Lady Margaret School

E-Safety Policy

Adopted: November 2015
Next Review: Autumn 2016

Contents

Policy

Procedures

Equipment and Digital Content

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

Policy

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 Lady Margaret School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Lady Margaret 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)

(Ref Ofsted 2013)

Scope

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

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the Lady Margaret 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.

Lady Margaret 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. In addition, the school will actively cooperate with the police and other agencies to identify and sanction offenders.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL (London Grid for Learning) • 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 Co-ordinator / Officer • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager)
E-Safety Co-ordinator	• To take day to day responsibility for e-safety issues and has 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 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 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

Role	Key Responsibilities
	• Is 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. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. Nicky Thomson, a member of the Governing Body has taken on the role of E-Safety Governor • To support the school in encouraging parents 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 Co-ordinator (including e-safety incident logs, filtering / change control logs)
ICT / Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum

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 ICT system • To ensure that access controls 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 keep 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 remote access and email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation and, if necessary, sanction. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To ensure that all data held on pupils on the school machines have appropriate access controls in place. • 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 pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand and adhere to the school Use of ICT Network and Equipment Policy • To understand and adhere to the school policy on passwords. • 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 e-safety coordinator • To maintain an awareness of current e-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 pupils should be on a professional level and only through school based systems including school email.

Role	Key Responsibilities
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy for ICT • 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 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 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 • 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/ review of e-safety policies • To understand that their use of the school network and school email is monitored. • In addition, some pupils have been asked to participate in a peer mentoring scheme.
Parents/carers	• To support the school in promoting e-safety by signing and endorsing Pupil Acceptable Use Policy for ICT • To consult with the school if they have any concerns about their children's use of technology

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Pupil Acceptable Use Policy for ICT discussed with pupils and signed by pupils and parents at the start of each year.

Handling 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. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

    - interview/counselling by tutor / Head of Year / E-Safety Coordinator / Headteacher;
    - informing parents or carers;
    - removal of Internet or computer access for a period,
    - referral to LA / Police.

- Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

The e-safety policy is referenced from within other school policies: Use of ICT Network and Equipment policy, Child Protection policy, Data Protection policy, Anti-Bullying policy, Behaviour policy, PSHE and Citizenship 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 every two years or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

Procedures

Education and Curriculum

Pupil e-safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum and PSHE curriculum. It is built on LGfL 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 / 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;
    - ✓ [for older pupils] 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 be aware of the role and function of extremist recruitment sites.
    - ✓ 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 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 a Pupil Acceptable Use Policy for ICT which every student will sign and keep in their daybooks.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils 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;

  In addition to the PSHE and Computing lessons pupils undergo a two day workshop at the end of Y9 covering many aspects of e-safety

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to adequately secure any school data on devices they are using
- Makes regular training available to staff on e-safety issues and the school's e-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 e-safeguarding policy and the school's E-Safety Policy.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Yearly Pupil Acceptable Use Policy for ICT, to ensure that principles of e-safe behaviour are made clear
    - Yearly mailings sent home with suggestions for safe Internet use at home and provision of information about national support sites for parents. These mailings are also made available on the school website

Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy for ICT which pupils will be expected to sign before being given access to school systems and the Use of ICT Network and Equipment policy which covers staff use of ICT.
- 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 cyber-bullying

Staff

- are responsible for reading the school's e-safety policy and Use of ICT Network and Equipment policy and using the school ICT systems accordingly.

Pupils

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

Parents/Carers

- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In this 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 its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively.
- support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues. The school will actively cooperate with the police and other agencies to identify and sanction offenders.

- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited 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.
- Pupils are able to speak to specially trained peer mentors to discuss e-safety issues.

Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

This 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 / stage of the students;
- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or LGfL approved systems (Egress Switch) 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;
- Uses security time-outs on the network ;
- 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 pupils' 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 students have signed an acceptable use agreement form and understands that they must report any concerns;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. Google Safe Search,
- Informs all users that Internet use is monitored;
- 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 programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents

- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all;
- 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;
- Ensures the network manager is up-to-date with LGfL services and policies

To ensure the network is used safely, this school:

- Ensures staff read and that they have understood the school's e-safety Policy and Use of ICT Network and Equipment policy. Following this, they are set-up with Internet, email access and network access.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with an individual network log-in username. They are also expected to use a personal password;
- All pupils have their own unique username and password which gives them access to the Internet, and their own school approved email account;
- 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 pupils and one for staff. Staff and pupils 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 lock a PC if they are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Automatically switch off all computers at 21:00 to save energy;
- Has set-up the network so that pupil accounts cannot download executable files / programmes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network and maintains a separate wifi network for guest devices ;
- 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
- 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;
  e.g. teachers access report writing module; SEN coordinator - 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:
- 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;
- Uses the DfE secure s2s website for all CTF (Common Transfer Files) sent to other schools;
- Ensures that all pupil 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 FX (secure file exchange);
- Follows ISP (Internet Service Provider) advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- 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.

Passwords

- This school makes it clear that staff and pupils 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 a different password to access the MIS (Management Information System) from the one they use to access the network.
- All staff are required to change passwords for the MIS and the school network at the beginning of every term.
- The Staff part of the network has additional password protection. This password is also changed termly.

- If staff are accessing school email via a device where the password has been saved such as a personal phone or tablet they must ensure that a passcode or password for that device is used.

E-mail

This 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 pupils.
- Will contact the Police if one of our staff or pupils 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.
- 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, 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.

Pupils:

- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- Pupils 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.

- Pupils sign the Pupil Acceptable Use Policy for ICT 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.

Staff:

- Staff can only use the e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems (Egress Switch).
- Staff know that e-mail 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 'house-style':

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 Office Manager
- The school web site 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, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, admin@ladymargaret.lbhf.sch.uk Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images

Social Media

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, 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 Lady Margaret School
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation.

Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information
- We ensure staff know who 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 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.
- 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

- Staff have secure areas on the network to store sensitive documents
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 5 minutes idle time.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- We use RAv3 / VPN solution with its 2-factor authentication for remote access into our systems.
- We use LGfL's USO FX and S2S 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 locked filing cabinets in the school office
- All servers are locked in the server room managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fire-proof cabinet.

- We comply with the WEEE (Waste Electronic and Electrical Equipment) 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.
- 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.
- Storage devices are physically destroyed before disposal.

Equipment and Digital Content

Pupil use of personal devices

School policy concerning the use of personal electronic devices by pupils is set out in the Use of Personal Electronic Devices section of the Use of ICT Network and Equipment policy.

Staff use of personal devices

- School policy concerning the use of personal electronic devices by staff is set out in the Virtual Access to LMS Network section of the Use of ICT Network and Equipment policy. In addition to this.
- 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.
- 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 unless there is a clear and documented need for specialist equipment.

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 school agreement form when their daughter joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;

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 library.
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 physically destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use the local authority to dispose of equipment.