Hamilton Primary School

HAMILTON
PRIMARY SCHOOL

E-Safety Policy

Approved by Governors: May 2023

Review Date: May 2026

E-Safety 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 Hamilton Primary School with respect to the use of Computing based technologies.
- Safeguard and protect the children and staff of Hamilton Primary 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 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.
- 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
- Bullying or unkind messages through social media

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft 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)

Scope

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils 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.

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

Role	**Key Responsibilities**
Headteacher / Designated Child Protection Lead	● To take overall responsibility for e-Safety provision ● To take overall responsibility for data and data security (SIRO) ● To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g., LfGL Gridstor ● 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 Computing Champion ● 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) ● To liaise with the local authority and relevant agencies

Computing / E-Safety Champion	● Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents ● Promotes an awareness and commitment to e-safeguarding throughout the school community ● Ensures that e-safety education is embedded across the curriculum ● Liaises with school computing technical staff ● To communicate with SLT and the designated e-Safety Governor to discuss current issues, review incident logs and filtering/change control logs ● To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident ● To ensure that an e-Safety incident log is kept up to date ● Facilitates training and advice for all staff ● To oversee the delivery of the e-safety element of the Computing curriculum ● 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 receiving regular information about e-safety incidents and monitoring reports. ● To support the school in encouraging parents and the wider community to become engaged in e-safety activities

Computing Technician	● 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 password protection policy ● 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 computing system ● To ensure that 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 e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant ● That the use of the *network / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Computing Champion /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. ● To keep up-to-date documentation of the school's e-security and technical procedures
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, extracurricular 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 ● To ensure that pupils know procedures to follow in the event of an e-safety related incident ● To know and be aware of the school's e-safety SMART Rules (www.childnet.com)
All staff	● To read, understand and help promote the school's e-Safety policies and guidance ● To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy through the Code of Conduct ● 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 Computing Champion ● 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 including, but not limited to social media. ● To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g., email, text, mobile phones etc. ● To know and be aware of the school's e-safety SMART Rules (www.childnet.com)
Pupils	● Read, understand, sign and adhere to the Pupil Acceptable Use Policy (nb. at KS1 it would be expected that parents / carers would sign on behalf of the pupils) ● Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations ● To understand the importance of reporting abuse, misuse or access to inappropriate materials ● To know what action to take if they or someone they know feels worried or vulnerable when using online technology. ● To know and understand school policy on the use of mobile phones, digital cameras and handheld devices. ● To know and understand school policy on the taking / 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 know and be aware of the school's e-safety SMART Rules (www.childnet.com)
Parents/carers	● To support the school in promoting e-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 ● To read, understand and promote the school Pupil Acceptable Use Agreement with their children ● To access the school website in accordance with the relevant school Acceptable Use Agreement. ● To consult with the school if they have any concerns about their children's use of technology

	● To share details of e-safety issues that their children have encountered, so that learning can be shared with others.

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

- Policy to be posted on the school website and emailed to all staff
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils 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 pupil and personnel files

Issues Arising

- 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 with class teacher / Headteacher;
    - informing parents or carers;
    - removal of Internet or computer access for a period,
    - referral to LA / Police.

- Any complaint about staff misuse should be 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: Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour and Relationships policy, Personal, Social and Health Education policies.

- The school has a Computing Champion who will be responsible for document ownership, review and updates
- The e-safety policy will be reviewed regularly 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 Computing Champion 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-safety policy will be discussed in detail with all members of teaching staff.

Education and Curriculum

Pupil e-Safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on the Purple Mash Scheme of Work in accordance with the Computing curriculum. 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;
    - [for KS2] 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 upper KS2] 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 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 the school's e-safety SMART Rules.

- 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;

Staff and governor training

This school:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues.
- 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 Safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school 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;
- suggestions for safe Internet use at home;
- provision of information about national support sites for parents.

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, UK Safer Internet Centre helpline) in dealing with e-safety issues
- Monitoring and reporting of e-safety incidents takes place and contributes to developments in policy and practice in e-safety within the school.
- Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

Managing the ICT infrastructure

- **Internet access, security (virus protection) and filtering**

This school:

- Has the educational filtered secure broadband connectivity through London Grid for Learning (LGFL)
- Ensures network health through use of RM Education virus guards
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Works in partnership with the London Grid for Learning 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;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment: the school's virtual learning environment;
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Google service as a key way to direct students to age / subject appropriate web sites;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Is vigilant when conducting 'raw' image search with pupils e.g., Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that they must report any failure of the filtering systems directly to the Computing Champion
- 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 ECC.

- **Network management (user access, backup)**

This school

- Uses individual, audited log-ins for all users;
- *Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;*
- *Has additional local network auditing software installed;*
- Ensures the Systems Administrator / network manager is up-to-date with London Grid for Learning services and policies / requires the Technical Support Provider (Martin Goodwin) to be up-to-date with ECC services and policies;
- Storage of all data within the school will conform to the UK data protection requirements

To ensure the network is used safely, this school:

- Are inducted appropriately and sign to say they have received a copy of the code of conduct
- Following this, they are set-up with Internet, email access and network access.
- We provide pupils with a year-group log-in and username for use on the network.
- All pupils have their own unique G-Suite username and password which gives them access to Google Classroom

- 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;
- Provides a common Google User account for use on school iPad and Laptops to support sharing across devices;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Uses 2 Factor Authentication to access email and web services
- Laptops that are used out of school are automatically updated when re-connected to the network.
- Makes clear that staff are responsible for ensuring that any laptop or device loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any “significant personal use” as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
  e.g., projector filters cleaned by technicians, equipment installed and checked by approved Suppliers
- 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;
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote backup of critical data;
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- Staff or third-party equipment may not connect to the school Wireless Network, which requires installation of an appropriate certificate. This latter is not provided to be used on non-school equipment;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors/Interactive White Boards are maintained so that the quality of presentation remains high;
- Reviews the school computing systems regularly with regard to health and safety and security.

Password’s policy

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

E-mail

This school

- Provides staff with an email account for their professional use;
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- 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.
- Care must be taken to ensure that email addresses of other recipients are not disclosed in emails - BCC should be used to prevent other recipients' emails addresses.

Pupils:

- Pupils are introduced to, and use e-mail as part of the 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 email, 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 school Agreement Form 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.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school website complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, 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. 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 networking

- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils.

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 the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, pupil's & parents' or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.
- Pupil mobile phones which are brought into school must be turned off (not placed on silent) and given to the class teacher. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times. All visitors are requested to keep their phones on silent.
- 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 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.

Pupils' use of personal devices

- The school advises that pupil mobile phones 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 pupil 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.
- 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.

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 child 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
- 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 website, in the prospectus or in other high-profile publications the school will obtain individual parental or pupil 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;
- Pupils are taught about how images can be manipulated in their eSafety 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, 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.

Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.