Churchfields Infants' School, Nursery Unit & Language Facility

Managing the Internet Safely

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 pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils 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 provides many benefits to pupils and the professional work of staff through, for example:

- access to world-wide educational resources, including museums and art galleries;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide;
- collaboration between pupils, professionals and across sectors;
- access to learning wherever and whenever convenient.

The Internet enhances the school's management information and business administration systems through, for example:

- communication systems;
- improved access to technical support, including remote management of networks and automatic system updates;
- online and real-time ‘remote’ training support;
- secure data exchange between local and government bodies.

In support of this, the government provides a Standards Fund grant to support Local Authorities procure broadband services through local Regional Broadband Consortia (RBC). In London the London Grid for Learning (LGfL) is the RBC. London schools are connected onto this broadband network. The LGfL is part of the National Education Network (NEN). All English maintained schools are expected to be part of the NEN.

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 pupils. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a ‘No Blame’, supportive culture if pupils are to report abuse. Risks can be high outside school, so schools should consider extending an education programme to parents and carers.

Schools also need to protect themselves from possible legal challenge. The legal system continues to struggle with the application of existing decency laws to computer technology. It is clearly a criminal offence to hold images of child pornography on computers or to use Internet communication to ‘groom’ children. 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).

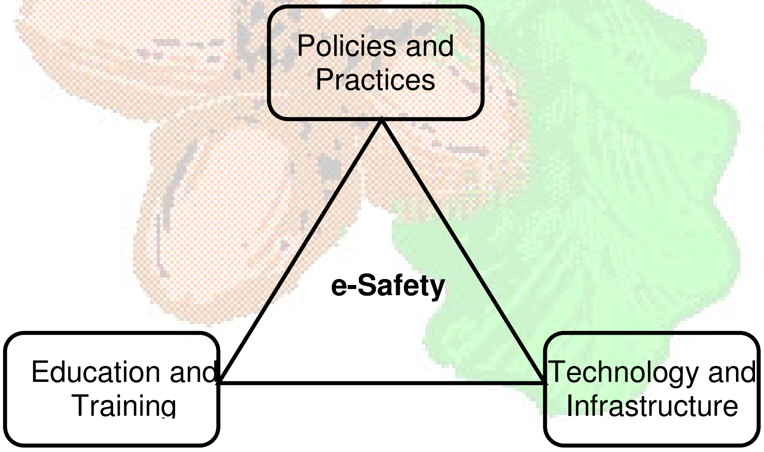
Schools help protect themselves by making it clear to users that the use of school equipment to view or transmit inappropriate material is “unauthorized” and infringements will be dealt with; and by ensuring that all reasonable and appropriate steps have been taken to protect pupils. Reasonable steps include technical and policy actions and an education programme for pupils and staff, (and parents).

There are three core elements for an institution to address when considering whole school e-safety:

Technology

Policy and Practices

Education



Technology and infrastructure: Background information

Schools should be connected to the NEN through their RBC. In London this is the London Grid for Learning (LGfL) who procure the broadband supply from Synetrix. Across this schools' fibre network, a range of services are provided. Internet filtering is a key service. This is updated and monitored by Synetrix working with their Third Party Suppliers. All London maintained schools should be part of this network.

Additionally, schools should have up-to-date anti-virus, anti-spyware and anti-spamware software and approved firewall solutions installed on their network. There are LGfL solutions provided for all of these and they should be set-up to be automatically updated so that networks remain up-to-date.

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, staff and pupils should not be able to download executable files and software.

Unfortunately, inappropriate materials will inevitably get through any filtering system. So, schools should be vigilant and alert so that sites can be blocked. Conversely, sometimes appropriate websites need to be unblocked. In larger schools, network managers will be able to block or liaise directly with Synetrix over this. In primary or smaller schools, there should be a named member of the ICT strategy team who manages the filtering policy for the school: this person may be the technician or the ICT coordinator, and the LA will usually be able to provide them with advice and back-up. By working together, London schools help to make the filtering system as effective as possible. .

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

London MLE (powered by Fronter), removes the difficulties of pupils publishing on a publicly available Web site because this is, by default, a safe, closed environment that only they will have access to via their username and password.

Schools should not send personal data across the Internet unless it is encrypted or sent via secure systems such as the DCSF COLLECT sites or an approved Learning Platform.

Technical and Infrastructure:

This school:

- Maintains the filtered broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- 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.;
- 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;

- 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;
- Has *the RM* network auditing software installed;
- Always ensures that children are supervised when accessing the internet.
- Uses class log-ins for pupils and individual logins for all other users;
- 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 or safely secured in the MLE;
- Ensures pupils only publish within appropriately secure learning environments such as their own closed secure Learning Platform.

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. Is it sufficient for a teacher or a learning support assistant to be in the area? Should Internet machines be placed in a common area between classrooms? Are there circumstances outside normal lesson time where pupils justifiably need access to the Internet?

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’.

As with other resources, the teacher needs to have checked and selected internet resources so they are appropriate for the age group and fit for purpose. Favourites or prepared links within the year group resources or MLE 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 Virtual Learning Environment or London MLE so pupils can, access out of school, from home etc. Some schools have put links on are put 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, for example, to a pornographic one. 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 (at a Corporate level). 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. LGfL guidance is available on the safety site.
[NB: Images usually have copyright attached to them.]

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 oracy and presentations skills, helping children consider their content and audience. However, schools should focus on using the social collaboration tools in the London Learning Platforms, rather than externally hosted Internet sites.

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 Becta advice or 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 and the other national regional grids for learning have 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: http://cms.lgfl.net/lgfl/web/vc

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

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 My Space, Facebook, 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 where adults hang out. 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 Platfom provides a safe environment for pupils to create their own webspace, 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. http://www.lgfl.net/lgfl/leas/camden/schools/podcast/

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 See additionally the Becta advice.

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.

Policy and procedures:

This 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 [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 pupils' ability.
- Never allows 'raw' image search with pupils e.g. Google 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 *system administrator / ICT Co-ordinator.* 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;
- 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 such as LGfL's Audio Network;
- Requires parents/carers, to individually sign an e-safety / acceptable use agreement form;
- Uses closed / simulated environments for e-mail with Key Stage 1 pupils;
- Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- 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;
- 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 daughter's / son's entry to the school;
- 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 programme: background information

It is a sad fact that pupils will occasionally be confronted with inappropriate material, despite all attempts at filtering and monitoring. Pupils (and staff) need to know how to respond responsibly if they come across material that they find distasteful, uncomfortable or threatening. For example: to turn off the monitor and report the incident to the teacher or ICT manager for inclusion in the list of blocked sites.

Pupils and staff must learn to recognise and avoid risks online – to become 'Internet Wise'. To STOP and THINK before they CLICK. Both need to understand how to ensure personal information is, and remains, private. Staff must not confuse or compromise their professional role with any personal online activity, for example inviting pupils into their personal social networking site.

Pupils also need to be 'savvy' about what they read, hear and see. In the same way that the quality of information received via radio, newspaper and television is variable, everyone needs to develop skills in selection and evaluation of Internet – based information. Just because something is published in text or on-line does not make it fact. It's therefore important that any education programme links to activities to help pupils evaluate what is fact, what is fiction and what is opinion, and that pupils consider whether something is plausible or biased.

Information literacy skills therefore need to be taught. These include skills to 'read' content – (contextual clues including design, lay-out, text, use of images, links to and from the content), where the material originates from and how the content can be validated. *See the LGfL eSafety site for further guidance*.

More often in schools, pupils will be accessing reliable material but need to select that which is relevant to their needs, for instance to answer a homework question. Pupils should be taught research techniques including how to narrow down searches and how to skim and scan content.

Pupils also need to understand the dangers of using unfiltered web access outside school at a location where parental controls or filtering have not been enabled. Pupils should be encouraged never to chat through a website or over a webcam with people that they do not already know and trust in the real world and not to post details about themselves to a website, in a message or in a social networking environment..

Pupils and staff need to know how to deal with any Cyber Bullying incidents. Pupils need to know about the national agencies, such as Child Exploitation Online Protection (CEOP), http://www.ceop.gov.uk/ – so that in an extreme case, they know how to "report abuse". See key organisation links: http://cms.lgfl.net/lgfl/web/safety/organisations

Where they do communicate or publish work outside of the LGfL environment or other approved educational environment, it should be under adult supervision wherever possible.

Pupils and staff need to know appropriate / netiquette in their general communications:

So, to enable this, e-safety must be built into schemes of work as appropriate, to ensure pupils are 'taught' safe behaviours and practice and the school must foster a 'No Blame' culture to ensure pupils feel able to report any abuse, misuse or inappropriate content. Key resources include Becta's Signposts to Safety guidance; together with resources from CEOP's Think U Know site.

Parents have an important role in supporting safe and effective use of the Internet by pupils – so schools need to consider a rolling training programme of support.

See parents' resources: http://cms.lgfl.net/lgfl/web/safety/resources

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;
- Ensures that staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report abuse;
- Has a clear, progressive e-safety education programme throughout the Key Stage. 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 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, photographs and videos.
    - to understand why they must not post pictures or videos of others without their permission;
    - to have strategies for dealing with receipt of inappropriate materials;

- 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 encrypt data where the sensitivity requires and that they understand data protection and general ICT security issues linked to their role and responsibilities;
- 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 appropriate parents materials
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.