	Name of School	**Brettenham Primary School**
	Policy review Date	**October 2022**
	Date of next Review	**October 2023**
	Who reviewed this policy?	**Headteacher/ICT Assistant**

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;

- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;.

- 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 users - the London USO system;;

- 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;

- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;

- 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;

- Uses security time-outs on Internet access where practicable / useful;

- 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;

- *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 and students are aware of the acceptable use agreement form displayed in the ICT suite and understands that they must report any concerns;

- Ensures pupils only publish within the appropriately secure school's learning environment, such as the Purple Mash MLE or the school's panning folder

- 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.

- 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 class teacher or ICT Assistant Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL (Atomwide) as necessary;

- 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 E-safety 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; o to have strategies for dealing with receipt of inappropriate materials; o [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;

- 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; online 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: o Information leaflets; in school newsletters; on the school web site; o demonstrations, practical sessions held at school; o distribution of 'think u know' for parents materials o suggestions for safe Internet use at home; o provision of information about national support sites for parents.

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'.

.

Social Networking Sites – not available in this school

These are a popular aspect of the web for young people. Sites such as Facebook, My Space, Habbo Hotel, Bebo, Piczo, Instagram , whatsapp and only with supervision You Tube 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. 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.

Chatrooms

All chatrooms are blocked at school.

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.

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.