e-Safety Policy for

Edmonton County School

January 2014

Contents

Contents

Context

Edmonton County is aware that 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.

However, as stated in the DCSF e-Strategy: In order to use these technologies effectively and safely we need to highlight the risks as well as the benefits. We need to provide opportunities for the development of new skills so that appropriate use is made of technology both in and outside of the classroom.

The Every Child Matters agenda and the Students Act 2004: Working Together to Safeguard Students sets out how organisations and individuals should work together to safeguard and promote the welfare of students.

The 'staying safe' outcome includes aims that students 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.

Many of these aims apply equally to the 'virtual world' that students 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 students 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 students and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school 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 is underpinned by the recommendations of BECTA. It aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of students 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 students include:

- the Internet
- e-mail
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / http://www.hi5.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)

Contents

- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

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 students, staff and parents.

Roles and Responsibilities

e-Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. She 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 our School Business Manager: Mr George Georgiou and AHT with responsibility for the PSHCE programme: Mr Andrew Martin.

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 The Child Exploitation and Online Protection (CEOP)[1]. The school's e-Safety coordinator ensures the Headteacher, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance 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.

Students are required to be fully aware of the e-safety Policy and this is covered in ICT lessons.

Phase Leaders should keep matters of e-Safety at the fore of any discussion with students regarding friendship problems. Central to this is fostering a 'No Blame' culture so students feel able to report any bullying, abuse or inappropriate materials.

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

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

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

Contents

- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of student information/photographs and use of website;
- eBullying / Cyberbullying procedures;
- their role in providing e-Safety education for students;

Staff are reminded / updated about e-Safety matters at least once a year and are requested to sign the policy to accept the regulations.

How will complaints regarding e-Safety be handled

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

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

- interview/counselling by tutor / Head of Phase/ student manager / e-Safety Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- referral to LA / Police.

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

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

Managing the Internet Safely - Why is Internet Access Important?

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; indeed ICT is now seen as a functional, essential life-skill along with English and mathematics. The statutory curriculum requires students to learn how to locate, retrieve and exchange information using technology including the Internet. All students should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet can benefit the professional work of staff and enhances the school's management information and business administration systems.

The Risks

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for students. In addition, there is information on weapons, crime and racism that would be more considered inappropriate and restricted elsewhere.

Contents

Our e-Safety lessons delivered within the ICT curriculum aims to provide students with as safe an Internet environment as possible and to teach students to be aware of and respond responsibly to any risk. Our supportive culture encourages students to report abuse. Risks can be high outside school, so our Parents' Guide will inform parents of the risks and how to identify safe and unsafe use.

Schools also need to protect themselves from possible legal challenge. It is clearly a criminal offence to hold images of child pornography on computers or to use Internet communication to 'groom' students. The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Sending malicious or threatening e-mails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984).

Technology

Edmonton County School has up-to-date anti-virus, anti-spyware and anti-spamware software and approved firewall solutions installed on our network. To make sure rogue applications are not downloaded and hackers cannot gain access to the school's equipment or into users' files through Internet use, students should not be able to download executable files and software.

Unfortunately, inappropriate materials will inevitably get through any filtering system. We are vigilant and alert so that sites can be blocked as soon as they are apparent. Conversely, sometimes appropriate websites need to be unblocked. The network manager is able to block or liaise directly with LGFL over this.

High level monitoring of website access is also undertaken by Synetrix and logs can be obtained where a site is under investigation.

We do not send personal data across the Internet unless it is encrypted or sent via secure systems such as the DfES s2s site or our approved Learning Platform, Fronter.

Network Policy

Edmonton County School:

- Ensures network health through appropriate anti-virus software etc and network set-up so staff and students cannot download executable files such as .exe / .com / .vbs etc.;
- Ensures their network is 'healthy' by having health checks regularly on the network;
- Ensures the Systems Administrator / network manager is up-to-date with services and polices
- Ensures the 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 students access to Internet logs;
- Uses individual log-ins for students and all other users;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Uses 'safer' search engines with students such as bbc.co.uk and activates 'safe' search where appropriate;
- Ensures students only publish within appropriately secure learning environments such as their own closed secure LGfL portal or Learning Platform.

Contents

Policy Procedures for Teaching and Learning

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. Students are supervised in their use of technology for the majority of their time.

Surfing the Web

Internet use should always be purposeful. It is good practice to teach students to use the Internet in response to an articulated need – e.g. a question arising from work in class. Students should be able to answer the question "Why are we using the Internet?"

Search engines can be difficult to use effectively and students can experience overload and failure if the set topic is too open-ended. Of course the experienced teacher will choose a topic with care, select the search engine and then discuss with students sensible search words, which should be tested beforehand.

Students do not need a thousand Web sites on weather. A small selection may be quite enough choice. Favourites are a useful way to present this choice to students. If teachers' web site selections for various topics are put on the school web site, access by students from home and by other schools is made possible. However, hackers can infiltrate a site or take over the domain, resulting in a previously acceptable site suddenly changing, for example, to a pornographic one. Therefore, sites should always be previewed as far as is possible.

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 podcasting (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 oral and presentations skills, helping students consider their content and audience. However, they are high risk environments and it is essential that teachers use them carefully.

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. Schools should follow Local Authority advice. A 'safe' blogging environment is likely to be part of a school's future Learning Platform.

Video Conferencing

Webcams: are used to provide a 'window onto the world' to 'see' what it is like somewhere else. [E.g the LGfL nature cam and weather cams.] Webcams are also used widely across London for streaming video as part of a video conferencing project. Using the Click to Meet LGfL approved software, video conferencing provides a 'real audience' for presentations and access to places and professionals – bringing them into the classroom. Synetrix provides a video conferencing service across the broadband network and it is managed by LGfL. LGfL has made an agreement with JVCS (the Janet Videoconferencing Service) to host calls. In order to create calls the school needs to register with JVCS and with the Click-to-Meet server. All conferences are therefore timed, closed and safe. Advice can be found from: www.vc.lgfl.net

Schools wishing to use Internet webcams outside of the LGfL environment should be aware of, and follow LA and Becta advice.

Students 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 students.

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

Social Networking Sites and Chatrooms

These are a popular aspect of the web for young people. Sites such as My Space, Habbo, Bebo, Piczo, and YouTube allow users to share and post web sites, videos, podcasts etc. It is important for students to understand that these sites are public spaces where adults frequent. Students are taught to use these sites safely to enable responsible and safe use outside of school.

Students should not be allowed to use chat rooms unless it is an educational resource and is part of a subject area's programme of study.

Sanctions and Infringements

The school's Internet e-safety policy has been made available and explained to staff, Governors, students and parents.

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 referred at the earliest opportunity to the local police station. 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.

Use of the Internet Policy

Edmonton County School:

- Supervises students' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older students have more flexible access
- Uses the pan-London LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature
- previews all sites before use [where not previously viewed and cached] or only use sites accessed from managed 'safe' environments such as the Learning Platform
- Plans the curriculum context for Internet use to match students' ability, using child-friendly search engines where more open Internet searching is required
- 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 Network Manager or classroom teacher. Our systems administrators report to 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 the LGfL service for video conferencing activity
- Only uses approved Blogging or discussion sites, such as on the LGfL / approved Learning Platform and blocks others
- Only uses approved or checked webcam sites

- Has blocked student access to music download or shopping sites – except those approved for educational purposes such as LGfL's Audio Network
- Requires students (and their parent/carer) to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme in ICT lessons
- 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;
- Maintains a record of any bullying or inappropriate behaviour *(the e-Safety log)* and acts to deal with the perpetrator of this behaviour
- Ensures parents provide consent for students to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their daughter's entry to the school;
- Makes information on reporting offensive materials, abuse / bullying etc available for students, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – LA Police.

How E-mail is managed

E-mail is now an essential means of communication for staff in our schools and increasingly for students and homes. Directed e-mail use in schools can bring significant educational benefits through increased ease of communication between students and staff, or within local and international school projects.

However, un-regulated e-mail can provide a means of access to a student that bypasses the traditional school physical boundaries. The central question is the degree of responsibility for self-regulation that may be delegated to an individual. Once e-mail is available it is difficult to control its content.

Incoming and outgoing e-mail is monitored by LGFL only when emails are sent and read via the school network. When used outside school there is no monitoring.

Procedures

In the school context, e-mail should not be considered private and most schools, and indeed Councils and businesses, reserve the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of students and the preservation of human rights, both of which are covered by recent legislation.

The use of personal e-mail addresses, such as Hotmail, should be avoided by all working in schools and staff are asked to use the school domain system for professional purposes as far as possible and unless the Headteacher has agreed that an exception may be made.

Many teenagers will have their own e-mail accounts, such as the web-based Hotmail or G-mail, which they use widely outside school, usually for social purposes. If e-mail accounts are not monitored there is the risk that students could send or receive inappropriate material. External web-based e-mail accounts with anonymous names such as pjb354@emailhost.com make monitoring difficult. Consequently, Edmonton County School limits e-mail use to accounts on the school domain only.

Education

Students need to be made aware of the risks and issues associated with communicating through e-mail and to have strategies to deal with inappropriate e-mails. This should be part of the school's e-Safety and anti-bullying education programme.

Students need to understand good 'netiquette' style of writing, (this links to English) and appropriate e-mail behaviour appropriate to their age.

Contents

Edmonton County School Statement on use of Email

- If one of our staff or students 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

Students

- Students and staff are all allocated an email account through the school (Edmonton.enfield.sch.uk) domain. This enables them to access their email from school
- Students are introduced to, and use e-mail as part of the ICT scheme of work.
- Students are taught about the safety and 'netiquette' of using e-mail i.e.
  - not to give out their e-mail address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer;
  - that an e-mail is a form of publishing where the message should be clear, short and concise;
  - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
  - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
  - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
  - the sending of attachments should be limited;
  - embedding adverts is not allowed;
  - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
  - not to respond to malicious or threatening messages,
  - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
  - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
  - that forwarding 'chain' e-mail letters is not permitted;
- A copy of the school policy is in Student Planners and we explain how any inappropriate use will be dealt with.

Staff

- Staff use our school domain e-mail system as far as possible for professional purposes unless given authorization from the Headteacher
- Ensure that e-mail sent to an external organisation is written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style';
  - the sending of chain letters is not permitted;
  - embedding adverts is not allowed;
- Staff are provided with the e-safety policy which contains information on how any inappropriate use will be dealt with. E-safety is discussed at a staff meeting every year.

Contents

Fronter at Edmonton County School

Edmonton County School use a Managed Learning Environment (MLE) provided through our educational broadband provider, London Grid for Learning (LGfL).

This is a closed environment, requiring teachers and students to log in to use the service.

The MLE allows teachers to provide materials to support lessons for use both inside and outside the school. Students will be able to hand in work, work collaboratively, ask for help and participate in discussion forums.

Links will be made to other sites on the Internet. While every care is taken to ensure the direct link is to a suitable site or resource, we can have no control over other links that are made on that site.

All use of discussion forums and collaborative features are monitored by the teachers that create the resource and all usage can be tracked by the administrator.

There will be occasions when the student is required to use the MLE as part of a course.

Using Digital Images and Video Safely

Developing safe school web sites

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work. Procedures and practice need to ensure website safety. A senior member of staff monitors the website's content and checks suitability. Only the Website Co-ordinator is able to upload detail to the School website

Use of still and moving images

Most importantly, care needs to be taken when using photographs or video footage of students on the school website. We do not use the first name and last name of individuals in a photograph. Our policy is:

- If the student is named, avoid using their photograph / video footage
- If the photograph /video is used, avoid naming the student.

When we showcase examples of students work we use only their first names, rather than their full names. We only use images of students in suitable dress to reduce the risk of inappropriate use.

Contents

In many cases, it is unlikely that the Data Protection Act will apply to the taking of images e.g. photographs taken for personal use, such as those taken by parents or grandparents at a school play or sports day. However, photographs taken for official school use, which are likely to be stored electronically alongside other personal data, may be covered by the Data Protection Act. As such, students and students are always informed as to why they are being taken.

Parental permission should be obtained before publishing any photographs, video footage etc of students on the school website or in a DVD.

Procedures

Links to any external websites are thoroughly checked before inclusion on a school website to ensure that the content is appropriate both to the school and for the intended audience. The school checks all links regularly, not only to ensure that they are still active, but that the content remains suitable too.

Text written by students are always reviewed before publishing on the school website. We make sure that the work doesn't include the full name of the student, or reveal other personal information, such as membership of after school clubs or any other details that could potentially identify them. We check that students' work doesn't contain any statements that could be deemed defamatory.

We also ensure also that the school is not infringing copyright or intellectual property rights through any content published on the website. For example, using images sourced through Google, or using a Trademark for which copyright permission has not been sought.

If the school's website contains any guestbook, noticeboard or blog, they need to be monitored to ensure they do not contain personal details of staff or students.

If the school website is using a webcam – then this must be checked and monitored to ensure misuse does not occur accidentally or otherwise.

If showcasing school-made digital video work, we take care to ensure that students aren't referred to by name on the video, and that students' full names aren't given in credits at the end of the film.

Digital images - photographs and video clips - can now readily be taken using mobile phones. Extreme abuse is the so called 'happy slapping' incidents sent to others or posted onto a website, e.g. a recent case of a posting on YouTube. It is therefore important to ensure that the risk of inappropriate use is minimised. Staff are advised not to use their personal phone or camera **without permission** e.g. for a school field trip. If personal equipment is being used it should be registered with the school and a clear undertaking that photographs will be transferred to the school network and will not be stored at home or on memory sticks and used for any other purpose **than school approved business.**

Technical

Digital images / video of students need to be stored securely on the school network and old images deleted after a reasonable period, or when the student has left the school.

When we save pictures, we ensure that the image file is appropriately named. We do not use students' names in image file names

Edmonton County School Policy Statement on use of Digital and Video Images

In this 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 one administration officer
- 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 and telephone number. Home information or individual e-mail identities will not be published;
- Photographs 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 as part of the school agreement form when their child joins the school;
- Digital images /video of students are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless needed for resources for lessons, assemblies, school displays
- We do not use students' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- We do not include the full names of students in the credits of any published school produced video materials / DVDs;
- Students are only able to publish to their own 'safe' web-portal on the LGfL in school;
- Students are taught to publish for a wide range of audiences which might include governors, parents or younger students as part of their ICT scheme of work;

Students are taught about how images can be abused in their eSafety education programme.

Contents

What is Cyber Bullying?

Cyber bullying **is bullying through the use of communication technology like mobile phone text messages, e-mails or websites. This can take many forms for example:**

- **Sending threatening or abusive text messages or emails, personally or anonymously**
- **Making insulting comments about someone on a website, social networking site (eg: MySpace) or online diary (blog)**
- **Making or sharing derogatory or embarrassing videos of someone via mobile phone or email (such as 'Happy Slapping' videos)**

It should be noted that the use of ICT to bully could be against the law.

Abusive language or images, used to bully, harass or threaten another, whether spoken or written (through electronic means) may be libellous, may contravene the *Harassment Act 1997 or the Telecommunications Act 1984* for example.

Edmonton County School Cyber Bullying Policy

Use of the web, text messages, e-mail, video or audio to bully another student or member of staff will not be tolerated.

"Bullying can be done verbally, in writing or images, **including through communication technology (cyber bullying) e.g.: graffiti, text messaging, e-mail or postings on websites.** It can be done physically, financially (including damage to property) or through social isolation. Verbal bullying is the most common form.

If a bullying incident directed at a child occurs using email or mobile phone technology either inside or outside of school time.

1. Advise the child not to respond to the message
2. Refer to relevant policies including e-safety/acceptable use, anti-bullying and PHSE and apply appropriate sanctions
3. Secure and preserve any evidence
4. Inform the sender's e-mail service provider
5. Notify parents of the students involved
6. Consider delivering a parent workshop for the school community
7. Consider informing the police depending on the severity or repetitious nature of offence
8. Inform the LA e-safety officer

If malicious or threatening comments are posted on an Internet site about a student or member of staff:

1. Inform and request the comments be removed if the site is administered externally – there is a service available at Scotland Yard whose Computer Misuse Department will assist in removing offending/unsuitable video clips from 'YouTube' within 48 hours. This service is accessed via our safer schools officer
2. Secure and preserve any evidence
3. Send all the evidence at ww.ceop.gov.uk/contact_us.html
4. Endeavour to trace the origin and inform police as appropriate
5. Inform LA e-safety officer

Our e-safety lessons inform students of the importance of reporting inappropriate incidents involving the internet or mobile technology: it is stressed that they must be able to do this without fear.

How will Infringements be handled?

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

The following are provided as exemplification only:

Students

Category A infringements

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

The student is referred to the **head of phase**. The mobile phone is confiscated and a parent/carer is required to collect it from the school office

Category B infringements

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

The student is referred to the **head of phase** who will contact the parents/carer. There may be removal of Internet access rights for a period.

Category C infringements

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

Referred the head of phase who will invite parent/carer in for a discussion. Involvement of the School’s Safer Schools Officer . Removal of internet use for a period of time

Category D infringements

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

Referred the Head of Phase and the line managing Deputy Head teacher who will invite parent/carer in for a discussion. Involvement of the School's Safer Schools Officer. Removal of internet use for a period of time. Possible exclusion.

Staff

Category A infringements (Misconduct)

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

Referred to line manager and warning given

Category B infringements (Gross Misconduct)

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

Referred to Headteacher to follow school disciplinary procedures; report to LA Personnel/ Human resources, report to Police

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 students 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.

Contents

Child Pornography found?

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

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

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

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's e-safety. All staff will be required to sign the school's e-safety Policy acceptance form
- Students will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Students 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 students, staff and parents.
- Staff are issued with the 'What to do if?' guide on e-safety issues (see LGfL safety site).

What Do We Do If?

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Be sensitive to the situation.
2. Report to the head teacher/e- safety officer and decide whether to inform parents of any students who viewed the site.
3. Inform the school technicians and ensure the site is filtered.
4. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed intentionally by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you; do not view the misuse alone.
2. Report the misuse immediately to the head teacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head teacher should then:
   - remove the PC to a secure place.
   - Instigate an audit of all ICT equipment by the schools ICT managed service providers to ensure there is no risk of students accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action. (Contact Personnel/Human Resources)

  - Inform governors of the incident.

4. In an extreme case where the material is of an illegal nature:
    - remove the PC to a secure place and document what you have done.
    - contact the local police and follow their advice.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender’s e-mail service provider.
5. Notify parents of the students involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform the LA e-safety officer.

ICT Acceptable Use: Staff Agreement Form

Malicious or threatening comments are posted on an Internet site about a student or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to Child Exploitation and Online Protection (**CEOP**) Centre at ww.ceop.gov.uk/contact_us.html
4. Endeavour to trace the origin and inform Safer Schools Officer as appropriate.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child.

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA e-safety officer.
6. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the head teacher and e-safety officer.

Students should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

The use of the school communications systems and equipment, including electronic e-mail and Internet/Intranet systems, along with their associated hardware and software, are for official and authorised purposes only. However, we realise that the school communication systems may need to be used for other purposes in relation to our roles and therefore we need to be aware of and commit to the following guidelines:

- I will only use the school's Email / Internet / Intranet for purposes in a way that it will not interfere with the performance of my professional duties and will be of reasonable duration and frequency as deemed 'reasonable' by the Headteacher and Governing Body
- In using the school's email/internet/intranet for Professional purposes I will always use appropriate written language and not discriminate against, harass or victimise anyone I come into contact with, on any grounds, including: race, ethnic or national origin, gender, sexual orientation, marital status, religious or other beliefs, disability, HIV status, age, trade union involvement, having responsibilities for dependants, working on a temporary or part time basis (note that discrimination, harassment and victimisation include the use of language, making remarks, telling jokes, displaying materials or behaving in a way that may be interpreted as discriminatory, even if not directed at a particular individual(s)
- I will only use the approved, secure email system(s) for legitimate school interest such as enhancing professional interests or education
- I will not overburden the system or create any additional expense to the school
- I will conduct myself honestly and appropriately on the **Internet,** and respect the copyrights, software licensing rules, property rights, privacy and prerogative of others. The transmitting or downloading

of materials that are obscene, pornographic, threatening, racially or sexually harassing or in any way contravene the Equal Opportunities Policy is prohibited. I understand that Chat Rooms may not be visited nor any sites known to contain offensive material.

- I will not keep a personal diary on the Internet (whether at school or at home) where reference is made to the school without authorisation this is not advisable as such usage could cause harm to the reputation of the school and may undermine the confidence of our parent/carers.
- I will report any accidental access to inappropriate materials to the appropriate line manager
- I will not download any software or resources from the Internet that can compromise the network, or is not adequately licensed.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols
- I will not download or install any software or resources from the Internet on to my PC or laptop without checking with the Network Manager first as to its suitability or compatibility with Edmonton County's setup, or is not adequately licensed. I understand that the programmes which must definitely not be installed are Kazaa, Limewire, EMule and other similar peer to peer packages that are usually used for file swapping
- I will not use personal digital cameras or camera phones for transferring images of students or colleagues without permission
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice
- I will not allow unauthorised individuals to access Email / Internet / Intranet.
- I understand that all Internet usage will be logged and this information could be made available to my manager on request.
- I will only use LA systems in accordance with any Corporate policies
- I understand that this policy is binding to all school staff and that it applies to those staff deployed within the school who are employed by external Agencies or the Council and I will adhere to its principles. I understand that Breaches of the Policy and standards expressed in it could result in disciplinary action, including dismissal for serious offences.