



E-Safety Policy and Procedures

The Acceptable Use of the Internet and Related Technologies

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 approved by Governors. It will be reviewed annually.

Monitored by the ICT Co-ordinator in conjunction with the Pastoral Care Team

Date: November 2010

Review date: November 2011

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

1. Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our children with the skills to access life-long learning and employment.

Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom 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.kazaa.com/>, <http://www.livewire.com/>)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Canonbury Primary School we have a responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school; (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobiles phones, camera phones and portable media players, etc).

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.

3. Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The position of e-Safety Coordinator will be held by the ICT Coordinator, Anna Gibbs and the Designated Member of Staff (DMS) for child protection, Diane Thompson, as the roles overlap.

Our E-Safety Coordinator will ensure that 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)¹. The school's E-Safety coordinator will ensure that the Head, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of E-Safety issues and strategies at Canonbury. We ensure our governors are aware of our local and national guidance² on E-Safety and are updated at least annually on policy developments. The Pastoral and Community committee review this annually looking at a spreadsheet of signed agreements from staff and pupils.

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 'Telling School' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff will be made familiar with the schools' E-Safety 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;
 - 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;

All Staff (all teachers, supply staff and teaching partners) are reminded / updated about E-Safety matters at least once a year.

4. Handling E-Safety Complaints

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.

⁵ <http://www.ceop.gov.uk/>

⁶ 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

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. Any complaint about Headteacher misuse will be referred to the Chair of Governors.

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.

Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach e-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- 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.

Education programme

Canonbury Primary School:

- Fosters a 'Telling School' culture 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 at Key Stage 2.
- Ensures pupils and staff know what to do if a cyber-bullying or other e-safety incident occurs;

Managing Internet Access

1. Information system security

This school:

- Ensures virus protection will be updated regularly.
- Uses class and individual log-ins for pupils

We use the a 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 ICT Co-ordinator who then informs system administrator. Our systems administrators report to the Headteacher 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 approved blogging or discussion sites, such as on the LGfL / approved Learning Platform and blocks others.
- Only uses approved or checked webcam sites;

2. Authorising Internet access

EMAIL

- Pupils maybe introduced to, and use e-mail as part of the ICT scheme of work.

STAFF

- Staff can use the 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;
- 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 E-Safety education programme;

USING THE NETWORK AND EQUIPMENT

This school:

- Ensures staff 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.
- 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.

Handling Infringements

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 Headteacher or the Governors in the case of the Headteacher.

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

Category A Sanctions:

- Referred to class teacher
- *Referred to SLT if deemed serious or child protection issue

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 sites such as instant messaging / chatrooms, social networking sites.
- 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

Category B Sanctions

- Referred to class teacher, senior teacher and E-Safety coordinator. Next steps/consequences agreed by both.

- If deemed more serious, in consultation with HT/DHT/Senior teachers
- Parents informed.

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

Category C Sanctions:

- Referred to class teacher, senior teacher and E-Safety coordinator. Next steps/consequences agreed by both.
- If deemed more serious, in consultation with HT/DHT/Senior Teachers
- Parents informed.
- Removal of Internet and/or Learning Platform access rights for a period.
- Removal of equipment if applicable.

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

Category D Sanctions:

- Referred to class teacher, Senior Teacher and E-Safety coordinator. Next steps/consequences agreed by both.
- If deemed more serious, in consultation with HT/DHT
- Parents informed.
- Removal of Internet and/or Learning Platform access rights for a period.
- Removal of equipment if applicable.
- Refer to LA E-Safety officer and/or Community Police Officer.

Other safeguarding actions:

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

Staff

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

Category A Sanctions:

- Referred to Line Manager and E-Safety officer.
- If deemed more serious, referred to Headteacher and 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.

Category B Sanctions:

- Referred to Deputy/Headteacher.
- Governors informed and to follow school disciplinary procedures.
- Report to LA Personnel/Human Resources.
- Report to Police if appropriate.

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.

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

Informing staff and students of our procedures.

- They will be fully explained and included within the school's E-Safety / Acceptable Use Policy. All staff will be required to sign the school's e-safety policy acceptance form; that is kept in the school office.
- 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 E-Safety / acceptable use form;
- The school's e-safety policy will be made available and explained to parents, who will sign an acceptance form; that is kept in the school office when their child starts at school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.