FX] to transfer admissions data.
- Staff with access to the Admissions System also use a LGfL OTP tag as an extra precaution.
- We use RAv3 and VPN solutions with its 2-factor authentication for remote access into our systems.
- We use LGfL's USO FX to transfer other data to schools in London, such as references, reports of children.
- We use the LGfL secure data transfer system, USO Auto Update, for creation of online user accounts for access to broadband services and the London content
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fire-proof cabinet. Back-ups are encrypted. No back-up tapes leave the site on mobile devices.
- We use a remote secure back-up and for disaster recovery of our Network, Administration and/or Curriculum Servers.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the School [for use by staff at home], where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder and/or collected by a secure data disposal service.
- We are using secure file deletion software.

6.0 Equipment and Digital Content

6.1 Personal Mobile 'Phones and Mobile Devices

- Mobile 'phones brought into school are entirely at the staff, students', parents'/carers' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- Student mobile 'phones which are brought into school must be turned off [not placed on silent] and stored out of sight to and from school and on arrival at school. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times. All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided, except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile 'phone use is to be open to scrutiny and the Headteacher may withdraw or restrict authorisation for use at any time, if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on or outside the School campus, where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or handheld devices may be searched at any time as part of routine monitoring.
- Where parents/carers or students need to contact each other during the School Day, they should do so only via the School's landline telephone. Staff may use their 'phones during break times. If a staff member is expecting a personal call, they may leave their phone with the School Office to answer on their behalf or seek specific permissions to use their 'phone at a time other than their break time.
- Mobile 'phones and personally owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile 'phones and personally owned mobile devices brought into school are the responsibility of the device owner. The School accepts no responsibility for the loss, theft or damage of personally owned mobile 'phones or mobile devices.
- Mobile 'phones and personally owned devices are not permitted to be used in certain areas within the school site, e.g. Changing Rooms and Toilets.
- Mobile 'phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile 'phone should be switched off at all times and not be used to send images or files to other mobile 'phones.

- Personal mobile 'phones will only be used during lessons with permission from the Teacher.
- No images or videos should be taken on mobile 'phones or personally owned mobile devices without the prior consent of the person or people concerned.

Students' Use of Personal Devices

- The School strongly advises that students' mobile 'phones should not be brought into school. However, the School accepts that there may be particular circumstances in which a parent/carer wishes their child to have a mobile 'phone for their own safety though this is not without its own dangers.
- If a student breaches the School Policy, then the 'phone or device will be confiscated and will be held in a secure place in the School's Main Office. Mobile 'phones and devices will be released to parents/carers in accordance with the School Policy.
- 'Phones and devices must not be taken into examinations. Students found in possession of a mobile 'phone during an examination will be reported to the appropriate Examining Body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact their parent/carer, they will be allowed to use a school phone. Parents/Carers are advised not to contact their child via their mobile 'phone during the School Day but to contact the School via the Main Office.
- Students should protect their 'phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile 'phones and personally owned devices and will be made aware of boundaries and consequences.
- Students may be provided with school mobile 'phones or devices for use in specific learning activities and under the supervision of a member of staff. Such mobile 'phones and/or devices will be set up so that only those features required for the activity will be enabled.

Staff Use of Personal Devices

- Staff handheld devices, including mobile 'phones and personal cameras must be recorded by the School – Name, Make & Model, Serial Number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile 'phones or devices for contacting children, young people or their families within or outside of the School in a professional capacity.
- Staff may be issued with a school 'phone, where contact with students, parents/carers is required.
- Mobile 'phones and personally owned devices should be switched off or switched to 'silent' mode. Bluetooth communication should

be 'hidden' or switched off and mobile 'phones or other personally owned devices should not be used during teaching periods unless permission has been granted by a member of the Strategy and Leadership Team in or for emergency circumstances.

- If members of staff have an educational reason to allow children to use mobile 'phones or a personally owned devices as part of an educational activity, then this should only take place when approved by a member of the Strategy and Leadership Team.
- Staff should not use personally owned devices, such as mobile 'phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the School Policy, then disciplinary action may be taken.
- Where staff members are required to use a mobile 'phone for school duties, for instance in case of emergency during off-site activities or for contacting students or parents/carers, then a school mobile 'phone will be provided and used. In an emergency where a staff member does not have access to a school-owned device, they should use their own device and hide [by inputting 141] their own mobile number for confidentiality purposes.

6.2 Digital Images and Video

In this School:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the Home-School Agreement Form when their child joins the School
- We do not identify students in online photographic materials or include the full names of students in the credits of any published school produced video materials or DVDs
- Staff sign the School's Acceptable Use Policy/Agreement and this includes a clause on the use of mobile 'phones/personal equipment for taking pictures of students
- If specific student photographs [not group photographs] are used on the School Website, in the Prospectus or other high profile publications, the School will obtain individual parental or student permission for its long-term use
- We block/filter access to social networking sites or newsgroups, unless there is a specific approved educational purpose;
- Students are taught about how images can be manipulated in their E-Safety Education Programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents/carers or younger children as part of their IT and PSHE Schemes of Work
- Students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to

understand the need to maintain privacy settings so as not to make public, personal information.

- Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images [including the name of the file] that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

6.3 Asset Disposal

Details of all school-owned hardware will be recorded in a hardware inventory.

Details of all school-owned software will be recorded in a software inventory.

All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Appendix 1

Staff, Governor and Volunteer Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure that:

- Staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk in their use of ICT in their everyday work.

The School will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the School will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of School ICT systems [e.g. laptops, email, VLE etc] out of school and to the transfer of personal data [digital or paper based] out of school.
- I understand that the School ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the School.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using School ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the School's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published [eg on the school website/VLE] it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the School's policies.
- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I am aware of the risks attached to using my personal email addresses, mobile 'phone or social networking sites for such communications and will not do so unless in an emergency.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The School has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *School*:

- When I use my mobile devices [PDAs/laptops/mobile 'phones] in school, I will follow the rules set out in this Agreement, in the same way as if I was using School equipment. I will also follow any additional rules set by the School about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the School ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email [due to the risk of the attachment containing viruses or other harmful programmes].
- I will ensure that my data is regularly backed up, in accordance with relevant School policies.
- I will not try to upload, download or access any materials which are illegal [child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act] or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try [unless I have permission] to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in School policies.

- I will not disable or cause any damage to School equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy [or other relevant policy]. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted Data must be held in lockable storage.
- I understand that Data Protection Policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by School policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies [including music and videos].

I understand that I am responsible for my actions in and out of the School:

- I understand that this Acceptable Use Policy applies not only to my work and use of School ICT equipment in school but also applies to my use of School ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the School.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension or referral to Governing Body or the Local Authority and, in the event of illegal activities, may lead to the involvement of the police.

I have read and understand the above and agree to use the School ICT systems [both in and out of school] and my own devices [in school and when carrying out communications related to the school] within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

Appendix 2

Student Acceptable Use Agreement

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure that:

- Young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- The School will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use School ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the School will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of 'stranger danger', when I am communicating online.
- I will not disclose or share personal information about myself or others when on-line [this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc]
- If I arrange to meet people off line that I have communicated with on line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the School systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try [unless I have permission] to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not use the School systems or devices for on line gaming, on line gambling, internet shopping, file sharing or video broadcasting [eg YouTube], unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the School has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the School:

- I will only use my own personal devices [e.g. mobile phones] in school if I have permission to do so. I understand that, if I do use my own devices in the School, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies [including music and videos].
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the School also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community [examples would be cyber-bullying, use of images or personal information].

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, detention, exclusion, contact with parents/carers and, in the event of illegal activities, involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student Acceptable Use Agreement Form

This Form relates to the Student Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to School ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the School systems and devices [both in and out of school].
- I use my own devices in the School [when allowed], e.g. mobile 'phones, gaming devices, cameras etc.
- I use my own equipment out of the School in a way that is related to me being a member of this School, e.g. communicating with other members of the School, accessing School email, VLE, website etc.

Name of Student:	
Tutor Group;	
Signed:	
Date:	

Appendix 3

Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure that:

- Young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Parents/Carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on line behaviour.

The School will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student Acceptable Use Policy is attached to this Permission Form so that parents/carers will be aware of the School expectations of the young people in their care.

Parents/Carers are requested to sign the Permission Form below to show their support of the School in this important aspect of the School's work.

Permission Form

Parent /Carer's Name: **Student's Name:**

As the parent/carer of the above student, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the School will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be monitored and that the School will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed: **Date:**

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in Newsletters, on the School Website and occasionally in the public media.

The School will comply with the Data Protection Act and request parents'/carers' permission before taking images of members of the School. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use [as such use in not covered by the Data Protection Act]. To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites nor should parents/carers comment on any activities involving other students in the digital or video images.

Parents/Carers are requested to sign the Permission Form below to allow the School to take and use images of their children and for the parents/carers to agree to this.

Digital/Video Images Permission Form

Parent/Carer's Name:

Student's Name:

As the parent/carer of the above student, I agree to the School taking and using digital/video images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the School.

Yes / No

I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Yes / No

Signed:

Date:

Use of Cloud Systems Permission Form

The School may use Google Apps for Education or other cloud hosting services for students and staff. This Permission Form describes the tools and student responsibilities for using these services.

The following services are available to each student and hosted by Google as part of the School's online presence in Google Apps for Education:

Mail - an individual email account for school use managed by the school

Calendar - an individual calendar providing the ability to organize schedules, daily activities, and assignments

Docs - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office

Sites - an individual and collaborative website creation tool

Using these tools, students collaboratively create, edit and share files and websites for school related projects and communicate via email with other students and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

The School believes that use of the tools significantly adds to your child's educational experience.

As part of the Google Terms and Conditions we are required to seek your permission for your child to have a Google Apps for Education account:

Parent/Carer's Name:

Student's Name:

As the parent/carer of the above student, I agree to my child using Google Apps for Education. Yes / No

Signed:

Date:

Use of Biometric Systems

The School uses biometric systems for the recognition of individual children in the School Canteen for payment and in the Learning Resource Centre.

Biometric technologies have certain advantages over other automatic identification systems as students do not need to remember to bring anything with them to the Canteen or Learning Resource Centre so nothing can be lost, such as a swipe card.

The School has carried out a privacy impact assessment and is confident that the use of such technologies is effective and justified in a school context.

No complete images of fingerprints are stored and the original image cannot be reconstructed from the data. That is, it is not possible for example, to recreate a student's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

Parents/Carers are asked for permission for these biometric technologies to be used by their child.

Parent/Carer's Name:

Student's Name:

As the parent/carer of the above student, I agree to the School using biometric recognition systems, as described above. I understand that the images cannot be used to create a whole fingerprint of my child and that these images will not be shared with anyone outside the School.

Yes / No

Signed:

Date:

First Line Information

Support for E-Safety Incidents

E-safety is a key element of safeguarding, subject to inspection by Ofsted and applies to adults and children of all ages.
The consequences of e-safety incidents will cover a range of challenges, with consequences that range from those that may appear trivial to serious abuse and loss of life. This means First Line colleagues must ensure that they treat all reports with appropriate professionalism and follow correct and agreed procedures.
This resource is intended to provide support for those who are new to E-Safety and First Line support.
You are encouraged to regularly view *digitallyconfident.org* where we provide links to current news, opinion and resources in the areas of digital literacy and online safety.
We gratefully acknowledge the assistance of the following people in collating the following resources;
Penny Patterson [LGfL]
David Wright and Ken Corish [SWGfL]
Alan Mackenzie [Independent E-Safety Advisor]

Types of Incidents

Predators

There will be cases where children will agree to meet face to face with abusers who they know or who have become 'friends' via online networks. Some children will be victims of emotional, sexual and physical abuse. There are cases where these relationships result in the death of a child.
Some children will be more vulnerable than others however it is important to recognise that all young people can seek comfort and friendship in online relationships. These relationships can appear more open, trusting and supportive than face to face interactions and as such can pose new and different challenges and dangers.

Bullying & Cyberbullying

Cyberbullying typically takes two forms - by peers and strangers. Most common are the incidents where young people are bullied by other young people who are known to them in their School or wider community. There are incidents where individuals are victims of online bullying by strangers, members of the wider online communities and 'trolls'.

It is also important to note that adults who work with young people can be bullied and threatened by young people, parents and even colleagues.

Illegal or Inappropriate?

It is important to recognise the difference between illegal and inappropriate content and activity. For example; most pornography, whilst inappropriate within a school or work environment, is not illegal. Images of child exploitation (we do not use labels such as 'child pornography' – these images are child abuse and exploitation) are illegal. This can be complicated and sensitive where, for example, children under the age of eighteen are sharing sexual images of themselves. A young person is, in the UK, a child until the age of eighteen and it is understandable that there is ignorance around this when the age of consent is sixteen.

Young people need to be helped to understand that they are creating illegal content which will possibly lead to their friends and relatives becoming convicted and placed on the sex offenders register.

Offence

It is also worth noting that using the labels legal and illegal is not always helpful and it is more effective to ascertain; is the activity an offence?

This distinction is important and **if in doubt, err on the side of caution**. It is an offence to open, view, forward, copy and distribute images of child sex abuse. This means you must not forward or copy files and links to share with colleagues, authorities or the police.

Not an Offence

- Opening an attachment or URL that proves to hold illegal content is an illegal act and is classed as possession of illegal material.
- Showing anyone else illegal material that you have received is an illegal act
- Printing and sharing a copy of the material is an illegal act and is classed as distributing illegal material.
- Receiving unsolicited emails that may contain potentially illegal material [either as an attachment or in a URL] is not an illegal offence.

Never open unsolicited URLs or attachments. If you are suspicious that the content could be illegal report it and log that you have received it.

Sexting and the Law

1. You could end up with a police caution

Sending a naked image of yourself via text message, or social media, when you're below the age of 18 is technically illegal. It counts as an offence of distributing an indecent image of a child. You could even end up on the sex offenders register.

"*The law doesn't distinguish between an indecent image of you and an indecent image of someone else.*"

2. It is worse to send a photo of a sexual act

Even though the age of sexual consent is 16, the age for distributing indecent images is 18. That means that a 17-year-old who can legally have sex cannot legally send a naked image. It's just as bad for a 15-year-old as a 17-year-old to sext but what is worse for a 15-year-old is to send a photo showing them having sex. It is illegal for anyone below the age of 16 to have sex, so if the photo shows this, it could lead to them having doubly bad consequences.

If a 17-year-old sent a sext showing them having sex, they would still be committing an offence by sending a naked image - but it wouldn't break the law around consent. A 15-year-old doing the same would be committing two offences.

3. An unwanted sext could be seen as a crime

But if you do send a naked selfie to someone who is likely to be upset by it, that could be a crime under the Malicious Communications Act.

4. Forwarding them on breaches civil law

"*When you create a photo, as the creator you automatically become the owner of the copyright. Anyone who's taking a risqué picture and sending it to their partner, they'll own the copyright.*"

If the receiver of the image then circulates it, or posts it on a website, they are then infringing that copyright.

5. You could become a victim of revenge porn

One serious risk of sending explicit pictures is that someone could pass them on – either by circulating them or posting them onto a website. Once the pictures are there, it is hard to get them taken down.

You could approach websites with claims of breaching harassment laws and copyright laws, but it's often too late.

However someone who posts photos of an ex, perhaps, in a moment of anger, could be prosecuted for this.

6. You could break Privacy Law

Another issue with forwarding on images.

'*We'd argue that communication was being made in the private constraints and any wider dissemination of that content would be breach of privacy.*'

So...Can you sext safely?

If you are under 18, it is an offence to take and/or send a naked picture of yourself. It's not illegal to be naked with someone, even if you are 15 but you cannot send that picture.

As strange as it seems, it is the law and it's best to know the risks now.

Source: www.telegraph.co.uk/women/womens-health/10985660/Sexting-scare-6-sexting-myths-busted.html

The Law with regard to illegal activity

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority.
- Obtain unauthorised access to a computer.
- 'Eavesdrop' on a computer.
- Make unauthorised use of computer time or facilities.
- Maliciously corrupt or erase data or programs.
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The Act states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts
- Ascertain compliance with regulatory or self-regulatory practices or procedures
- Demonstrate standards, which are or ought to be achieved by persons using the system
- Investigate or detect unauthorised use of the communications system
- Prevent or detect crime or in the interests of national security
- Ensure the effective operation of the system

Monitoring but not recording is also permissible in order to:

- Ascertain whether the communication is business or personal
- Protect or support help line staff.
- The School reserves the right to monitor its systems and communications in line with its rights under this Act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol [words, shapes or images] that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, television broadcasts and other media [e.g. YouTube].

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour or

- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs [digitally collated or otherwise]. A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice [including by phone or using the Internet] it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. [Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust]. Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate, page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an ‘obscene’ article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers [and nominated staff] to search for electronic devices. It also provides powers to search for data on those devices and to delete data.
[cf DfE guidance:
www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening- searching-and-confiscation]

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems.

The School Information Regulations 2012

Requires schools to publish certain information on its website:
www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations

Dealing with a device where there is suspicion of illegal content

It is advised that if there is suspicion of something illegal on a school device [and this would now also relate to a device brought in by a student], then the device is to be powered off at the plug (not Shut Down), locked away in a secure cabinet and nobody allowed to access that cabinet until the police have arrived and determined, upon investigation, whether the device warrants seizure or not.

As many devices such as 'phones, tablets and laptops have their own power supply via a battery, the advice to power off via the mains supply is not relevant. In such cases the device can be turned off and secured immediately in a safe location to ensure no one has further access to it prior to investigation.

It is also good practice that when the member of staff seizes the device they record the date and time.

We can see in the following materials by SWGfL that the decision to search a student or adult's device must be made with care. There is a balance between infringing people's rights and protecting the individual. With this in mind it would be prudent to ensure that responsible individuals [Senior Leaders and those with responsibility for safeguarding and e-safety] follow an agreed and documented procedure to search a device. The act of searching a personal device may be seen as sensitive as a physical search of the child or adult involved.

Extract from SWGfL School E-Safety Policy Template Document

The Education Act 2012, the basis of this template, sets out what the law is presumed to be, based on prior legal and educational knowledge, and common sense. Rights and responsibilities regarding physical contact and personal data are still evolving rapidly. So too are social, entertainment and educational technologies and the skills necessary to use them safely and prudently. This is particularly so where those who are under 18 are involved.

No existing law or policy can fully insulate anyone from the risk involved in searching for, access to or deletion of the personal data of others. Anyone refraining from any such search, access or deletion when hindsight shows circumstances merit such actions may however be at significant risk and may put seriously at risk the wellbeing of children entrusted to their care. This template cannot therefore be relied on as justification for any act or lack of action by anyone – there is no substitute for the proper and well documented exercise of adequately informed professional judgement. .

It is for each School's Headteacher and Governors to set, apply and monitor application of their own policies as guided by their head teacher, local authority and official guidance, especially if the school is local authority maintained. This template is intended as an aide to this. South West Grid for Learning Trust does not and cannot accept and does not have responsibility for any school's policy on this or any other matter.

Where sections in the template are written in ITALICS it is anticipated that schools would wish to consider whether or not to include that section or statement in their completed policy.

Where sections are highlighted in BOLD text, it is the view of the SWGfL E-Safety Group that these ought to be an essential part of a school E-Safety Policy.

The template uses the term students to refer to the children/young people attending the learning institution and the term Headteacher. Schools will need to choose which terms to use and delete the others accordingly.

Introduction

The changing face of information technologies and ever increasing student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 [Discipline] there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the School Rules are determined and publicised by the Headteacher [Section 89 Education and Inspections Act 1996].

An item banned by the School Rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- Are banned under the school rules and
- Are banned AND can be searched for by authorised school staff

The Act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the School Rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Headteacher must publicise the School Behaviour Policy, in writing, to staff, parents/carers and students at least once a year. [There should therefore be clear links between the search etc. policy and the Behaviour Policy].

DfE advice on these sections of the Education Act 2011 can be found in the document: 'Screening, searching and confiscation – Advice for Headteachers, Staff and Governing Bodies' www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

It is recommended that Headteachers [and, at the least, other senior leaders] should be familiar with this guidance.

Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 [Discipline]
- The School Behaviour [Determination and Publicising of Measures in Academies] Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

Responsibilities

The Headteacher is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headteacher will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: [insert relevant names / roles / group]

The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data/files on those devices: [the policy should here list those staff/roles given such authority. A Headteacher may choose to authorise all staff willing to be authorised but should consider training needs in making this decision].

The Headteacher may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Members of staff [other than Security Staff] cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff.

Training/Awareness

It is essential that all staff should be made aware of and should implement the School's policy.
Members of staff should be made aware of the School's Policy on 'Electronic Devices – Searching and Deletion':

- At induction
- At regular updating sessions on the School's E-Safety Policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy Statement relating to Searching Devices

The School Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data/ files on those devices.

The School has a policy relating to whether or not mobile phones and other electronic devices are banned or are allowed only within certain conditions. The School should therefore consider including one of the following statements in the policy:

Authorised staff [defined in the responsibilities section above] have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

Searching without consent - Authorised staff may only search without the student's consent for anything which is either 'prohibited' [as defined in Section 550AA of the Education Act 1996] or appears in the School Rules as an item which is banned and may be searched for.

IN CARRYING OUT THE SEARCH

The authorised member of staff must have reasonable grounds for suspecting that a student is in possession of a prohibited item. ie an item banned by the School Rules and which can be searched for. [Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training].

The authorised member of staff should take reasonable steps to check the ownership of the mobile 'phone/ personal electronic device before carrying out a search. [The powers included in the Education Act do not extend to devices owned - or mislaid - by other parties eg
Students are allowed to bring mobile 'phones or other personal devices to school but may only use them within the rules laid down by the School and sanctions applied as laid down in the School Behaviour Policy and in the Policy on the use of mobile devices in school.

The authorised member of staff should take care that, where possible, searches do not take place in public places, eg an occupied classroom, which might be considered as exploiting the student being searched.

The authorised member of staff carrying out the search must be the same gender as the student being searched and there must be a witness [also a staff member. If at all possible, they too should be the same gender as the student being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a student of the opposite gender including without a witness present **but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately**

and where it is not reasonably practicable to summon another member of staff.

EXTENT OF THE SEARCH

The person conducting the search may not require the student to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear [outer clothing includes hats, shoes, boots, coat; blazer; jacket; gloves and scarves].

'Possessions' means any goods over which the student has or appears to have control. This includes desks, lockers and bags. [The School will take account of religious beliefs particularly with regard to garments/headwear]

A student's possessions can only be searched in the presence of the student and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets but not an intimate search going further than that, which only a person with more extensive powers [eg a police officer] can do.

Use of Force – force cannot be used to search without consent for items banned under the School Rules regardless of whether the rules say an item can be searched for.

Further information relating to searching students can be found in this Department of Education document [published February 2014] www.gov.uk/government/publications/ searching-screening-and-confiscation

ELECTRONIC DEVICES

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so [ie the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules].

The examination of the data/files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence [of a criminal offence or a breach of school discipline] or whether the material is of such seriousness that it requires the involvement of the police.

Examples of illegal activity would include:

- Child sexual abuse images [including images of one child held by another child]
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The School will also consider its duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. Arrangements will be put in place to support such staff.

Further guidance on reporting the incident to the police and the preservation of evidence can be found in the SWGfL flow chart in the main School Template Policies document.

DELETION OF DATA

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data

FIRST LINE SUPPORT FOR ESAFETY INCIDENTS

For files, if they think there is a good reason to do so ie the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules].
A record should be kept of the reasons for the deletion of data/files. [DfE guidance states and other legal advice recommends that there is no legal reason to do this, best practice suggests that the school can refer to relevant documentation created at the time of any search or data deletion in the event of a student, parental or other interested party complaint or legal challenge. Records will also help the school to review e-safety incidents, learn from what has happened and adapt and report on application of policies as necessary].

CARE OF CONFISCATED DEVICES

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices (particularly given the possible high value of some of these devices).
The school may wish to add a disclaimer to the relevant section of the Behaviour Policy which may assist in covering the school against damage / loss claims.

AUDIT / MONITORING / REPORTING / REVIEW

The responsible person Assistant Headteacher with accountability for E-Learning will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files. (A template log sheet can be found in the appendices to the E-

Safety Template Policies]. These records will be reviewed by the E-Safety Officer and E-Safety Governor] at regular intervals [state the frequency].

This policy will be reviewed by the Headteacher and Governors annually and in response to changes in guidance and evidence gained from the records.

The School is required is publish its Behaviour Policy to parents/carers annually [including on its website] – the Behaviour Policy should be cross referenced with this policy on search and deletion.

E-Safety Log

Schools must have rigorous and meaningful reporting procedures in place and this includes an e-safety log. The purpose of the log is to record all illegal/inappropriate/accidental/deliberate incidents. The log ensures that appropriate action is taken and child safeguarding is the priority. Over time the log will also act to inform policy and practice reviews by highlighting the types and frequency of incidents. Training and teaching can then be set in place to help minimise the likelihood of similar incidents in future.

Further to completing the incident log, all adults involved in the reporting process should email a brief summary of the incident to the Headteacher. This means that they have a time/date stamped record of when they notified their Headteacher, and leaves a clear audit trail for future reference if required.

E-Safety Incident Log

The E-Safety Incident Log details of ALL e-safety incidents to be recorded by the E-Safety Coordinator. This incident log will be monitored termly by the SaLT and the E-Safety Designated Governor.

Record of Reviewing Devices/Internet Sites [Responding to Incidents of Misuse]
Details of first reviewing person:
Details of second reviewing person
Name and location of computer used for review (for web sites)

Date & Time	Name of pupil or staff member	Room and computer / device number	Details of incident (including evidence)	Actions	Name and role of person completing this entry

Group	
Date	
Reason for investigation	

Name	
Position	
Signature	
Name	
Position	
Signature	

Website[s] address/device

Conclusion

Reason for concern

Action proposed or taken

Managing Incidents

For Headteachers, Senior Leaders and Governors

Involving staff as victims

All incidents should be reported to the Headteacher and/or Governors who will:

- Record in the School's E-Safety Incident Log
- Keep any evidence – printouts and/or screen shots
- Use the 'Report Abuse' button, if appropriate
- Consider involving the Chair of Governors and/or reporting the incident to the Governing Body

Parents/Carers as Instigators

Contact the person and invite into school and discuss using some of the examples below:

- You have become aware of discussions taking place online ...
- You want to discuss this…
- You have an open door policy so disappointed they did not approach you first
- They have signed the Home School Agreement which clearly states ...
- Request the offending material be removed

If this does not solve the problem:

- Consider involving the Chair of Governors
- Consider involving the police [Communications Act 2003 & Malicious Communications Act 1988]

Staff/Colleagues as Instigators

- Contact Schools HR for initial Advice and/or contact Schools E-Safety Coordinator In all serious cases this is the first step.
- Contact the member of staff and request the offending material be removed immediately, [in serious cases you may be advised not to discuss the incident with the staff member]
- Refer to the signed ICT Acceptable Use Agreement, Professional Code of Conduct and consider if this incident has an impact on the Contract of Employment of the member of staff.
- Provide additional training
- Invoke disciplinary procedures

Students as instigators

Follow some of the steps below:

- Identify the students involved
- Ask student to remove offensive material. Refer to the signed Acceptable Use Agreement.
- If the perpetrator refuses to remove the material and is under 13 contact the Social Network who will close the account
- Take appropriate actions in line with School Policies and Rules
- Inform parents/carers if serious or persistent incident
- For serious incidents or further advice contact the Local Police Safer Neighbourhood

- Inform your Local Police Safer Neighbourhood Team, Local Authority support services re-bullying
- If the child is at risk inform your school Child Protection Officer

Further Support

- The School' s HR Manger
- Governor Services
- Teaching Union
- Police
- School's External HR Support
- School Solicitors
- Local Authority
- **Where a child is believed to be at risk, contact Child Protection Officer**

Illegal E-Safety Incident

For Headteachers, Senior Leaders and Governors

Examples of illegal activity/content:

- Downloading child abuse images/files
- Sharing images or video containing child abuse
- Inciting racial or religious hatred
- Extreme cases of Cyberbullying
- Promoting illegal acts

If illegal material or activity found or suspected:

- Isolate device securely. [do not view or share content]
- Inform E-Safety Officer, SaLT, Police, Chair of Governors, Secondary School Senior Education Advisor, London Borough of s If a student is involved notify Child Protection Officer
- If a member of staff is involved contact LA Designated Officer for allegations against staff.

Non-Illegal E-Safety Incident

For Headteachers, Senior Leaders and Governors

Involving staff as victims

Incident could be:

- Using another person's password, online identity or log on details.
- Accessing websites which are against School Policy, eg games, social networks.
- Using a mobile 'phone to take video during a lesson.
- Using the technology or social media to upset or bully or bring the individual, profession or organisation into disrepute.

If member of staff has:

- Behaved in a way that has harmed a child, or may have harmed a child.
- Possibly committed a criminal offence against or related to a child; or
- Behaved towards a child or children in a way that indicates he or she would pose a risk of harm if they work regularly or closely with children.

- Contact the LADO
- Review evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow School Disciplinary Procedures

Non-Illegal E-Safety Incident

Students as instigators

- Review incident and identify if other pupils were involved
- Decide appropriate sanctions and/or support based on School Rules/ Guidelines
- Inform parents/carers if serious or persistent incident. In serious incidents consider informing the Child Protection Officer as the child instigator could be at risk
- Review school procedures/policies to develop best practice

Students as victims

In –school action to support pupil by one or more of the following:

- Class Teacher
- E-safety Coordinator
- Senior Leader or Headteacher
- Designated Senior Person [s] for Child Protection
- School Police Community Support Officer

Then do the following:

- Inform parents/carers as appropriate.
- If the child is at risk inform CSPLO immediately.
- Confiscate the device, if appropriate.

Useful Links

Digitally Confident
www.digitallyconfident.org
South West Grid for Learning
www.swgfl.org.uk/Staying-safe
Childnet
www.childnet.com
Thinkyouknow
www.thinkyouknow.co.uk
Internet Watch Foundation
www.iwf.org.uk
CEOP
http://ceop.police.uk
Beat Bullying
www.beatbullying.org/gb/who-is-on-this-site
Reporting links for popular online services
http://cyberbullying.us/report
Guidelines on prosecuting cases involving communications sent via social media
www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media
Dealing with indecent images of children in the workplace: A Best Practice Guide
www.iwf.org.uk/resources/best-practice-guide