Sir Thomas Abney Primary School

Internet Acceptable Use Policy

December 2014

Internet Acceptable Use Policy

We all shine

We pride ourselves on being an inclusive school, where we celebrate diversity and difference and acknowledge the richness that this brings to our school community. We aim to provide opportunities for all children to access a broad, balanced and creative curriculum, regardless of age, attainment, ethnicity, language or background that is personalised to meet children's individual needs.

The children at Sir Thomas Abney are fully aware of different forms of bullying, including cyber-bullying and actively try to prevent it from occurring. Bullying in all forms are very rare and dealt with highly effectively.

Technical and Infrastructure approaches

At Sir Thomas Abney we:

- have educational filtered secure broadband connectivity through the LGfL and so connect to the 'private' National Education Network;
- Use 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;
- Use USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensure the network is healthy through use of Sophos anti-virus software (from LGfL) and network set-up so staff and pupils cannot download executable files;
- Use 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 where staff need to access personal level data off-site;
- Block all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblock other external social networking sites for specific purposes / Internet Literacy lessons;
- Use security time-outs on Internet access where practicable / useful;
- Provide *highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils* where used; Use Londonmail with students as this has email content control and the address does not identify the student or school;
- Provide staff with an email account for their professional use via the Learning Trust, and make clear that personal email should be through a separate account;
- Work in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Ensure 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:

Sir Thomas Abney:

- Is vigilant in its supervision of childrens' 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 children have signed an acceptable use agreement form and understand that they must report any concerns;
- Ensures children only publish within the appropriately secure school's learning environment.
- Requires staff to preview websites before use [where not previously viewed or cached]. Plans the curriculum context for Internet use to match children's 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 children e.g. Google or Lycos image search;
- Informs users that the Internet use is monitored;
- Informs staff and children that that they must report any failure of the filtering systems directly to the *Headteacher and ICT technician*. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL (Atomwide) as necessary;
- Requires children to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;
- 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 and safeguarding system;
- Provides advice and information on reporting offensive materials, abuse/bullying etc available for children, staff and parents/carers
- Provides e-safety advice for children, staff and parents/carers;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Education and training:

At Sir Thomas Abney we:

- Foster a 'No Blame' environment that encourages children to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Teach children and inform staff of 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.
- Ensure children and staff know what to do if there is a cyber-bullying incident;
- Ensure all children know how to report any abuse;
- Have a clear, progressive e-safety education programme throughout all Key Stages, built on LA / London / national guidance. Children 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 children] 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 children] to understand why and how some people will 'groom' young people for sexual reasons;

- Ensure that when copying materials from the web, staff and children understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensure that staff and children 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;
- Ensure staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Make training available annually to staff on the e-safety education program;
- Run 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.

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 children in an embarrassing or potentially dangerous situation.

Surfing the Web

Aimless surfing should never be allowed. It is good practice to teach children 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 children can experience overload and failure if the set topic is too open-ended. It is not sensible to have younger children 'searching the Internet'.

Children 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 children.

Teachers' web site selections for various topics can be put as links on the school website so children can have access out of school, from home 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.

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 the 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 children 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 presentation skills, helping children consider their content and audience.

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 the school's website 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

Children 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 children.

The highest risks lie with streaming webcams [one-to-one chat / video] that children use or access outside of the school environment. Children 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, Bebo, 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 children and staff, need to know how to keep their personal information private and use these environments safely.

Most schools will block such sites. However, children 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. Children 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.penguinchat.com

Sanctions and infringements

The school's Internet Acceptable Use policy needs to be made available and explained to staff / Governors, children and parents/carers, 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 behaviour policy.*

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.