Name of School	Hanover Primary School
Policy review Date	March 2012
Date of next Review	March 2013
Who reviewed this Policy?	Richard Thackray

e-Safety Policy

Contents:

Overview

Managing the Internet safely

Managing e-mail safely

Using digital images and video safely

Using the school network, equipment and data safely

Infringements and possible sanctions

Our e-Safety Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance. It has been agreed by the senior management and will be approved by Governors. It will be reviewed annually. This policy is written, and should be read, in conjunction with the school ICT Policy.

Created by: Frankie McGowan

The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / http://www.hi5.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

2. Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for pupils, staff and parents.

Reference: Becta - E-safety Developing whole-school policies to support effective practice [1]

3. Roles and Responsibilities

e-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and in compliance with the Policy monitored.

Our school **e-Safety Co-ordinator** is Damien Parrott

Our e-Safety Coordinator ensures they 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)[2]. The school's e-Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance [3] on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;

[1] http://schools.becta.org.uk/index.php?section=is

[2] http://www.ceop.gov.uk/

[3] Safety and ICT - available from Becta, the Government agency at: http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_str_02&rid=10247

- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of pupil information/photographs and use of website;
- eBullying / Cyberbullying procedures;
- Their role in providing e-Safety education for pupils;

In whole school staff INSET days, staff are reminded / updated about e-Safety matters at least once a year.

4. How will complaints regarding e-Safety be handled?

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:

- Discussion with e-Safety Coordinator / Headteacher;
- Informing parents or carers;
- Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- Referral to LA / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was revised by: … … … … ……………………
- It was approved by the Governors on: … … …………………………

INTERNET

Why Internet use is important

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

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- When appropriate the school will use 'safer' search engines with pupils such as http://yahooligans.yahoo.com/ | http://www.askforkids.com/ and activates 'safe' search where appropriate;
- The school Is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search;
- Pupils only publish within appropriately secure learning environments such as their own closed secure LGfL portal or Learning Platform

Education programme:

This school:

- 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;
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or e-safety co-ordinator
- Pupils are taught how to evaluate Internet content and to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- **E-safety** is taught using the CEOP **www.thinkuknow.co.uk/cybercafe** at Key Stage 1 and 2
- We deliver support to parents who have an important role in supporting safe and effective use of the Internet by pupils
- Makes training available annually to staff on the e-safety education program;
- Ensures pupils and staff know what to do if a cyber-bullying or other e-safety incident occurs;

Managing Internet Access

Information system security

This school:

- Maintains broadband connectivity through the LGfL and so connects to the National Education Network;
- Ensures virus protection will be updated regularly.
- Uses class log-ins for pupils

We use the pan-London LGfL / Synetrix filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature; Informs staff and students that that they must report any failure of the filtering systems directly to the [*system administrator / teacher / person responsible for URL filtering]*. Our systems administrators report to LA / LGfL where necessary.

This school:

- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only uses LGfL for pupil's own online creative areas such as web space and ePortfolio;
- Only uses the LGfL service for video conferencing activity;
- Only uses approved blogging or discussion sites, such as on the LGfL / approved Learning Platform and blocks others.
- Only uses approved or checked webcam sites;

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.

EMAIL

Pupils:

- We only use LGfL 'safemail' with pupils.
- Pupils can only use the LGfL / school domain e-mail accounts on the school system.
- Pupils are introduced to, and use e-mail as part of the ICT scheme of work.

Staff

- Staff can use the LGfL / school domain e-mail accounts or web-based email for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

IMAGES

- Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- We do not use pupils' names when saving images in the file names
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- All 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;
- Pupils are only able to publish to their own 'safe' web-portal on the LGfL in school;
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are taught about how images can be abused in their eSafety education programme;
- 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;

USING THE SCHOOL NETWORK AND EQUIPMENT

This school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;
- Provides pupils with a class network log-in username;
- Makes it clear that staff must keep their log-in username and password private and must not leave them where others can find;
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Makes clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or 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;
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day

- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.

How will infringements be handled?

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

The following are provided as exemplification only:

Students

Category A infringements:

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

[Possible Sanctions: referred to class teacher / tutor / senior manager / e-Safety Coordinator]

Category B infringements:

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups
- Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

[Possible Sanctions: referred to Class teacher/ Head of Department / Year tutor / e-safety Coordinator / removal of Internet access rights for a period / removal of phone until end of day / contact with parent]

Category C infringements:

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

[Possible Sanctions: referred to Class teacher / e-safety Coordinator / Headteacher / removal of Internet and/or Learning Platform access rights for a period / contact with parents / removal of equipment]

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform LA / Synetrix as appropriate

Category D infringements:

- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

[Possible Sanctions* – Referred to Head Teacher / Contact with parents / *possible exclusion / removal of equipment / refer to Community Police Officer / LA e-safety officer]

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider

<u>Staff</u>

Category A infringements (Misconduct):

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

[Sanction - referred to line manager / Headteacher/ warning given.]

Category B infringements (Gross Misconduct):

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

[Sanction – Referred to Headteacher / Governors and follow school disciplinary procedures; report to LA Personnel/ Human resources, report to Police]

Other safeguarding actions:

1. Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
2. Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
3. Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child Pornography found?

In the case of Child Pornography being found, the member of staff should be **immediately suspended** and the Police should be called: see the free phone number **0808 100 00 40** at: http://www.met.police.uk/childpornography/index.htm

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's e-safety / Acceptable Use Policy.;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate acceptable use form;
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on e-safety issues, (see LGfL safety site).