Roe Green Infant and Strathcona School
E-Safety Policy

Managing the Internet Safely

Technical and Infrastructure approaches

This school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the ‘private’ National Education Network;
- Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved ‘web filtering management’ status;
- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc and network set-up so staff and pupils cannot download executable files;
- Uses individual, audited log-ins for all staff users;
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Only uses approved or checked webcam sites;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Provides *highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils*; Uses Londonmail with students as this has email content control and the address does not identify the student or school;
- Provides staff with an email account for their professional use, *London Staffmail / LA email* and makes clear personal email should be through a separate account;
- *Uses teacher ‘remote’ management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, in the ICT suite;*
- *Has additional local network auditing software installed;*
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;

Policy and procedures:

This school:

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within the appropriately secure school's learning environment, such as the London MLE.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg yahoo for kids or ask for kids
- Is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search;
- Informs users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the teacher. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL (Atomwide) as necessary;
- Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named child protection officer has appropriate training;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Provides Esafety advice for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Education and training:

This school:

- Fosters a ‘No Blame’ environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Teaches pupils and informs staff what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report any abuse;
- Has a clear, progressive e-safety education programme throughout all Key Stages, built on LA / London / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
    - to STOP and THINK before they CLICK
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to skim and scan information;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand ‘Netiquette’ behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line ‘friends’ may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
    - [for older pupils] to understand why and how some people will ‘groom’ young people for sexual reasons;
    - Extremism
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line;

  on-line gaming / gambling;

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes training available annually to staff on the e-safety education program;
- Runs a rolling programme of advice, guidance and training for parents, including:
  - Information leaflets; in school newsletters; on the school web site;
  - demonstrations, practical sessions held at school;
  - distribution of ‘think u know’ for parents materials
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for Online Safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL • To be responsible for ensuring that staff receive suitable training to carry out their Online safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the Online Safety Co-ordinator / Officer • To ensure that there is a system in place to monitor and support staff who carry out internal Online safety procedures(e.g. network manager)
Online Safety Co-ordinator / Designated Child Protection Lead	• takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policies / documents • promotes an awareness and commitment to Online safeguarding throughout the school community • ensures that Online safety education is embedded across the curriculum • liaises with school Computing technical staff • To communicate regularly with SLT and the designated Online safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident • To ensure that an Online safety incident log is kept up to date • facilitates training and advice for all staff • liaises with the Local Authority and relevant agencies • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • sharing of personal data

Role	Key Responsibilities
	• access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • Online bullying and use of social media
Governors / Online safety governor	• To ensure that the school follows all current Online safety advice to keep the children and staff safe • To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the Online Safety Governor will include: • regular review with the Online Safety Co-ordinator / Officer (including Online safety incident logs, filtering / change control logs)
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum • To liaise with the online safety coordinator regularly
Network Manager/technician	• To report any online safety related issues that arise, to the Online safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school IT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • LGfL is informed of issues relating to the filtering applied by the Grid

Role	Key Responsibilities
	• that he / she keeps up to date with the school's Online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • that the use of the network / Virtual Learning Environment (LEARNING PLATFORM) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator / Officer /Headteacher for investigation / action / sanction • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's online security and technical procedures

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use <STRONG passwords for access into our MIS system>.
- We require staff to change their passwords into the MIS, LGfL USO admin site, <other secure system> <every 90 days / twice a year>.

Policy written December 2015. To be reviewed annually.

Appendix 1

Internet policy and procedures: background information

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

Surfing the Web

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

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

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

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

Search Engines

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

Images usually have copyright attached to them which is an issue commonly overlooked but a key teaching point to pupils and staff.

Collaborative Technologies

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

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

Webcams and Video Conferencing

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

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

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

Social Networking Sites

These are a popular aspect of the web for young people. Sites such as Facebook, My Space, Habbo Hotel, Bebo, Piczo, and YouTube allow users to share and post web sites, videos, podcasts etc. It is important for children to understand that these sites are public spaces for both children and adults. They are environments that should be used with caution. Users, both pupils and staff, need to know how to keep their personal information private and set-up and use these environments safely. [See Education programme]

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

Podcasts

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

Chatrooms

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

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

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