HARMONDSWORTH PRIMARY SCHOOL

LONDON BOROUGH OF HILLINGDON

COMPUTING POLICY

At Harmondsworth Primary School we seek to develop children's understanding and appreciation of information and communication technology (ICT) and the way it impacts on our everyday life. We believe it is essential to provide opportunities in all National Curriculum subject areas for children to develop their computing capability and to use it to support their learning. Computing makes education accessible to all, irrespective of learning styles and individual needs. At Harmondsworth we recognise that pupils are entitled to quality hardware and software and a structured and progressive approach to the learning of the skills needed to enable them to use it effectively. Computing education is provided in a safe, happy and disciplined environment to stimulate and challenge both pupils and staff. The purpose of this policy is to state how the school intends to make this provision.

Rationale

"A high-quality computing education equips pupils to use computational thinking and creativity to understand and change the world. Computing has deep links with mathematics, science, and design and technology, and provides insights into both natural and artificial systems. The core of computing is computer science, in which pupils are taught the principles of information and computation, how digital systems work, and how to put this knowledge to use through programming.

Building on this knowledge and understanding, pupils are equipped to use information technology to create programs, systems and a range of content. Computing also ensures that pupils become digitally literate – able to use, and express themselves and develop their ideas through, information and communication technology – at a level suitable for the future workplace and as active participants in a digital world."

National Curriculum 2014

Aims & Objectives of Computing

The school's aims are to:
- Provide a relevant, challenging and enjoyable curriculum for computing for all pupils.
- Meet the requirements of the national curriculum programmes of study for computing.
- Use ICT and computing as a tool to enhance learning throughout the curriculum.
- To respond to new developments in technology.
- To enhance learning in other areas of the curriculum using ICT and computing.
- To develop the understanding of how to use ICT and computing safely and responsibly.
- To encourage children to develop positive attitudes to ICT and to understand its importance and relevance to today's world.
- To enable children to acquire a broad range of ICT and computer capabilities and to be confident about using a range of hardware and software.

Aims & Objectives of Computing (continued...)

- To enable children to develop ICT as a tool for learning and investigation in all subject areas.
- To use ICT to develop independent ways of working which encourage children to take responsibility for their own actions.
- To use ICT to encourage children to work co-operatively, taking responsibility collectively.
- To set ICT tasks which require flexibility of mind and open mindedness in problem solving.
- To learn how to stay safe online (see separate Online Safety Policy)

The national curriculum for computing aims to ensure that all pupils:
- Understand and apply the fundamental principles of computer science, including logic, algorithms, data representation, and communication
- Analyse problems in computational terms, and have repeated practical experience of writing computer programs in order to solve such problems
- Evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems.
- Are responsible, competent, confident and creative users of information and communication technology.

Teaching & Learning

Early Years & Foundation Stage
It is important in the foundation stage to give children a broad, play-based experience of computing in a range of contexts, including outdoor play. Computing is not just about computers. Early years learning environments should feature ICT scenarios based on experience in the real world, such as in role play. Children gain confidence, control and language skills through opportunities to 'paint' on the whiteboard or drive a remote-controlled toy. Outdoor exploration is an important aspect, supported by ICT toys such as walkie-talkie sets. Recording devices can support children to develop their communication skills. This is particularly useful with children who have English as an additional language.

By the end of key stage 1 pupils should be taught to:
- understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following a sequence of instructions
- write and test simple programs
- use logical reasoning to predict and computing the behaviour of simple programs
- organise, store, manipulate and retrieve data in a range of digital formats
- Communicate safely and respectfully online, keeping personal information private, and recognise common uses of information technology beyond school.

By the end of key stage 2 pupils should be taught to:

- design and write programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts.

- use sequence, selection, and repetition in programs; work with variables and various forms of input and output; generate appropriate inputs and predicted outputs to test programs

- use logical reasoning to explain how a simple algorithm works and to detect and correct errors in algorithms and programs

- understand computer networks including the internet; how they can provide multiple services, such as the world-wide web; and the opportunities they offer for communication and collaboration

- describe how internet search engines find and store data; use search engines effectively; be discerning in evaluating digital content; respect individuals and intellectual property; use technology responsibly, securely and safely

- Select, use and combine a variety of software (including internet services) on a range of digital devices to accomplish given goals, including collecting, analysing, evaluating and presenting data and information.

Online Safety KS1/KS2

Children learn why it is important to stay safe online. In the same way children learn about safety when they leave the house, it is important they learn how to stay safe online as these are important life skills.

Most of children are 'connected' via laptops, mobile phones, tablets or personal computers. The potential for the internet to be a valuable and a fun resource for entertainment, making friends, keeping in touch and learning is huge. However using internet, could put children at risk of illegal activity or abuse. (Please refer to the Online Safety Policy)

Planning

The curriculum map and scheme of work sets out the knowledge, skills and understanding to be taught, along with suggested activities. This will ensure coverage of the National Curriculum, progression of skills, knowledge and understanding, and the use of computing in all subject areas.

Resources

The school acknowledges the need to continually maintain, update and develop its resources and to make progress towards a consistent, compatible pc system by investing in resources that will effectively deliver the strands of the national curriculum and support the use of ICT and computing across the school. Teachers are required to inform the ICT and computing coordinator of any faults as soon as they are noticed. Resources if not classroom based are located in the server room and computing suite. A service level agreement with entrust is currently in place to help support the coordinator to fulfil this role both in hardware & audio visual.

Resources (continued…)

ICT and computing network infrastructure and equipment has been sited so that:

- Every classroom from nursery to y6 has a PC connected to the school network, a tablet for assessment purposes, an interactive whiteboard with sound, DVD and video facilities, digital viewer and a digital camera.
- There is a computing suite of 31 desktops.
- There is a tablet trolley in school containing 15 LearnPads with internet access available to use in classrooms.
- Each class from nursery to year 6 has an allocated slot in the computer suite timetable for the teaching of specific computing skills and/or cross curricular activities.
- The computing suite and LearnPads are available for use throughout the school day as part of computing lessons and for cross curricular use.
- The school has a computing technician who is in school one afternoon every week.
- Other resources available are: mini video recorders, recording and listening stations, control devices (e.g. Beebots) and digital microscopes. The hall and library computers are networked and connected to a projector and sound system.

Planning

The curriculum map and scheme of work sets out the knowledge, skills and understanding to be taught, along with suggested activities. This ensures coverage of the National Curriculum, progression of skills, knowledge and understanding, and the use of computing in all subject areas.

Staff will use schemes of work and medium term planning to produce weekly plans. The curriculum co-ordinator over sees these plans.

Differentiation by task, support or outcome will be used to support and extend all children. Short focussed tasks will be used for children to consolidate or enrich skills learned. Some children will have particular learning requirements which go beyond the provision for that age range; these may include G&T children, SEND or those who have EAL. Teachers must take account of these requirements and plan, where necessary, to support individuals or groups of pupils to enable them to participate effectively in the curriculum activities.

Each subject co-ordinator will also incorporate computing activities in his/her own scheme of work and is jointly responsible, with the ICT co-ordinator, for their implementation and monitoring.

Assessment

Teachers regularly assess capability through observations and looking at completed work. Key objectives to be assessed are taken from the national curriculum to assess key computing skills each term. Assessing computing work is an integral part of teaching and learning and central to good practice. It should be process orientated - reviewing the way that techniques and skills are applied purposefully by pupils to demonstrate their understanding of the concepts of computing.

Once the children complete a unit of work, a summary judgement of the work for each pupil is used to assess whether they have yet to meet, met or exceeded the expectations of the unit/stage objectives. Computing work is saved on the school network. Other work may be included in topic work books within the subject from which the task was set.

Monitoring & Review

The computing co-ordinator is responsible for monitoring and evaluating the planning and use of computing in school, providing support, organising training and arranging whole school INSET when appropriate.

The computing co-ordinator is responsible in conjunction with the computer support technician for monitoring the condition of computing equipment in school and organising repair/ replacements as and when it is necessary. Together with the ICT team the co-ordinator should plan ahead to ensure the continuous updating of equipment and resources.

The computing co-ordinator is responsible for the budget, reviewing and updating the computing and online safety policies and the schemes of work. The co-ordinator should carry out a subject scrutiny and observe teaching and learning.

Whenever a curriculum is reviewed, as part of staff or curriculum development, the use of ICT in that particular subject will be an integral part of the training/planning.

The subject leader is responsible for monitoring the standard of the children's work and the quality of teaching in line with the schools monitoring cycle. This may be through lesson observations and saved work.

SEND

For children with SEND, computing can provide a means of reinforcing concepts and knowledge. Computing has excellent motivational potential for children experiencing learning difficulties or behavioural problems, for example using a word processing programme supports presentational skills and a spell check may help with spellings. To fully consolidate their skills, SEND children may require greater access to computing in short, frequent sessions.

HARMONDSWORTH PRIMARY SCHOOL

LONDON BOROUGH OF HILLINGDON

Equal Opportunities

Harmondsworth Primary School will ensure that all children are provided with the same learning opportunities regardless of social class, gender, culture, race, disability or learning difficulties. As a result we hope to enable all children to develop positive attitudes towards others. All pupils have equal access to ICT and computing and all staff members follow the equal opportunities policy. Resources for SEND children and gifted & talented will be made available to support and challenge appropriately.

Ngaire Hepworth
Spring 2016

Online Safety Policy

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety <u>must</u> follow the school's safeguarding and child protection processes.

Contents

1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy is communicated to staff/pupils/community
- Handling complaints
- Reviewing and Monitoring

2. Education and Curriculum

- Pupil online safety curriculum
- Staff and governor training
- Parent awareness and training

3. Expected Conduct and Incident Management

4. Managing the IT Infrastructure

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

5. Data Security

- Management Information System access
- Data transfer
- Asset Disposal

6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video

Appendices (separate documents):

A1:   Acceptable Use Agreement (Staff, Volunteers and Governors)

A2:   Acceptable Use Agreements (Pupils – adapted for phase)

A3:   Acceptable Use Agreement including photo/video permission (Parents)

A4:   Protocol for responding to online safety incidents
http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx - handling infringements
http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf - page 23 onwards

A5:   Prevent: Radicalisation and Extremism

A6:   Data security: Use of IT systems and Data transfer

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

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 Harmondsworth Primary 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
- Lifestyle websites promoting harmful behaviours
- Hate content
- 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)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

HARMONDSWORTH PRIMARY SCHOOL

London Borough of Hillingdon

Scope

This policy applies to all members of Harmondsworth Primary School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Harmondsworth Primary School IT systems, both in and out of Harmondsworth Primary 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 appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services
	• To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
	• 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 pupils, including risk of children being radicalised
	• To receive regular monitoring reports from the Online Safety Co-ordinator
	• 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	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • To communicate regularly with SLT and the designated online 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 online safety incident • To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise 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.
Governors/Safeguarding governor (including online safety)	• To ensure that the school has in place policies and practices to keep the children and staff safe online • 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

Role	Key Responsibilities
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 • 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 • To ensure appropriate backup procedures and 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 (IAOs)	• 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
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant
Teachers	• To embed online safety in the curriculum • 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

Role	Key Responsibilities
All staff, volunteers and contractors.	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction. • 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 **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 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.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy annually • 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 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• To read, understand and promote the school's Pupil 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 and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
External groups including Parent 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/pupils/community in the following ways:

- Policy to be posted on the Fronter/website.

- Policy to be part of school induction pack for new staff.

- Regular updates and training on online safety for all staff.

- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.

- Staff and pupils are given information about infringements in use and possible sanctions.

- Online Safety Coordinator acts as first point of contact for any incident.

- Any suspected online risk or infringement is reported to Online Safety Coordinator that day

- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

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 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 pupils.

LONDON
GRID FOR LEARNING

---

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- 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 pupil 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 pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This 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.

Parent awareness and training

This school:

- provides induction for parents which includes online safety;
- runs a rolling programme of online safety advice, guidance and training for parents.

LONDON
GRID FOR LEARNING

---

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;

- 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;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;

- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;

- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;

- all members of the school 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 (i.e. the local authority, 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;

- the Police will be contacted if one of our staff or pupils 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 IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;

- has the educational filtered secure broadband connectivity through the LGfL;

- 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)

This school

- Uses individual, audited log-ins for all users - the LGfL 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, this school:

- Ensures staff read and sign that they have understood the school's online 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;

- All pupils have a unique username and password which gives them access to Fronter/ Internet and other services;

- 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;

- 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 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.

- 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 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 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;

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.

- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.

- We require staff to use STRONG passwords.

- We require staff to change their passwords into the MIS, LGfL USO admin site, every 90 days/twice a year.

- We require staff using critical systems to use two factor authentication.

E-mail

This school

- Provides staff with an email account for their professional use, London Staffmail and makes clear personal email should be through a separate account;

- 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

- 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.

Pupils:

- We use LGfL pupil email system.

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff can only use the LA or LGfL e mail systems on the school system

- Staff will use LA or LGfL 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. '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.

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;

- 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 pupils' names when saving images in the file names or in the tags when publishing to the school website;

Cloud Environments

- 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, pupils are only able to upload and publish within school approved 'Cloud' systems.

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 student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff;

- School staff should not be online friends with any pupil/student. 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 /academy or local authority 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.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.

- Pupils are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement 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.

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

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. 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.

- All staff are DBS checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.

- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after an idle time.

- 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.

- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.

- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / SLT.

- Pupil personal mobile devices, which are brought into 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 until the end of the day.

- Mobile devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.

- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.

- Staff members may use their phones during school break times but not while on playground duty.

- All visitors are requested to keep their phones on silent.

- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.

- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.

- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Storage, Synching and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.

The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Students' use of personal devices

- The School strongly advises that pupil mobile phones and devices should not be brought into school.
- The 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 device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Staff will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities.
- 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.

- 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 and then report the incident with the Headteacher / Designated Officer.

- If a member of staff breaches the school policy then disciplinary action may be taken.

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/son 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;

- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;

- If specific pupil 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 pupil permission for its long term, high profile use

- The school blocks/filter access to social networking sites;

- Pupils are taught about how images can be manipulated in their online 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 computing scheme of work;

- Pupils 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.

- Pupils 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. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.