Hampton
Primary
Partnership

Hampton Infant School and Nursery

Online Safety Policy

Version	Date	Review date	Comments
1	Feb '14		New policy – shared with all staff
2	July '18	July '20	Amendments in line with new structure

Online Safety Policy

Introduction

Technology is developing at an increasing rate and, year on year, impacts the lives of citizens and education. While developing technology brings many opportunities, it also brings risks and potential dangers. Through our Online Safety Policy we aim to reduce the risk to our pupils by:

- Protecting and educating pupils and staff in their use of technology.
- Outlining appropriate mechanisms to intervene and support any online safety incidents at home or in school.
- Providing clear advice and guidance on how to minimise risks and how to deal with any infringements of school policy.

The policy applies to all members of the school community both within and outside of school. The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to online safety. This policy relates to other policies including Behaviour, Safeguarding, Health and Safety and Facebook.

.

Responsibilities

At Hampton Infant School and Nursery (HISN) we believe that all staff and children have a **shared responsibility for online safety** and that ICT usage by all network users is safe and secure. The Leadership team, with the support of the Governing Body, aims to embed safe practices into the culture of the school. The Leadership team ensures that the policy is implemented and compliance with the policy is monitored.

Our Designated Safeguarding Lead, Claire Tester, and our Deputy Designated Safeguarding Lead, Helen Lockey, ensures they keep up to date with online safety issues and guidance through organisations such as LGfL & Child Exploitation and Online Protection (CEOP). The Designated Safeguarding Lead ensures the senior leadership, staff and Governors are updated as necessary.

Governors have an overview understanding of online safety issues and strategies at HISN. The Designated Safeguarding Lead will update the Governing Body at least once a year to ensure that governors are aware of changes in local and national guidance.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms. All staff are required to sign the school's Acceptable Use Agreement (see Appendix A). The signed copies are kept in the individual member of staff's file and a copy is available in the staffroom to refer to if necessary. Staff are reminded / updated about online safety issues at least once a year.

Managing Access to the Internet

The school takes all reasonable precautions to prevent access to inappropriate material. We have a managed system which we feel enables our children to understand how to deal with online safety incidents. This system is managed through Richmond Borough. As such, the school internet feed is filtered through LGfL (London Grid for Learning). However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

All users have a responsibility to report immediately to class teachers / the Leadership team any infringements of the school's filtering system of which they become aware or any sites that are accessed, which they believe should be blocked.

Pupils are made aware of the importance of filtering systems through the school's Online Safety Curriculum.

Staff users will be made aware of the filtering systems through the Acceptable Use Agreement (as part of their induction process) and through briefing in staff meetings, training days, memos etc

Parents play an essential role in the education of their children and in the monitoring and regulation of the children's online experiences. The school will therefore seek to provide information and awareness to parents and carers through the Acceptable Use Agreement, letters, newsletters, web site and parents' evenings etc

In order to provide safe access to the Internet, staff and governors will ensure that every reasonable measure is taken.

The following safe guards are in place:

- The school e-safety Coordinator will keep up to date with e-safety issues and guidance through liaison with the Local Authority e-safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP).
- The school's e-Safety coordinator ensures the Head, Senior Management and Governors are updated as necessary.
- Educational filtered secure broadband connectivity through the LGfL connects to the 'private' National Education Network.
- The LGfL filtering system blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
- Adults in school will report immediately to the ICT co-ordinator any sites deemed unsuitable. The ICT coordinator will report these sites to the school service provider for blocking.
- Use of Sophos anti-virus software (from LGfL) and network set-up ensures staff and pupils cannot download executable files.
- LA and LGfL approved systems such as S2S, USO FX and secured email are used to send personal data over the Internet and secure remote access is available were staff need to access personal level data off-site.

- All Chat rooms and social networking sites (except those that are part of an educational network or approved Learning Platform) are blocked.

- Staff are provided with an LGfL staffmail email account for their professional use and are made aware that personal email should be through a separate account.

- All e-mails are filtered for inappropriate language and pictures.

- Highly restricted (Safe mail) or simulated environments for e-mail are used from Year 2 for pupils to experience online communication. All e-mails sent and received by children are supervised.

- Individual, audited log-ins are used by all users - the London USO system.

- Only LGfL / NEN services are used for video conferencing activity.

- Only approved or checked webcam sites are used.

- Working in partnership with the LGfL, the school will ensure any concerns about the system are communicated so that systems remain robust and protect students.

- The systems Administrator / network manager is expected to remain up-to-date with LGfL services and policies.

- The Technical Support Provider is expected to remain up-to-date with LGfL services and policies.

Adults Use of the Internet

- Staff are provided with details for logging into the school network. These details are not to be shared and any visitors, volunteers or supply teachers must be logged into the system using the visitor login.

- Staff must **lock** classroom computers before leaving the room and **log off** any computers at open workstations once they have finished working on them.

- The ICT coordinator and School Business Manager will ensure that all staff have been shown how to send or receive sensitive and personal data via USO FX and understand the requirement to encrypt data where the sensitivity requires data protection.

- The e-safety coordinator will make e-safety training available annually to staff and ensure that it is provided for new staff upon joining the school.

- All staff are responsible for promoting and supporting safe behaviours in their classrooms and following school e-safety procedures.

- All staff and relevant visitors or volunteers must sign an e-safety /Acceptable Use Agreement form which will be kept on file.

- All staff are made aware of what the ‘rules of appropriate use’ are and what sanctions result from misuse – through staff meetings and INSET.

- All staff must preview any websites before use in lessons.

- All staff must remain vigilant when conducting ‘raw’ image search with pupils e.g. Google or Lycos image search.

- All staff must report any failure of the filtering systems directly to the designated e-safety coordinator who will log and escalate as appropriate to the Technical service provider or LA e-safety officer.

- The designated person for Safeguarding has appropriate training.

- Staff are given advice and information on reporting offensive materials, abuse/ bullying etc.

- The school will immediately refer any material suspected of being illegal to the appropriate authorities, police and the LA.

- All staff are made aware that Internet use and email content is monitored.

- Although YouTube may be accessed through the school’s network, videos must be downloaded and may not be shown to pupils directly from the YouTube website.

Teaching and Learning

The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school’s management information and business administration systems. Access to the Internet is a necessary tool for staff and students. It helps to prepare students for their on-going career and personal development needs. Internet use enhances learning and is planned to enrich and extend learning activities. Staff select sites which support the learning outcomes planned for pupils’ age and maturity.

As part of the Computing National Curriculum, pupils should be taught to “use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour and identify a range of ways to report concerns about content and contact.” Therefore, we have a planned and progressive curriculum that also incorporates the Ofsted ‘Keeping Children Safe in Education’ guidelines September 2016.

Online Safety education will be provided in the following ways:

- A planned Online Safety programme will be provided as part of Computing, PHSE and other lessons and will be regularly revisited. This will cover both the use of ICT and new technologies in school and outside school.
- Key online safety messages should be reinforced through further input via assemblies (Safer Internet Day) and pastoral activities as well as informal conversations when the opportunity arises.

- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use of ICT both within and outside school.
- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information they find.

Managing Internet Access

The school ICT system security is reviewed regularly. Virus protection is updated regularly. Security strategies are discussed with the Local Authority.

Pupils are allowed to use school email accounts only. Pupils must tell a teacher immediately if they receive offensive email. In emails, pupils are taught that they must not reveal their personal details, those of others or arrange to meet anyone without specific permission. Pupils are taught not to open suspicious incoming email or attachments. The forwarding of chain letters is not permitted.

Passwords

Staff and pupils should always keep their passwords private, must not share with others and 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. We require staff to use strong passwords and to change their passwords twice annually when prompted to do so. Staff using critical systems are required to use two factor authentication.

E-mail

E-mail is now an essential means of communication for staff at HISN. We:

- Use the LGfL email on the school system for professional purposes.
- Do not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for any communication with the wider public.
- Contact the police if one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law.
- Manage accounts effectively, with up to date account details of users.
- May block access in school to external personal email accounts.
- Do not use email to transfer staff or pupil personal data unless anonymised.
- Teach pupils about the online safety of using e-mail both in school and at home.

The school website

The Head of School 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. Children's photographs are only allowed to go on the website if written permission is held from the child's parents. The contact details on the website are for school admin only.

Social networking and personal publishing

Reference should not be made in social media to students/pupils, parents/carers or school staff. School staff should not be online friends with any current or former pupil/student nor should they 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 and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute.

Pupils will not be allowed to access public chat rooms. New applications are thoroughly tested before pupils are given access. Pupils are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our Online Safety Curriculum. Students are required to sign and follow our pupil Acceptable Use Agreement.

The Head of School ensures that occasional checks are made to certify that the filtering methods selected are effective in practice. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Headteacher or the Computing Lead.

Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement. Parents are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

Mobile Devices

Currently, our policy is that members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Pupils are not currently permitted to bring their personal hand held devices into school. 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.

The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided. If a personal mobile device is used for such matters, the image or recording needs to be downloaded and fully removed from the mobile device the same day. 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.

The sending of any abusive or inappropriate messages is forbidden. Consequences in accordance with our Behaviour Policy will be adhered to in such incidences.

Use of digital and video images

- When using digital images, staff should teach children to recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Pupils must not take, use, share, publish or distribute images 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.

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement when their daughter / son joins the school.
- Staff sign the school's Acceptable Use Agreement.
- The school blocks/filters access to social networking sites unless there is a specific approved educational purpose.
- 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.

Data Security

Staff must report any incidents where data protection may have been compromised to the Head of School. We ensure staff know who to report such incidents to.

Staff have secure area(s) on the network to store sensitive files. We require staff to logout of systems when leaving their computer, but also enforce lock-out after 30 minutes idle time. All servers are managed by DBS-checked staff.

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.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Staff must not keep confidential information on removable devices such as USB devices unless suitably security protected.

Staff training

It is essential that all staff receive online safety training and understand their responsibilities, including ensuring that they fully understand the school's Online Safety Policy and Acceptable Use Agreements which are signed as part of their induction. The Designated Safeguarding Lead will also provide advice, guidance and training as required to individual. Governors should also take part in online safety training / awareness sessions.

Acceptable Use Agreement

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate Acceptable Use Agreement, which they will be expected to sign before being given access to school systems.

Acceptable Use Agreements are revisited annually, and amended if necessary (requiring resigning), in light of new developments.

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to unsuitable content or which promote any kind of discrimination.

The school's Online Safety Policy and its implementation will be monitored and reviewed on a regular basis.

Complaints of internet misuse, including staff misuse, must be referred to the Head of School. Complaints of a child protection nature must be dealt with in accordance with our

Safeguarding Policy. Pupils and parents are informed of the complaints procedure. Pupils and parents are informed of the consequences for pupil misuse.

Failure to comply with our Acceptable Use Policy, either in or outside of school, will require the children involved and their parents to meet with the Head of School, potentially receiving consequences in accordance with our Behaviour Policy.

Responding to online incidents and safeguarding concerns.

- The Designated Safeguarding Lead (DSL) will be informed of any online safety incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- Parents and children will need to work in partnership with the school to resolve issues.

APENDIX A – Pupils e-safety/Acceptable Use Agreement form
APENDIX B – Staff e-safety/Acceptable Use Agreement form
APENDIX C – Visitor and Volunteer e-safety/Acceptable Use Agreement form

Hampton Infant School and Nursery

Pupils' E-Safety / Acceptable Use of Technology Agreement

My technology promise:

- I will only use computers, Beebots or other kinds of school technology when I have a teacher's permission.
- I will only open programs or files that I know I am allowed to open.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will not make or write anything on the computer that could upset somebody else.
- I will tell a teacher or suitable adult if I see something on the screen that upsets me.
- I will take care of the computers and other equipment.
- I know that if I break the rules I might not be allowed to use a computer.

Signed (child) ____________________________________

Full name ____

By signing this agreement, I give permission for my child to use various forms of technology at school and access suitable internet resources under adult supervision.

I agree that any photographs I take at school events containing children other than my own will not be shared on any social networking sites.
Signed (parent): ____________________________________

Hampton Infant School and Nursery

E-Safety / Acceptable Use of Technology Agreement for Staff

- I have read and agree to abide by the contents of the school's e-safety policy.
- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not reveal my password(s) to anyone.
- I will not allow unauthorised individuals to access email / Internet / extranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will only use the approved, secure email system(s) for any communication related to my professional responsibilities.
- I will only use the approved school email, school Learning Platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to the headteacher or e-safety coordinator on request.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the e-safety coordinator.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided. If a personal mobile device is used for such matters, the image or recording needs to be downloaded and fully removed from the mobile device the same day. Any photographs taken at school using a personal camera will be downloaded and remain at school. I will not store pupil images at home without permission.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role and bring neither myself nor the school into disrepute.

- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will access school resources remotely (such as from home) only through the LGfL / school approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching. (teaching staff)
- I will alert the school's Designated Safeguarding Person if I feel the behaviour of any child I teach may be a cause for concern.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to the headteacher or Designated Safeguarding Person.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Signed ____ date _____________________

Hampton Infant School and Nursery

E-Safety / Acceptable Use of Technology Agreement for Visitors and Volunteers

- I have read and agree to abide by the contents of the school's e-safety policy.
- I will log into the school network using only the visitor password with which I have been provided.
- I will only use the school's digital technology resources and systems for purposes specifically related to the reason for my visit to the school.
- I will not use the school network for the sending or receiving of personal emails.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to the headteacher or e-safety coordinator on request.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the e-safety coordinator.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I agree and accept that I am not permitted to take photographs of children using mobile telephones. Any photographs taken at school using a personal camera will be downloaded and remain at school. I will not store pupil images at home.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will uphold the school's e-safety curriculum in my dealings with pupils.
- I will alert the school's Designated Safeguarding Person if I feel the behaviour of any child I work with may be a cause for concern.

Signed ____ date _____________________