

	Name of School	Manor Primary School
	Policy review Date	September 2015
	Date of next Review	September 2017
	Who reviewed this policy?	Kate McGee & Petra Collins (HT & AHT/ICT Leader)

Policy - Managing the Internet Safely

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.
- 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 regularly having LA health checks on the network;
- Utilises caching as part of the network set-up;
- 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;
- Uses the Hector Protector screen blanker that pupils can activate should they find something on their screen which makes them feel uncomfortable;
- Uses individual log-ins for pupils and 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;
- Uses 'safer' search engines with pupils such and activates 'safe' search where appropriate;
- Ensures pupils only publish within appropriately secure learning environments such as their own closed secure LGfL portal or Learning Platform.

Policy and procedures: suggested strategy statements

This school:

- Supervises pupils' use at all times, as far as is reasonable.
- 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;
- We have additional user-level filtering, so adapt filtering to pupil or staff usage;
- 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, using child-friendly search engines where more open Internet searching is required;
- 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 they must report any failure of the filtering systems directly to the ICT subject leader or the E-safety Officer. 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 pupils (and their parent/carer) from Key Stage 1 and 2, to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;
- 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.

The philosophy of sharing information across the Internet has increased the risk of pupils infringing copyright and committing Plagiarism (the theft of ideas and works from another author and passing them off as one's own). For older pupils, there are numerous ‘essay bank’ websites offering access to essays for free or for a fee, often encouraging students to submit their own works. Students should be aware of the issues around copyright and encouraged to look for copyright information on websites, so reinforcing their understanding of the importance this issue. They also need to be aware that plagiarism is not only cheating but where sufficient is copied, an illegal infringement of copyright also constitutes a criminal offence.

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 the

DfES/Becta [Internet Proficiency Scheme](#) at Key Stage 2 and Becta's [Signposts to Safety](#) guidance for Key Stages 3 and 4; 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: suggested strategy statements

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 pupils and 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 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 some search engines / web sites that are more likely to bring effective results;
 - to know how to narrow down or refine a search;
 - to understand how search engines work;
 - 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 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;

- 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 'think u know' for parents materials
 - suggestions for safe Internet use at home;
 - provision of information about national support sites for parents.