



St. Stephen's School and Children's Centre

Learning for life

e-Safety Policy

Reviewed:	May 2011
By:	Jenna Van Loan (ICT Coordinator) Duncan Kilty (Multi Media Coordinator)

Contents

- **E-safety policy overview (this document)**
- **Section 1: Managing the Internet safely**
- **Section 2: Managing email**
- **Section 3: Use of digital and video images**
- **Section 4: Managing equipment**
- **Section 5: How will Infringements be handled**

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.

Context:

ICT in the SEF

3a - the extent to which information and communication technology (ICT) capability and other key skills enable learners to improve the quality of their work and make progress

4b - the extent to which learners adopt safe and responsible practices in using new technologies, including the Internet.

4e - through the development of literacy, numeracy, information and communication technology, enterprise capability, economic and business understanding and financial capability

We have a duty to ensure that all students are able to make a valuable contribution to society & this is impossible to achieve if we do not ensure that students develop and apply their ICT capability effectively in their everyday lives.

SRF elements – working towards ICT Mark

1c-4 Safeguarding

The school is aware of its responsibilities in ensuring that ICT usage by all network users is responsible, safe and secure. There are relevant and comprehensive policies in place which are understood and adhered to by many network users.

3b-2 Effective and safe use of digital resources

Most pupils have a good range of skills that enable them to access and make effective use of digital resources to support their learning. They understand the issues relating to safe and responsible use of ICT and adopt appropriate practices

*Harnessing Technology: Transforming learning and children's services*¹ sets out the government plans for taking a strategic approach to the future development of ICT.

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

The Green Paper *Every Child Matters*² and the provisions of the *Children Act 2004*³, *Working Together to Safeguard Children*⁴ sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

¹ <http://www.dfes.gov.uk/publications/e-strategy/>

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

At St. Stephens, we recognise it is our duty to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

1. The technologies

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

- The Internet
- e-mail
- Instant messaging (<http://www.msn.com>, <http://info.aol.co.uk/aim/>) often using simple web cams
- Blogs (an on-line interactive diary)

² See The Children Act 2004 [<http://www.opsi.gov.uk/acts/acts2004/20040031.htm>]

³ See Every Child Matters website [<http://www.everychildmatters.gov.uk>]

⁴ Full title: Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children. See Every Child Matters website [http://www.everychildmatters.gov.uk/_files/AE53C8F9D7AEB1B23E403514A6C1B17D.pdf]

- 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> / <http://www.facebook.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/> / <http://www.clubpenguin.com>)
- Music download sites (Popular <http://www.apple.com/itunes/> <http://www.napster.co.uk/> <http://www-kazzaa.com/>, <http://www-livewire.com/>)
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

2. Whole school approach to the safe use of ICT

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

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

*Ref: Becta - E-safety Developing whole-school policies to support effective practice*⁵

3. Roles and Responsibilities

e-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to a member of the senior management team.

Our school **E-Safety Co-ordinator** is Neena Lall

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as Becta and The

⁵ <http://schools.becta.org.uk/index.php?section=is>

Child Exploitation and Online Protection (CEOP)⁶. The school's e-Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance⁷ on e-Safety and are updated at least annually on policy developments.

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

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

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

Staff are reminded / updated about e-Safety matters at least once a year.

Schools should include esafety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to contrail and minimise online risks and how to report a problem.

Schools should ensure that they make efforts to engage with parents over e-safety matters and that parents/guardians/carers have signed and returned an e-safety/AUP form.

4. Communications

How will the policy be introduced to pupils?

Many pupils are very familiar with the culture of new technologies. Pupils' perceptions of the risks may not be mature; the e-safety rules may need to be explained or discussed.

Consideration must be given as to the curriculum place for teaching e-safety. It is delivered through leadership assemblies and through PSHE/ ICT lessons through the curriculum.

Useful e-safety programmes include:

- Think U Know (www.thinkuknow.co.uk/)
- Grid Club www.gridclub.com

⁶ <http://www.ceop.gov.uk/>

⁷ 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

- The BBC's ChatGuide: www.bbc.co.uk/chatguide/
- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.
- An e-safety module will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.

How will the policy be discussed with staff?

It is important that all staff feel confident to use new technologies in teaching. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies

Staff must understand that the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration, caretaker, governors and helpers should be included in appropriate awareness raising and training. Induction of new staff should include a discussion of the school's e-Safety Policy.

- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

How will parents' support be enlisted?

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. St. Stephens may be able to help parents plan appropriate supervised use of the Internet at home.

- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This will include e-safety sections in our termly newsletter, an e-safety area on our school website and suggestions for safe home Internet use during curriculum evenings.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

<i>5. How will complaints regarding e-Safety be handled?</i>

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by tutor / Head of Year / 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];
- referral to LA / Police.

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

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



SECTION 1 – MANAGING THE INTERNET SAFELY

Technical and infrastructure

The borough

- Maintains the filtered broadband connectivity through the LGfL and so connects to the 'private' National Education Network.
- Ensures their network is 'healthy' by having LA or Synetrix health checks annually on the network;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies;
- Provides a filtering service which prevents pupils and staff from accessing inappropriate websites or content e.g. facebook, youtube.

St. Stephens Primary School

- Works in partnership with the LA to ensure any concerns about the system are communicated to LGfL so that systems remain robust and protect students;
- Has additional user-level filtering in-place using the *Synetrix USO service*.
- Ensures network health through appropriate anti-virus software etc and network set-up so staff and pupils cannot download executable files such as .exe / .com / .vbs etc.;
- Utilises caching as part of the network set-up;
- Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows pupils access to Internet logs;
- Uses hector Protector that pupils can activate should they find something on their screen which makes them feel uncomfortable;
- Uses individual log-ins for pupils from reception and all other users;
- Uses security time-outs on Internet access where practicable / useful;
- Uses RM Tutor management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Never allows personal level data off-site unless it is on an encrypted device;
- Uses Google Safe Search to limit the possibility of pupils accessing inappropriate material;
- Ensures pupils only publish within appropriately secure learning environments such as their own closed secure LGfL portal or Learning Platform.

Policy and procedures

St. Stephens Primary School

- Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;
- We use the pan-London LGfL / Synetrix filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Staff preview all sites before use or only use sites accessed from managed 'safe' environments such as the Learning Platform;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Never allows pupils to conduct 'raw' image searches e.g. Google or Lycos image search;
- Informs users that Internet use is monitored;
- Informs staff and students that they must report any failure of the filtering systems directly to the Child Protection/E-safety Coordinator. Our systems administrators report to LA / LGfL where necessary;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only uses LGfL for pupil's own online creative areas such as web space and ePortfolio as well as using NEN for video conferencing activity;

- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes such as LGfL’s Audio Network;
- Requires pupils (and their parent/carer) from Key Stage 1 and 2, to individually sign an e-safety / acceptable use agreement form, including consent to use the internet, which is fully explained and used as part of the teaching programme;
- Uses closed / simulated environments for e-mail with Key Stage 2 pupils;
- Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file in the Single Central Record File and 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, e.g. print-out, 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;
- Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Education and training

St. Stephens Primary School

- Ensures pupils and staff know what to do if they find inappropriate web material i.e. use hector protector and report incident to the teacher immediately.
- 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, including cyber-bullying incidents.
- Ensures staff report all incidents listed above to E-safety coordinator;
- 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 understand data protection and general ICT security issues linked to their role and responsibilities;
- Runs a rolling programme of advice, guidance and training for parents, including: Information leaflets in school newsletters and on the school web site, distribution of ‘think u know’ for parents materials, demonstrations and practical sessions held at school.
- Has a clear, progressive e-safety education programme built on national guidance teaching a range of skills and behaviours appropriate to their age and experience:
 - **INTERNET SEARCHING**
 - to STOP and THINK before they CLICK
 - to develop a range of strategies to validate and verify information before accepting its accuracy;
 - 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;
 - to know not to download any files – such as music files - without permission;
 - **ON-LINE COMMUNICATION**
 - to understand ‘Netiquette’ behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour.
 - to never delete or respond to malicious or threatening emails or messages and show them to a responsible adult;
 - to get teacher approval before contacting external organisations or individuals;
 - to get teacher approval before opening or sending attachments;
 - to never embed information e.g. adverts, images;
 - to understand why on-line ‘friends’ may not be who they say they are;

- to never arrange to meet anyone they meet online without having discussed it with an adult and to never meet anyone you have met online without a responsible adult present;
 - to never forward chain email letters or open an email from an unknown sender;
 - to have strategies for dealing with receipt of inappropriate materials;
 - Pupils are encouraged to invite known friends only and deny access to others.
- **PROTECTION OF PRIVACY**
- to never give out personal details of any kind which may identify them and / or their location. Examples include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
 - to never place personal photos on any social network space due its public nature. Advice will include reference to background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
 - to understand why they must not post pictures or videos of others without their permission;
 - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
 - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, personal thoughts, photographs and videos and to know how to ensure they have turned-on privacy settings;
 - to set passwords, deny access to unknown individuals and block unwanted communications.

SECTION 2 – MANAGING E-MAIL

At St. Stephens Primary School

- We do not publish personal e-mail addresses of pupils or staff on the school website. We use info@st-stephens.newham.sch.uk for communication with the wider public.
- If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we contact the Police.
- Accounts are managed effectively, with up to date account details of users.
- Messages relating to or in support of illegal activities will be reported to the relevant Authority and Police.
- We use the Local Authority / LGfL anti-virus product Sophos and additional email, spam, phishing software provided by our LA .

For pupils

- We use and monitor communication tools within the ‘closed’ Learning Platform (London MLE) with the pupils for communication with staff and other pupils.
- We do not use email that identifies the name and school of the pupil.
- We only use LGfL ‘safemail’ with pupils.
- Pupils can only use the LGfL / school domain e-mail accounts on the school system.
- Pupils are introduced to, and use e-mail as part of the ICT scheme of work.
- Pupils are taught about the safety and ‘netiquette’ of using e-mail both in school and more generally, for example personal accounts set-up at home. See SECTION 1 – Education and training for more details.

For staff

- Staff use LGfL e-mail system for professional purposes;
- Staff are allowed to only use the LGfL / school domain e-mail accounts on the school system and we do not allow staff to access personal email during the school day;
- We have a ‘closed’ LA secure email system which is used for some ‘LA approved’ transfers of information we consider to be sensitive (some protect-level data);
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper, and should follow these guidelines:
 - That it should follow the school ‘house-style’;
 - the sending of multiple or large attachments should be limited;
 - personal information must not be sent as attachments on open email. A secure method of encrypted transfer should always be used;
 - the sending of chain letters is not permitted;

- embedding adverts is not allowed;

SECTION 3 – USE OF DIGITAL AND VIDEO IMAGES

At St. Stephens Primary School

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is restricted to School –Based Technician, Assistant Head Teacher and ICT Co-ordinator.
- The school web site complies with the school's guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, email address and telephone number.
- Photographs of pupils published on the web do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child at the beginning of every school year.
- Digital images /video of pupils are stored in the teachers' shared Multimedia folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a school purpose;
- when publishing to the school website we do not use pupils' names in the file titles or <ALT> tags of images;
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff are not allowed to use mobile phones / personal equipment for taking pictures of pupils as stated in the school's Acceptable Use Policy signed by all staff;
- Pupils are taught about how images can be abused in their eSafety education programme;

Social networking and personal publishing

St. Stephens Primary School

- The LA blocks access to all social networking sites in school;
- Newsgroups/forums will be blocked unless a specific use is approved by the e-safety coordinator;
- Actively advises parents and pupils that social networking sites e.g. Facebook are inappropriate and illegal for pupils under the age of 13;
- Encourages staff to regularly check privacy settings of any social networking site that they use at home to ensure privacy;
- For more information on this see SECTION See SECTION 1 – Education and training for more details.

SECTION 4 – MANAGING EQUIPMENT

Using the school network, equipment and data safely

The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely, St. Stephens Primary School:

- Maintains equipment to ensure Health and Safety is followed e.g. equipment installed and checked by approved Suppliers / LA electrical engineers;

- Uses our broadband network for our CCTV system and this has been set-up by approved LGfL partners;
- Uses the DfES secure s2s website for all CTF files sent to other schools;
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school ICT systems regularly with regard to security.
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems e.g. technical support or SIMS Support through LA systems;
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role e.g. SEN coordinator - SEN data;

For all users

- 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. [Users needing access to secure data are timed out after XX mins and have to re-enter their username and password to re-enter the network.];
- Request that teachers and pupils switch the computers off at the end of the day and the school automatically remotely switch off all computers at 8 o'clock;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music download or shopping sites – except those approved for educational purposes;
- Encourages all users to scan all mobile equipment with anti-virus / spyware before it is connected to the network;
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their Shibboleth compliant username and password.

For Staff

- Ensures staff read and sign that they have understood the school's Acceptable Use Form. Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;
- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- 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.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies e.g. Borough email or Intranet; finance system, personnel system.
- Ensures that access to the school's network resources by staff can only be done on-site;
- Managed Learning Environment can be accessed online by all staff but is password protected and staff users can only access modules related to their role;

For Pupils

- Provides pupils with an individual network log-in username. From Year 1 they are also expected to use a personal password;
- 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;

SECTION 5 – 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.

Pupils:

Dealt with by class teacher in accordance with behaviour policy e.g.

- Use of non-educational sites during lessons,
- unauthorised use of email,
- Use of unauthorised instant messaging / social networking sites.

Dealt with by class teacher in accordance with behaviour policy and Phase Leader/ E-Safety Coordinator informed e.g.

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

Dealt with by class teacher in accordance with behaviour policy and Phase Leader/ E-Safety Coordinator / Head Teacher informed and letter sent to parents e.g.

- 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,
- use of mobile phone (or other new technologies) in school e.g. to send texts to friends

Dealt with by Head Teacher and parents meeting. Also inform governor pupil disciplinary panel e.g.

- 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

Staff:

Referred to Line Manager

- 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 Headteacher / Governors and follow school disciplinary procedures; report to ITASS, report to Police e.g.

- 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.

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.

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.

If Child Pornography is found?

In the case of Child Pornography being found, the member of staff should be immediately suspended and the Police should be called: see the free phone number **0808 100 00 40** at:

<http://www.met.police.uk/childpornography/index.htm>

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

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

<http://www.iwf.org.uk>

How will Staff and Pupils 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 Policy acceptance 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 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).