HARLINGTON SCHOOL

Author I Wells
Reviewed and updated: June 2016
Next review: June 2017
Status: Non Statutory

E-Safety Policy

Contents

1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy be communicated to staff/students/community
- Handling complaints
- Review and Monitoring

2. Education and Curriculum

- Student e-safety curriculum
- Staff and governor training
- Parent awareness and training

3. Expected Conduct and Incident Management

- Expected conduct
- Staff, volunteers and contractors
- Parents/Carers
- Incident Management

4. Managing the ICT Infrastructure

- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Cloud Environments
- Social networking
- Video Conferencing

5. Data Security: Management Information System access and Data transfer

- Strategic and operational practices
- Technical Solutions including asset disposal

6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video
- Asset disposal

Appendices:

1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement (Students)
3. Protocol for responding to online safety incidents

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Harlington School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and 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 for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be 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 content including incitement
- Content validation: how to check authenticity and accuracy of online content

Contact
- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct
- Aggressive behaviours (bullying, trolling, etc)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (Internet or gaming), gambling, body image, etc)
- 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)

Scope

This policy applies to all members of Harlington School community (including staff, students / students, volunteers, parents / carers, visitors, community users) who have access to and are users of the school ICT systems, both in and out of Harlington School.

The Education and Inspections Act 2006 empowers Headteacher 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. 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. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Harlington 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.

Roles and responsibilities

Role	Key Responsibilities
Headteacher	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance. • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL services • To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious online safety incident. • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of students, including risk of children being radicalised • To receive regular monitoring reports from the Online Safety Co-ordinator / Officer • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager. • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information.

Role	Key Responsibilities
Online Safety Co-ordinator / Designated Child Protection Lead	• To take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents. • Promotes an awareness and commitment to e-safeguarding throughout the school community. • Ensure that online safety education is embedded within the curriculum • Educating Parents and raising awareness as instructed by Head? • Ensures that online safety education is embedded across the curriculum • Liaises with the schools ICT technical staff. • To communicate regularly with SLT and the designated e-safety Governor / committee 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 online safety incidents are logged as a safeguarding incident • Facilitates training and advice for all staff • Oversee any student surveys / student feedback on online safety issues • Liaises with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns. These may include: • 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 / Safeguarding governor (including online safety)	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the Online Safety Policy and review the effectiveness of the policy. • To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the online safety Governor will include: regular review with the online safety Co-ordinator.
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum
Network Manager/ technician	• To report online safety related issues that come to their attention, to the Online Safety Coordinator. • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis. • To ensure that all data held on students on the 3^{rd} party services such as

Role	Key Responsibilities
	Virtual learning environments are adequately protected. • That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher • LGfL is informed of issues relating to the filtering applied by the Grid • That the use of the *network / Virtual Learning Environment (LEARNING PLATFORM) / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *E-Safety Co-ordinator / Officer /Headteacher for investigation / action / sanction* • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. That disaster recovery plans are in place. • To keep up-to-date documentation of the school's online security and technical procedures
Data and Information (Asset Owners) Managers	• Ensure the processes and procedures contained in the data protection policy are followed. • To ensure that the data they manage is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • The school must be registered with Information Commissioner
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 if 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
All staff, volunteers and contractors.	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement, and understand any updates annually. The AUA is signed by new staff on induction. • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held 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 online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with students should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. **Exit strategy** • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN

Role	Key Responsibilities
	numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Students	• Read, understand, sign and adhere to the Student Acceptable Use Agreement. • 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 understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school • To contribute to any 'student voice' / surveys that gathers information of their online experiences • 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 mobile/hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good online 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
Parents/carers	• To read, understand and promote the school's Student Acceptable Use Agreement with their child/ren. • To consult with the school if they have any concerns about their children's use of technology. • To support the school in promoting online safety including the students' use of the Internet and the school's use of photographic and video images. • To consult with the school if they have any concerns about their children's use of technology.
External groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school • to support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

Communication:

The policy will be communicated to staff/students/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 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

Handling Incidents:

- 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/counselling by tutor / Director of Learning / Online Safety Coordinator / Headteacher;
    - informing parents or 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 LA / Police.
- Our Online Safety Coordinator acts as first point of contact for any incident. Any complaint about staff misuse is referred to the Headteacher. If the misuse concern is about the Headteacher then the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).
- Complaints and incidents are dealt with in accordance with our relevant school policies. Complaints related to child protection are dealt with in accordance with school child protection procedures.

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy).

- The school has an Online safety coordinator who will be responsible for document ownership, review and updates.
- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and students.

2. Education and Curriculum

Student e-safety curriculum

Harlington School:

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience. This includes:
    - 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 / 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 / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; 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, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- Plans online 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 the student Acceptable Use Agreement(s);
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- 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 / gambling;

- Ensures that staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- Ensure students only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

Harlington School:

- Makes regular training available to staff on online safety issues and the school's online safety education program;
- Provides, as part of the induction process, all new staff [including those on university/college placement, and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements
- 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 programs.
- Provides, as part of the induction process, all new staff [including those on university/college placement, apprentices and work experience] with information and guidance on the e-safety policy and the school's Acceptable Use Agreements.

Parent awareness and training

Harlington School:

- Provides induction for parents which includes online safety;

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
    - Information leaflets; in school newsletters; on the school web site;
    - demonstrations, practical sessions held at school;
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In Harlington School, all users:

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Agreement which they will be expected to sign before being given access to school systems.
- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences;

- Understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras; They should also know and understand school policies on the taking / use of images.

Staff, volunteers and contractors

- Are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.
- Know to take professional, reasonable precautions when working with students, previewing websites before use; using age-appropriate (student friendly) search engines where more open Internet searching is required with younger students;

Parents/Carers

- Should provide consent for students to use the Internet, as well as other technologies, as part of the student 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

Incident Management

Harlington School:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions.
- All members and its 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 (e.g. the local authority and LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school.
- Parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

Harlington School:

- Informs all users that IT devices/network/Internet/email use is monitored;
- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant;
- Ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)

Harlington School:

- Uses individual, audited log-ins for all users - the London USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Has additional local network monitoring/auditing software installed;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, Harlington School:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school's network / We also provide a different/use the same username and password for access to our school's network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;

- All students have their own unique username and password which gives them access to the Internet and other services;
- Makes clear that no one should log on as another user and makes clear that students should never be allowed to log-on or use teacher and staff logins;
- 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 log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- This school uses secure data transfer; this includes 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);
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;
- Requests that teachers 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. We request that they DO switch the computers off at the end of the day and we also automatically switch off all computers at 7 o'clock to save energy;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or 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;
- 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, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- 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's requirements;

- Uses our broadband network for our CCTV system and have had set-up by approved partners;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

- This school makes it clear that staff and students must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our MIS system.
- We require staff to change their passwords into the MIS, LGfL USO admin site, other secure processes twice a year.

E-mail

Harlington School:

- Provides staff with an email account for their professional use, London Staffmail and makes clear personal email should be through a separate account;
- Provides students with highly restricted email accounts that are anonymous; This is via Londonmail/Trustmail with students as this has email content control
- Does not publish personal e-mail addresses of students on the school website.
- Will contact the Police if one of our staff or students receives an e-mail that we consider is 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. This includes responding to the "Prevent" requirements.
- Monitors the content of the emails for safeguarding purposes within the limitations of the technology available.
- Knows that spam, phishing and virus attachments can make e mails 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 World Wide Web.

Students:

- We use LGfL LondonMail / TrustMail with students and lock this down where appropriate using LGfL SafeMail rules.
- Students' LGfL LondonMail e-mail accounts are intentionally 'anonymised' for their protection.
- Students are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- Students 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 / 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 is not permitted.

Staff:

- Staff can only use approved e mail systems on the school system including LGFL and Google
- Staff only use LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Staff 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. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX;

School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- Uploading of information is restricted to our website authorisers.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use students' names when saving images in the file names or in the tags when publishing to the school website;
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Cloud Environments

Harlington School is expanding its access and use of "Cloud" services. As this develops further we will include these protocols:

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In school, students are only able to upload and publish within school approved 'Cloud' systems.
- All third party 'Cloud' systems must comply with the data protection expectations outlined in our data protection policy.

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed **not** to run social network spaces for any current Harlington students use on a personal basis or for teachers to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- Teachers are strongly advised not to provide ex Harlington students with access to their own personal social networking spaces.
- The use of any school approved social networking will adhere to school's communications policy.
- School staff will ensure that in private use:
- No reference should be made in social media to Harlington students, parents/carers or school staff;
- School staff should not be online friends with any students. Any exceptions must be approved by the Headteacher.
- 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 and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Students:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our [age appropriate] student Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

Video Conferencing

Harlington School:

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

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We 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.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At Harlington School:

- The Head Teacher 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. We have listed the information and information asset owners .
- We ensure staff know who to report any incidents where data protection may have been compromised. This and other processes are outline in our data protection policy.
- All staff are DBS checked and records are held in one central record
  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

  This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow LA/Government 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 have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- Harlington 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.

Technical Solutions including asset disposal

- Staff have secure area(s) on the network to store sensitive documents or photographs. Currently home drives and the schools S: drive
- We require staff to log-out of systems when leaving their computer.
- We use encrypted flash drives if any member of staff has to take any sensitive/personal information off site.
- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.
- All servers are in lockable locations and managed by DBS-checked staff.
- 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.
- 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.
- Protected data, is disposed of through the same procedure.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
- We are using secure file deletion software.
- 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 an LGfL OTP tag as an extra precaution.
- We use RAv3 / VPN solution 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, USOAutoUpdate, 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.
- We lock any back-up tapes in a secure, fire-proof cabinet. No back-up tapes leave the site on mobile devices.
- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, students' & parents' or visitors own risk. Harlington School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Student mobile phones which are brought into Harlington School must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight in all lessons. All visitors are requested to keep their phones on silent.
- Students must not record , take or share images, video and audio on any mobile phone or other digital device whilst on school property. is to be avoided; except where it has been explicitly agreed 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 is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

- The recording, taking and sharing of images, video and audio by staff on any mobile phone is to be avoided; except where it has been explicitly agreed 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 is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- Harlington School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence, incitement, or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. 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 other than their break times.
- 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 in to school are the responsibility of the device owner. Harlington 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.

Students' use of personal devices

- Harlington School advises that student mobile phones should not be brought into school.
- Harlington School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- 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 office. Mobile phones and devices will be released to parents or 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 exam 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 his or her parents or carers, they will be allowed to use a school phone at an appropriate time not during lessons. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school 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.
- There may be occasions when students will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones 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 noted in 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 setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior 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, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't 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.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

In Harlington School:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son 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 / DVDs;
- Staff sign the school's Acceptable Use Agreement and this includes a clause on the use of mobile phones / personal equipment for taking pictures of students;
- If specific students photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or student permission for its long term use
- The school blocks/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 or younger children as part of their ICT scheme 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 identify 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.