COPENHAGEN PRIMARY SCHOOL

Where learning's an adventure

Computing, E-safety & Acceptable Usage Policy

	Name	Signature	Date
Prepared by:	Harsha Patel	Hatel.	4/1/2016
Checked and Reviewed by:			
Approved by:	Name: Chair of Governing Body		
Document Title:	Policy – Computing Policy		
Version Number:	2	Date of Next Review:	

This document contains Copenhagen Primary School's Policy for **Computing, E-safety & Acceptable Use.** It is intended for staff and children use.

Policy Contents

Policy Expectations and Standards Brief

Technical and Infrastructure approaches

This school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;

- Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;

- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;.

- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc and network set-up so staff and pupils cannot download executable files;

- Uses individual, audited log-ins for all users - the London USO system;;

- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;

- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;

- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;

- Only uses the LGfL / NEN service for video conferencing activity;

- Only uses approved or checked webcam sites;

- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;

- Uses security time-outs on Internet access where practicable / useful;

- Provides *highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils*; Uses Londonmail with students as this has email content control and the address does not identify the student or school;

- Provides staff with an email account for their professional use, *London Staffmail / LA email* and makes clear personal email should be through a separate account;

- *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;*

- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;

- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;

Policy and procedures

This school:

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;

- 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 the appropriately secure school's learning environment, such as the London MLE.

- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform 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; eg yahoo for kids or ask for kids

- Is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search;

- Informs users that Internet use is monitored;

- Informs staff and students that that they must report any failure of the filtering systems directly to the *teacher*. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL (Atomwide) as necessary;

- Requires pupils to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;

- Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;

- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school;

- 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;

- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;

- Ensures the named child protection officer has appropriate training;

- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents

- Provides Esafety advice for pupils, staff and parents;

- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Education and training:

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;

- Teaches pupils and informs staff what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.

- Ensures pupils and staff know what to do if there is a cyber-bullying incident;

- Ensures all pupils know how to report any abuse;

- Has a clear, progressive e-safety education programme throughout all Key Stages, built on LA / London / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

  - to STOP and THINK before they CLICK
  - to discriminate between fact, fiction and opinion;
  - to develop a range of strategies to validate and verify information before accepting its accuracy;
  - to skim and scan information;
  - 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 older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
  - to understand 'Netiquette' 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 older pupils] to understand why and how some people will 'groom' young people for sexual reasons;

- 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 observe and respect 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;

- 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 training available annually to staff on the e-safety education program;

- Runs a rolling programme of advice, guidance and training for parents, including:
  - Information leaflets; in school newsletters; on the school web site;
  - demonstrations, practical sessions held at school;
  - distribution of 'think u know' for parents materials
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents.

Section A - Copenhagen Primary School ICT Policy Overview

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, it is a schools responsibility to prepare our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based, computing hardware and mobile learning. It is also important to recognize the constant evolution of ICT within our society as a whole and how this impacts. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites

- Learning Platforms and Virtual Learning Environments

- E-mail and Instant Messaging

- Chat Rooms and Social Networking

- Blogs and Wikis

- Podcasting

- Video Broadcasting

- Music Downloading

- Gaming (including integrated chatroom servers)

- Mobile/ Smart phones with text, video and/ or web functionality

- Other mobile devices with web functionality

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 Copenhagen Primary School, we understand the responsibility to educate our children on E-Safety issues; teaching them the appropriate behaviors and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned

by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

Authorized ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorized to do so, please ask for their identification badge and contact their department. Any ICT authorized staff member will be happy to comply with this request.

Breaches

A breach or suspected breach of policy by a School employee, contractor or child may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Policy breaches may also lead to criminal or civil proceedings.

A breach or suspected breach of policy by a School employee, contractor or child may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's ICT co-ordinator or E-Safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your ICT co-ordinator.

Equal Opportunities

Pupils with Additional Needs

The school endeavors to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.
Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

Section B – Statutory Guidance and Legislation

Current Legislation

Acts Relating to Monitoring of Staff eMail

Data Protection Act 1998
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)

- unauthorised access, as above, in order to commit a further criminal act (such as fraud)

- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 2000

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, etc. and Trade Marks (Offences and Enforcement) Act 2002

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use

someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

<u>Acts Relating to the Protection of Personal Data</u>

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 200

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Section C – Framework of Acceptable use of ICT for Staff, Governors, Subsidiary Contractors and students.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB Drive, CD) must be checked for any viruses using school provided anti-virus software before using them

- Never interfere with any anti-virus software installed on school ICT equipment that you use

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider or ICT co-ordinator immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know

E-Mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognize that children need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving e-mails.

Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool This is to minimize the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

- It is the responsibility of each account holder to keep the password secure.

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes

- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

- Delete all e-mails of short-term value

- Organize e-mails into folders and carry out frequent house-keeping on all folders and archives

- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail

- Staff must inform (the eSafety co-ordinator/ ICT co-ordinator) if they receive an offensive e-mail

- Pupils are introduced to e-mail as part of the ICT Scheme of Work

- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Sending e-mails

- Use your own school e-mail account so that you are clearly identified as the originator of a message

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments

- School e-mail is not to be used for personal advertising

Receiving e-Mails

- Check your e-mail regularly

- Activate your 'out-of-office' notification when away for extended periods

- Never open attachments from an untrusted source; Consult your network manager first.

- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

- The automatic forwarding and deletion of e-mails is not allowed

E-mailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted

  - Do not send information to anybody/person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an e-mail
  - Provide the encryption key or password by a **separate** contact with the recipient(s)
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

Section D – Esafety & Incident Reporting

eSafety - Roles and Responsibilities

As eSafety 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 named eSafety co-ordinator in this school is the ICT leader who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as LB Islington LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety. The school provides opportunities within a range of curriculum areas to teach about eSafety. Pupils are educated on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum

eSafety Skills Development for Staff

- New staff receive information on the school's acceptable use policy as part of their induction

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart)

- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Managing the School eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used

- The eSafety policy will be introduced to the pupils at the start of each school year

- eSafety posters will be prominently displayed

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Senior Information Risk Owner.

Please also refer to the Infringements Escalation Policy found at **Appendix B** for clear guidelines for staff and student misconduct.

eSafety Incident Log

Some incidents may need to be recorded in other places, such as Solero, if they relate to a bullying or racist incident.

This   can   be   downloaded
http://www.thegrid.org.uk/eservices/safety/research/incident.shtml

Misuse and Infringements (see below) – Escalation Policy (Refer Appendices B)

'School name' eSafety Incident Log

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying should be recorded on the 'Integrated Bullying and racist Incident Record Form 2'

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and the **Islington Flowcharts for Managing an eSafety Incident** should be followed.
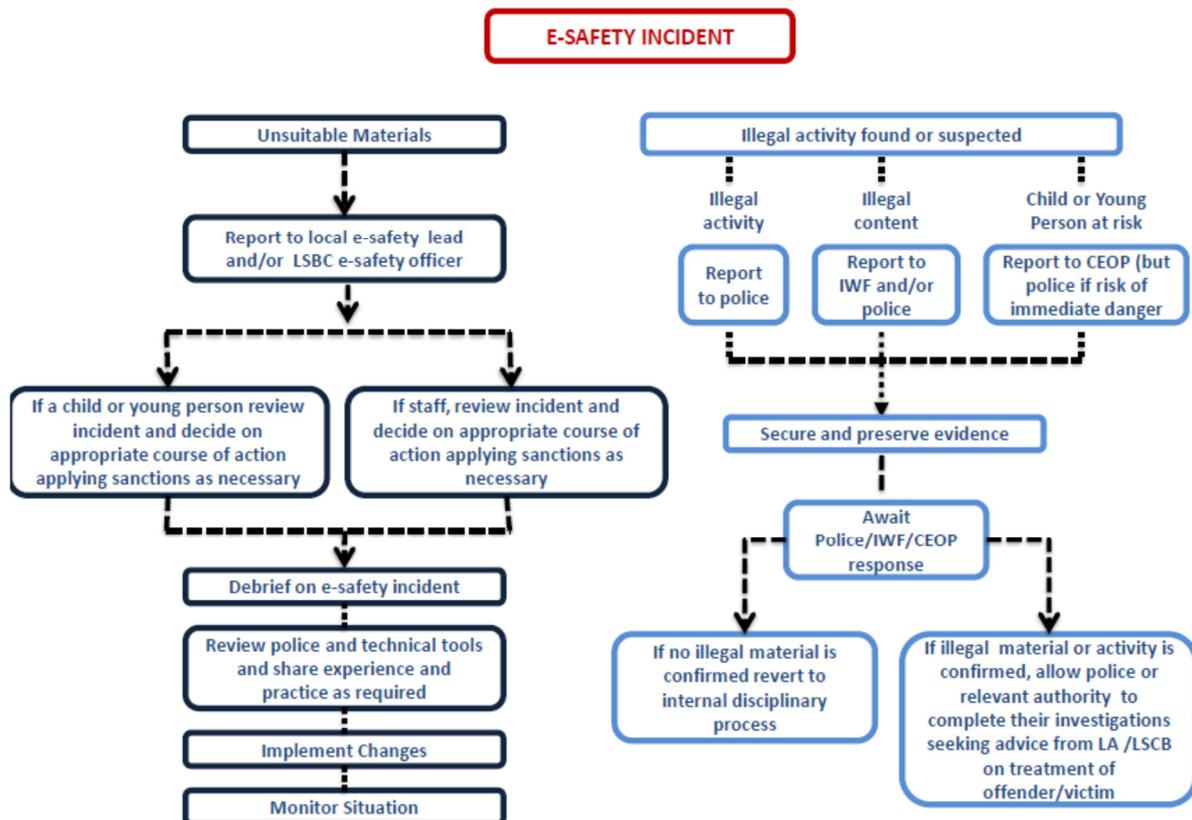
Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)

Flowcharts for Managing an eSafety Incident

http://www.thegrid.org.uk/eservices/safety/research/incident.shtml)

BECTA Flowchart for responding to e-safety incidents

E-SAFETY INCIDENT

Unsuitable Materials

Report to local e-safety lead and/or LSBC e-safety officer

If a child or young person review incident and decide on appropriate course of action applying sanctions as necessary

If staff, review incident and decide on appropriate course of action applying sanctions as necessary

Debrief on e-safety incident

Review police and technical tools and share experience and practice as required

Implement Changes

Monitor Situation

Illegal activity found or suspected

Illegal activity

Illegal content

Child or Young Person at risk

Report to police

Report to IWF and/or police

Report to CEOP (but police if risk of immediate danger

Secure and preserve evidence

Await Police/IWF/CEOP response

If no illegal material is confirmed revert to internal disciplinary process

If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations seeking advice from LA /LSCB on treatment of offender/victim

Section E – Internet Access & Information Security

Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

- The school maintains students who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology

- Staff will preview any recommended sites before use

- Raw image searches are discouraged when working with pupils

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources

- All users must observe copyright of materials from electronic resources

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience

- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog

- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion on what internet activities are permissible for

staff and pupils and how this is disseminated.

Infrastructure

- Islington Council has a monitoring solution via the LGFL where web-based activity is monitored and recorded

    - School internet access is controlled through the LA's web filtering service. For further information relating to filtering please go to : http://www.lgfl.net/services/pages/webscreen.aspx

- Copenhagen Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998

- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required

- The school does not allow pupils access to internet logs

- The school uses management control tools for controlling and monitoring workstations

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate

- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines

- *(for schools allowing personal removable media)* Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the *(technician/teacher)* for a safety check first

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from *(the Headteacher/technician/ICT subject leader)*

- If there are any issues related to viruses or anti-virus software, the network manager should be informed (*state how this is communicated*)

Managing Other Web 2 Technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking sites to pupils within school

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are

- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online

- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)

- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals

- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online

- Our pupils are asked to report any incidents of bullying to the school

- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Headteacher

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy through input gathered at specific eSafety school meetings or any other means used by school (e.g Survey, Interviews etc.)

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school

- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on

school website)

- Parents/ carers are expected to sign a Home School agreement containing the following statement or similar

    → **We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community**

- The school disseminates information to parents relating to eSafety where appropriate in the form of;

    o Information and celebration evenings
    o Posters
    o Website/ Learning Platform postings
    o Newsletter items
    o Learning platform training

Passwords and Password Security

Passwords
- Always use your own personal passwords to access computer based services

- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures

- Staff should change temporary passwords at first logon

- Change passwords whenever there is any indication of possible system or password compromise

- Do not record passwords or encryption keys on paper or in an unprotected file

- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished

- Passwords must contain a minimum of six characters and be difficult to guess

- User ID and passwords for staff and pupils who have left the School are removed from the system within 1 day

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with

others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security

- Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username.

- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others

- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

- Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer)

- In our school, all ICT password policies are the responsibility of **the Headteacher** and all staff and pupils are expected to comply with the policies at all times

Zombie Accounts

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left

- Prompt action on disabling accounts will prevent unauthorized access

- Regularly change generic passwords to avoid unauthorized access (Microsoft© advise every 42 days)

    Further advice available http://www.itgovernance.co.uk/

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any School information accessed from your own PC or removable media equipment is kept secure

- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access

- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others

- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person

- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment

- Only download personal data from systems if expressly authorised to do so by your manager

- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Ensure removable media is purchased with encryption

- Store all removable media securely

- Securely dispose of removable media that may hold personal data

- Encrypt all files containing personal, sensitive, confidential or classified data

- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Remote Access

- You are responsible for all activity via your remote access facility

- Only use equipment with an appropriate level of security for remote access

- To prevent unauthorised access to School systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone

- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers

- Avoid writing down or otherwise recording any network access information.

Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is

- Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment

Section F – Images and Photography

Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips.

- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site

- on the school's Learning Platform

- in the school prospectus and other printed publications that the school may produce for promotional purposes

- recorded/ transmitted on a video or webcam

- in display material that may be used in the school's communal areas

- in display material that may be used in external areas, ie exhibition promoting the school

- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Web Manager has authority to upload to the site.

Storage of Images

- Images/ films of children are stored on the school's network

- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) unless they are password encrypted USB sticks.

- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform

- The Senior Leadership Team has the responsibility of directing the deletion of the images when they are no longer required, or the pupil has left the school

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are the **Headteacher, Premises Assistant and Business Manager** Notification of CCTV use is displayed at the front of the school. Please refer to the hyperlink below for further guidance http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx

- We do not use publicly accessible webcams in school

- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults

- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
  - Webcams can be currently found on the laptop computers*. These should not be used to stream images outside of the school network.
  - Consent is sought from parents/carers and staff on joining the school, in the same way as for all images

For further information relating to webcams and CCTV, please see http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences (e.g inter-school skype sessions)

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school

- All pupils are supervised by a member of staff when video conferencing

- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school

- The school keeps a record of video conferences, including date, time and participants.

- Approval from the Headteacher is sought prior to all video conferences within school

- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences

- No part of any video conference is recorded in any medium without the written consent of those taking part

Additional points to consider:
- Participants in conferences offered by 3rd party organisations may not be CRB checked

- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

For further information and guidance relating to Video Conferencing, please see http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml

Section G – Hardware, Removable Media and Mobile Technologies

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you

- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory

- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available

- Ensure that all ICT equipment that you use is kept physically secure

- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990

- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive

- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted

- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc. accessing personal data must have a locking screensaver as must any user profiles

- Privately owned ICT equipment should not be used on a school network

- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled

- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal,

sensitive, confidential or classified information is disclosed to any unauthorised person

- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:

  o maintaining control of the allocation and transfer within their Unit
  o recovering and returning equipment when no longer needed

All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy

- Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey

- Synchronize all locally stored data, including diary entries, with the central school network server on a frequent basis

- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades

- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support

- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalized learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media

players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device

- Pupils are not allowed to bring personal mobile devices/phones to school This technology may be used. Year 6 pupils may request permission from the Headteacher to bring a mobile phone into school but it must be kept safe in the school office and picked up at 3.30pm.

- The school is not responsible for the loss, damage or theft of any personal mobile device.

- The sending of inappropriate text messages between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community

- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used

- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Removable Media

If storing/transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section '

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable **Media**' - Page 24

- Only use recommended removable media
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

Servers

- Always keep servers in a locked and secure environment

- Limit access rights

- Always password protect and lock the server

- Existing servers should have security software installed appropriate to the machine's specification

- Back up tapes should be encrypted by appropriate software

- Data must be backed up regularly

- Back up tapes/discs must be securely stored in a fireproof container

- Back up media stored off-site must be secure

Smile and Stay Safe Poster

eSafety guidelines to be displayed throughout the school (Example)

SMILE **and stay safe**

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)
Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.
Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'
Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC

- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you

- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access

- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time

- Do not introduce or propagate viruses

- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)

- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act

- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998

- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written**

guarantee that they will irretrievably destroy the data by multiple over writing the data. *RM and RecycleIT all offer this service*

Telephone Services

- You may make or receive personal telephone calls provided:

    1. They are infrequent, kept as brief as possible and do not cause annoyance to others

    2. They are not for profit or to premium rate services

    3. They conform to this and other relevant HCC and school policies.

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases

- Ensure that your incoming telephone calls can be handled at all times

- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask your unit manager

Mobile Phones

- You are responsible for the security of your school mobile phone. Always set the PIN code on your school mobile phone and do not leave it unattended and on display (especially in vehicles)

- Report the loss or theft of any school mobile phone equipment immediately

- The school remains responsible for all call costs until the phone is reported lost or stolen

- You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it

- School SIM cards must only be used in school provided mobile phones

- All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default

- You must not send text messages to premium rate services

- In accordance with the Finance policy on the private use of School provided mobiles, you must reimburse the school for the cost of any personal use of your

school mobile phone. This includes call charges incurred for incoming calls whilst abroad. [To assist you in identifying personal use, add * to the end of the number being contacted, these will be shown separately on your bill]. Payment arrangements should be made through your finance administrator

- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so

Section H – Guidance for Emerging Technologies

Internet policy and procedures: background information

Owing to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear. **Supervision is the key strategy.** Whatever systems are in place, something could go wrong which places pupils in an embarrassing or potentially dangerous situation.

Surfing the Web

Aimless surfing should never be allowed. It is good practice to teach pupils to use the Internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question "Why are we using the Internet?"

Search engines can be difficult to use effectively and pupils can experience overload and failure if the set topic is too open-ended. It is not sensible to have younger pupils 'searching the Internet'.

Pupils do not need a thousand Web sites on weather. A small selection will be quite enough choice, and as with other resources, the teacher needs to have checked and selected them so they are appropriate for the age group and fit for purpose. Favourites / bookmarks are a useful way to present this choice to pupils.

Teachers' web site selections for various topics can be put onto a topic page on the Learning Platform so pupils can, access out of school, from home etc. Some schools put links on their school web site, although there may even be difficulties here. Hackers can infiltrate a site or take over the domain, resulting in a previously acceptable site suddenly changing. Therefore, sites should always be previewed and checked, and work for children is best located on the closed Learning Platform.

Search Engines

Some common Internet search options are high risk, for example 'Google' image search. Some LAs and Councils block this. Others keep it unblocked because it can be a useful tool for teachers looking for images to incorporate in teaching. Where used – it must be with extreme caution. Google image search can be set-up to run in 'safe' mode although this is not fully without risk. Talk to your network manager or Technical support provider about this. LGfL guidance is available on the safety site. Images usually have copyright attached to them which is an issue commonly overlooked but a key teaching point to pupils and staff.

Collaborative Technologies
There are a number of Internet technologies that make interactive collaborative environments available. Often the term 'Social networking software' is used. Examples include blogs (personal web-based diary or journals), wikis (modifiable collaborative web pages), and podcast sites (subscription-based broadcast over the web) supported by technologies such as RSS (really simple syndication – an XML format designed for sharing news across the web). Using these technologies for activities can be motivational, develop oracy and presentations skills, helping children consider their content and audience. Schools are best protected by using the social collaboration tools within the school's Learning Platform, such as the London MLE..

Blogs: A School may want to use them as a method of online publishing, perhaps creating class blogs, or to creatively support a specific school project. A 'safe' blogging environment is likely to be part of a school's Learning Platform or within LGfL /LA provided 'tools'.

Webcams and Video Conferencing
Webcams: are used to provide a 'window onto the world' to 'see' what it is like somewhere else. LGfL has a number of nature cams showing life inside bird boxes for example and a plethora of weather cams across London providing detailed real-time weather data. Webcams can also be used across London for streaming video as part of a video conferencing project.
Video conferencing provides a 'real audience' for presentations and access to places and professionals – bringing them into the classroom.For large group work high quality video conferencing hardware equipment is required to be plugged into the network. LGfL, and the other national regional grids for learning, have made an agreement with JVCS (the Janet Videoconferencing Service) to host calls.   All conferences are therefore timed, closed and safe. This is a service that is included in LGfL 2. Advice can be found here
http://www.lgfl.net/SERVICES/CURRICULUM/Pages/WeatherStations.aspx
http://www.lgfl.net/learningresources/VideoConferencing/Pages/Home.aspx

Pupils can search on the Internet for other webcams - useful in subject study such as geography (e.g. to observe the weather or the landscape in other places). However, there are risks as some webcam sites may contain, or have links to adult material. In schools adult sites would normally be blocked but teachers need to preview any webcam site to make sure it is what they expect before ever using with pupils.

The highest risks lie with streaming webcams [one-to-one chat / video] that pupils use or access outside of the school environment. Pupils need to be aware of the dangers.

Social Networking Sites
These are a popular aspect of the web for young people. Sites such as Facebook, My Space, Habbo Hotel, Bebo, Piczo, and YouTube allow users to share and post web sites, videos, podcasts etc. It is important for children to understand that these

sites are public spaces for both children and adults. They are environments that should be used with caution. Users, both pupils and staff, need to know how to keep their personal information private and set-up and use these environments safely. [See Education programme]

Most schools will block such sites. However, pupils need to be taught safe behaviour as they may well be able to readily access them outside of school. There are educational, monitored services that schools can purchase such as GridClub SuperClubs. Additionally, the LGfL Learning Platform provides a safe environment for pupils to share resources, store files in an ePortfolio, and communicate with others through 'closed' discussions, etc.

Podcasts
Podcasts are essentially audio files published online, often in the form of a radio show but can also contain video. Users can subscribe to have regular podcasts sent to them and simple software now enables children to create their own radio broadcast and post this onto the web. Children should be aware of the potentially inappropriate scope of audience that a publicly available podcast has and to post to safer, restricted educational environments such as the LGfL. Podcast central area. http://www.lgfl.net/SERVICES/CURRICULUM/Pages/Podcasting.aspx

Chatrooms
Many sites allow for 'real-time' online chat. Again, children should only be given access to educational, moderated chat rooms. The moderator (or referee) checks what users are saying and ensures that the rules of the chat room (no bad language, propositions, or other inappropriate behaviour) are observed. Pupils should be taught to understand the importance of safety within any chat room because they are most likely at risk out of school where they may access chatrooms such as www.teenchat.com, www.habbohotel.co.uk, www.penguinchat.com

Sanctions and infringements
The school's Internet e-safety / Acceptable Use policy needs to be made available and explained to staff / Governors, pupils and parents, with all signing acceptance / agreement forms appropriate to their age and role. The school needs to have made clear possible sanctions for infringements. *See associated Sanctions and infringement document.*

Following any incident that indicates that evidence of indecent images or offences concerning child protection may be contained on school computers, the matter should be immediately referred to the Police. There are many instances where schools, with the best of intentions, have commenced their own investigation prior to involving the police. This has resulted in the loss of valuable evidence both on and off the premises where suspects have inadvertently become aware of raised suspicions. In some circumstances this interference may also constitute a criminal offence.

Section I – Policy Review

Staff and Pupil Involvement in Policy Creation

- Staff and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use through *(state how, ie school council, staff meetings)*

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them

There will be an on-going opportunity for staff to discuss with the SIRO/AIO any issue of data security that concerns them

This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

Section J - Appendices

Appendix A

Acceptable Use Policy (AUP): Staff agreement form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- 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 not reveal my password(s) to anyone.

- 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 allow unauthorised individuals to access email / Internet / intranet / 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 not engage in any online activity that may compromise my professional responsibilities.

- I will only use the approved, secure email system(s) for any school business. (This is currently: LGFL's Staffmail)

- I will only use the approved school email, blogs 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 report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.

- 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 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 will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff. I will use the school's Learning Platform in accordance with school protocols.

- 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.

- 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.

- I will alert the school's named child protection officer / relevant senior member of staff if I feel the behaviour of any child I teach may be a cause for concern.

- I will only use LA systems in accordance with any corporate policies.

- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.

- 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 a senior member of staff / named child protection officer at the school.

- I understand that failure to comply with this agreement could lead to disciplinary action.

Acceptable Use Policy (AUP): Staff agreement form

User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature ....Date ....

Full Name .... (printed)

Job title ....

School ....

Authorised Signature -Head Teacher

I approve this user to be set-up.

Signature .... Date...

Full Name .... (printed)

Appendix B

Policy: 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 and will reflect the school's behaviour and disciplinary procedures.

The following are provided as **exemplification** only:

STUDENT	
Category A infringements	**Possible Sanctions:**
• 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	**Refer to class teacher / tutor** Escalate to: senior manager / e-Safety Coordinator
Category B infringements	**Possible Sanctions:**
• 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 • Trying to buy items over online • 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	**Refer to Class teacher/ Head teacher/ Deputy Headteacher and Assessment Headteacher/ e-safety Coordinator** Escalate to: removal of Internet access rights for a period / removal of phone until end of day / contact with parent]

STUDENT	
Category C infringements	**Possible Sanctions:**
• Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site. • Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off) • Trying to access offensive or pornographic material (one-off) • Purchasing or ordering of items online • Transmission of commercial or advertising material	**Refer to Class teacher / Year Tutor / e-safety Coordinator / Head teacher / removal of Internet and/or Learning Platform access rights for a period** Escalate to: contact with parents / removal of equipment **Other safeguarding actions if inappropriate web material is accessed:** Ensure appropriate technical support filters the site
Category D infringements	**Possible Sanctions:**
• Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned • Deliberately creating accessing, downloading or 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	**Refer to Head Teacher / Contact with parents** **Other possible safeguarding actions:** • Secure and preserve any evidence • Inform the sender's e-mail service provider. • Liaise with relevant service providers/ instigators of the offending material to remove • Report to Police / CEOP where child abuse or illegal activity is suspected

STAFF	
Category A infringements (Misconduct)	**Possible Sanctions:**
- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc. - Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored. - Not implementing appropriate safeguarding procedures. - Any behaviour on the World Wide Web that compromises the staff members professional standing in the school and community. - Misuse of first level data security, e.g. wrongful use of passwords. - Breaching copyright or license e.g. installing unlicensed software on network.	**Referred to line manager / Head teacher** Escalate to: *Warning given*
Category B infringements (Gross Misconduct)	**Possible Sanctions:**
- 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 creating ,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	**Referred to Head teacher / Governors;** **Other safeguarding actions:** - Remove the PC to a secure place to ensure that there is no further access to the PC or laptop. - 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. - Identify the precise details of the material. *Escalate to:* *report to LA /LSCB, Personnel, Human resource.* Report to Police / CEOP where child abuse or illegal activity is suspected. ,

If a member of staff commits an exceptionally serious act of gross misconduct

The member of staff 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 abuse images found

In the case of Child abuse images being found, the member of staff should be **immediately suspended** and the Police should be called.

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

http://www.iwf.org.uk

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. All staff will be required to sign the school's e-safety acceptable use agreement form;
- 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 agreement form;
- The school's e-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- 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).

Sample agreement forms can be downloaded from the LGfL e-safety site

The school will try to ensure that pupils will have good access to technology (computing) to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school computing systems in a responsible way, to ensure that there is no risk to my safety or to others.

For my own personal safety:
- I understand that the school will monitor my use of the computing systems
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- I will tell an adult if I see any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable on-line.

I will act as I expect others to act toward me:
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language.
- I will not take or send images of anyone without their permission.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

I understand that I am responsible for my actions, both in and out of school:
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, suspensions and contact with parents.

Student / Pupil Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school computing systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school computing systems and equipment (both in and out of school)
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil (print please)

Signed | **Date**