Hampton Infant School and Nursery

E-Safety Policy 2013/14

Drafted the e-safety coordinator and Senior Management Team *February 2014*

The school's Designated E-safety Coordinator is Lynn Bima

The school's Designated Safeguarding Member of Staff is Beth Hoare

Introduction

Technology offers unimaginable opportunities and is constantly evolving. Access is becoming universal and increasingly more mobile and pupils are using technology at an ever earlier age. This increased use of technology at work and at home exposes people to a number of risks and dangers. In *the Review of Primary Education*, Sir Jim Rose states that "used well, technology strongly develops the study and learning skills children need now and in the future, including the fundamentals of 'e-safety'." It is important to protect our pupils through the access that they are given but it is also vital to equip them with the skills to handle this technology safely.

This policy applies to all users of ICT equipment, in its widest sense, whilst on school premises. It also applies to anyone who uses school ICT equipment, software or electronic data whilst off the premises.

Rational for using the internet in school

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

- The internet enables staff to access a rich variety of resources, remain up to date with new developments and network with other professionals in the world of education.

- The Early Years Foundation Stage Curriculum expects pupils to "Find out about and identify the uses of everyday technology and use information technology and programmable toys to support their learning".

- The statutory Key Stage 1 Computing curriculum expects pupils to "learn how to use technology purposefully to create, organise, store, manipulate and retrieve digital content".

Definition of e-safety

In its simplest form e-safety is about ensuring that adults and children use electronic technologies in a way which will keep them safe without limiting their opportunities for creativity and innovation. E-safety is also about protecting the hardware and software we use from attack by unscrupulous people, who may wish to cause disruption or commit illegal acts.

The breadth of issues classified within e-safety is considerable. OFSTED refers to three areas of risk categorised in the 2008 Byron review, *Safer children in a Digital World*.

- **content:** being exposed to illegal, inappropriate or harmful material
- **contact:** being subjected to harmful online interaction with other users
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

The school aims to address each of these risks through managing the technology with which pupils may come into contact, informing them of potential and relevant dangers and by equipping them with confidence and skills to make responsible choices to keep themselves and others safe.

Managing Access to the Internet

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.

Pupils' Use of the Internet:

- Staff are vigilant in their supervision of pupils' use of the internet at all times, as far as is reasonable.

- Staff will preview websites before directing pupils to access them. Pupils will access websites directly via links on the HISN Intranet page.

- All pupils in Key Stage 1 must individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme.

- Pupils' parents/carers are made aware of the pupils' e-safety / acceptable use agreement form which they must also sign, thereby giving consent for pupils to use the Internet, as well as other ICT technologies.

- The 'rules of appropriate use' will be explained to all pupils.

- Pupils only publish material within the appropriately secure school's learning environment, such as the platforms provided by LGfL.

- HISN fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable or upsets them.

E-safety in the Computing Curriculum

The National Curriculum requires that pupils in Key Stage 1 "use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies."

Hampton Infant School and Nursery has a clear, progressive e-safety education programme throughout Key Stages 1, based on local authority and national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience. Pupils are encouraged to STOP and THINK before they CLICK

Early Years

- Pupil computers are logged into the school network using the Reception pupil login.
- Pupils access programs from desktop icons.
- Online resources accessed for Reception pupils to use independently must come from LGfL

Year 1

Pupils are taught, and practice, the following good habits for keeping safe online:

- Pupils log into the school network using the KS1 pupil login.
- Pupils are taught the significance of a password and are encouraged to keep passwords secret.
- Individual unique pupil passwords are used for online resources such as BugClub, Purple Mash and some LGfL resources.
- Pupils are encouraged to tell an adult if they encounter something on the screen which they don't expect or something that upsets them.
- Pupils publish material using LGfL J2E using their first names only.

.

Year 2

In addition to what they have learnt in Year 1:

- Pupils are introduced to possible online dangers and how to stay safe on the internet through the *Hector's World* resources available through CEOPS. Lessons help pupils to:
    - Understand why on-line 'friends' may not be who they say they are
    - Understand why we do not sharing personal information online
    - Understand the public nature of material shared online
    - Understand that material published online cannot always be easily removed
    - Understand how to safely communicate with a 'stranger' online
    - Pupils are taught specific strategies for dealing with online materials which are hurtful or worrying
- Pupils practice commenting responsibly on each other's' published work.
- Pupils send and receive emails with class teachers using *London Mail.*

Parents and e-safety

HISN will make efforts to engage with parents over e-safety matters through a rolling programme of advice, guidance and training for parents, including:

- Information leaflets, in school newsletters and on the school web site
- demonstrations, practical sessions held at school
- distribution of 'think u know' materials for parents
- suggestions for safe Internet use at home
- provision of information about national support sites for parents.

Class teachers and the e-safety coordinator will ensure that parents/carers have signed and returned their child's e-safety/Acceptable Use Agreement form.

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

This policy should we read in conjunction with:

- Behaviour and Anti-Bullying policy
- SEN policy
- Curriculum policy
- HJS e-safety policy

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) _____

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.
- 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 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 _____