Education is that which liberates

B50 E-Safety Policy

The Swaminarayan School

260 Brentfield Road
Neasden
NW10 8HE
Tel No: 0208 965 8381
Fax No: 0208 961 4042
www.swaminarayan.brent.sch.uk

Governor in charge of E-Safety: Tarun Patel
Author: M Chouder
Last reviewed: M Chouder, 17/09/2018
Next review date: June 2019

Swaminarayan School

E-Safety Policy

Managing the Internet Safely

Technical and Infrastructure approaches

This school:

- Has two external agencies, **Smoothwall** provides security and **NK Computers** provides maintenance of machines and servers for the school.
- Has a filtered secure broadband connectivity;
- Uses the **Smoothwall** filtering system which blocks sites that fall into categories such as pornography, race hatred, extremism, gaming, sites of an illegal nature, etc. although it is impossible for the filter to block 100% of inappropriate material, nevertheless the school does everything it can to minimise the chances of this occurring.
- Ensures network healthy through use of Sophos anti-virus software etc. and network set-up so staff and pupils cannot download executable files, except for named administrators;
- Uses individual, audited log-ins for all staff and pupils in the Senior School, pupils in the Junior School login using a class login;
- Uses 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 by the school;
- Sites can only be unblocked by contacting Smoothwall and providing evidence that the site you need to access contains educational content, and not inappropriate material;
- Has blocked pupil access to music download or shopping sites – except those approved for educational;
- Uses security time-outs on Internet access where practicable/useful;
- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- ***NK Computers*** *uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;*
- Work in partnership with **NK Computers** 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 services and policies / requires the Technical Support Provider to be up-to-date with services and policies;
- Monitoring of pupil PCs is provided through **NetSupport** software.

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 pupils in the Junior School have signed an acceptable use agreement form which is fully explained and used as part of the teaching programme; pupils also understand that they must report any concerns. In the Senior School E Safety is taught and tested on it, as part of the curriculum.
- Ensures pupils only publish within the appropriately secure school's learning environment, such as the school's Google Apps for Education account, the school website or other school approved websites.
- Requires staff to preview websites before use[where not previously viewed or cached] and 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 safesearchforkids(KS1)
- Is vigilant when conducting 'raw' image search with pupils e.g. Google, Lycos or other search engines image search – again utilising google safe 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 immediately. Our system administrator(s)logs or escalates as appropriate to the Technical service provider as necessary;
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale of linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.
- 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;
- E-bullying. The school takes very seriously the matter of e-bullying, which can be described as using technology to communicate words and/or images that might cause distress or harm to another person.
- 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 designated safeguarding lead 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 Local Authority. See Safeguarding policy for advice on "sexting".
- Complaints of internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.
- The school respects the rights of each family to decide whether or not to apply for access of the internet during school time.

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 national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

    - Integrated in PSHCE lessons when discussing electronic bullying
    - 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;

  - to understand and recognise that some people on the internet have extremist views and to recognise and manage risk, make safer choices, and recognise when pressure from others threatens their personal safety and wellbeing;
  - to develop a resilience to radicalisation through the internet by discussing the issues of extremism so pupils know how and when to get help (see PSHCE policy for more information);

- 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;
- 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;
  - 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 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.

The school makes no warranties of any kind, whether expressed or implied, for the service it is providing. The school will not be responsible for any damages the user suffers while on this system. These damages include loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by negligence, errors or omissions. Use of any information obtained via the internet is at the users own risk. The school specifically denies any responsibility for the accuracy or quality of information obtained through its services.

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 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, 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

To prevent risk pupils under no account are permitted to access chatrooms. Whilst we recognise the advancement of technological communications our e-safety guidance remains rigorous.

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.

Last reviewed: M Chouder, 17/09/2018