St Paul's Church of England Primary School
E Safety Policy

Adopted by: Curriculum & Achievement Committee
On: Wednesday 17th October 2018
Review: October 2021

Introduction: Why is Internet access important?

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; indeed ICT is now seen as a functional, essential life-skill along with English and mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet provides many benefits to pupils and the professional work of staff through, for example:

- access to world-wide educational resources, including museums and art galleries;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide;
- collaboration between pupils, professionals and across sectors;
- access to learning wherever and whenever convenient.

The risks

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people. Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information (of a sexual nature, on weapons, crime and racism for example) that would be considered inappropriate and restricted elsewhere. In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of, and respond responsibly, to any risk.

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;
- Ensures network health through appropriate anti-virus software etc.
- 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;

- Never allows pupils access to chat rooms or sites with chat facilities;
- Never sends personal data over the Internet
- Makes staff aware of taking personal level data off-site unless it is on an encrypted device;
- Whenever possible, uses 'safer' search engines with pupils such as https://swiggle.org.uk and activates 'safe' search where appropriate;

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, and our policy is to help ensure children know what to do in these situations.

Surfing the Web

Aimless surfing is not allowed at St Paul's. Pupils to use the Internet in response to a question or problem – as a rule, children should be able to answer the question "Why are we using the Internet?" Staff are aware that websites should always be previewed and checked carefully before they are used by children.

Search Engines

Some common Internet search options are high risk, for example Google image search, and should be used with caution. Google image search can be set-up to run in 'safe' mode although this is not fully without risk.

Collaborative Technologies: Webcams

Pupils can search on the Internet for 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 are made aware of the dangers through e-Safety lessons.

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, and have recommended (though not legal) age limits. 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 and responsibly. *(See Acceptable Use Policies)*

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.

Chatrooms

Many sites – particularly games (including console based games) - allow for 'real-time' online chat. Again, children should only be given access to educational, moderated chat rooms as part of a planned computing lesson. 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 those on Roblox or Fortnite.
(See additionally www.thinkuknow.org)

Snapchat, Instagram and other mobile apps

Snapchat and Instagram are mobile apps that are used to share images and video with other users. Despite having recommended age requirements, these apps are used by a significant proportion of children. Through the delivery of e-safety lessons, children are made aware of potential problems with these apps through both viewing inappropriate content or being encouraged to post inappropriate content as well as the importance of privacy settings.

Policy and procedures

This school:

- Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;
- Uses the pan-London (LGfL) filtering system which blocks sites that fall into categories such as (and not limited to) pornography, race hatred, gaming, sites of an illegal nature;
- Previews all websites before use
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Informs users (staff, visitors and children) that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the ICT & Computing / e-safety Coordinator;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks 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 (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;*
- Only introduces email to Key Stage 2 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 programmes;
- 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 child'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.

Additionally, our 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 a screen 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.
- 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 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;
- Create a 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.

Sanctions and infringements

- The school's Internet e-safety / Acceptable Use Policy (AUP) is available to staff / Governors, pupils and parents, with all signing acceptance / agreement forms appropriate to their age and role. This also includes sanctions for infringing the AUP in line with the school's behavior policy.

- Following any serious incident (for example evidence of indecent images or offences concerning child protection that may be contained on school computers), the matter will be immediately referred to the Police.

Safety Teaching

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;
- older Key Stage 2 children to understand why and how some people will 'groom' young people for sexual reasons;
- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;