St Mary's and St Peter's C of E School

Online Safety Policy

We believe high standards of care and love are an integral part in the quality of teaching and learning across the whole curriculum. Our school Christian vision of 'Life in all its fullness' applies to all areas of our school. The two great commandments given by Jesus will underwrite the life of our school; they are to 'love God' and to 'love your neighbour as yourself'. It is our aim for both of these instructions to be evident in the whole life of the school, in the relationships between all members of the community; pupils, staff and parents.

St Mary's and St. Peter's school fully recognises its moral and statutory responsibility to safeguard and promote the welfare of all pupils and staff. Our Online Safety Policy is one of a range of documents which set out the safeguarding responsibilities of the school. We wish to create a safe, welcoming and vigilant environment for children and staff where they feel valued and are respected.

Aims

- To outline the schools provision for online safety teaching to the school community.
- To outline the technical and behavioural structures in place to protect the school community.

Internet Acess

- Access to the Internet takes place via a range of devices: PCs, laptops, netbooks or tablets. Some of these devices require personal authentication (via either network or Google Education credentials) but some (such as the iPads) allow free access.
- At Key Stage 1, access to the Internet should only take place under direct supervision, preferable in groups, and using vetted on-line materials.
- At Key Stage 2, Internet access should, as much as is practical, take place via a credential-regulated device. In either case, Internet use should only take place with permission from a member of staff present during its use.
- KS2 students who have signed the Acceptable Use Policy will be permitted a level of independent access to the Internet (appropriate to their age and in-line with curriculum requirements). Parents will be asked to sign and return the AUP along with their children to confirm their consent.
- Personal e-mail accounts may be provided to individual KS2 users, but will be limited to internal and approved communications only.
- Staff access to the Internet is subject to a more comprehensive Acceptable Use Agreement.

Infrastructure

The school is responsible for ensuring that the school infrastructure, network and Internet service is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the following sections will be effective in carrying out their online safety responsibilities:

- School IT systems are managed in ways that ensure the school meets the online safety technical requirements outlined in the Data Security Policy and Acceptable Use Policy and any relevant Local Authority Online Safety Policy and guidance;
- There are regular reviews and audits of the safety and security of school ICT systems;
- Servers, wireless systems and cabling are securely located and physical access to such systems is restricted;
- All users have clearly defined access rights to school IT systems;
- The administrator passwords for the school IT system are kept secure and only known to the School Technician, Computing Leader and approved external technical services;
- Individual users are responsible for the security of their username and password and must not allow others unsupervised access the systems using their credentials. Any suspicions or evidence of a misuse of passwords must be immediately reported to the Computing leader, on-site technician or the head teacher;
- The school's Internet service is filtered by the LGfL service, in accordance with their policies, which the school abide by;
- The LGfL filtering system serves to enforce SafeSearch on Google – the recommended search engine for use at SMSP.
- Overriding of the LGfL filtering settings can only be performed under approval from the Computing leader or a member of senior management after due consideration to the risks & benefits.
- The Computing leader and on-site technician regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users' activity;
- Appropriate security measures are in place (in the form of access keys, encryption, passwords and physical security) to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Established logins are provided for limited, temporary access of "guests" (e.g. trainee teachers, supply staff, visitors) onto the school system.
- An agreed policy is in place (see Acceptable Use Policy & Data Security Policy) regarding the extent of personal use that users (staff / students / guests) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place (see Acceptable Use Policy) that details staff permissions to install applications on school devices.
- The school infrastructure and individual workstations are protected by up-to-date virus software that is provided and updated by LGfL.
- Personal data is not permitted to be sent over the internet or taken off site unless safely encrypted or otherwise secured (see Data Security Policy).
- The school employs a monitoring system to record and notify the eLearning coordinator of breaches in this policy, including potential Child Protection issues. All users of the school IT systems are subject to this monitoring and are made aware of this through the Acceptable Use Policy. At present, this system does not cover all devices in use at SMSP, so staff are expected to not rely on this system and are required to supervise student activities.

Online Safety Information

Online safety education for students will be provided in the following ways:

- A planned online safety programme ("Switched On to Online Safety") is provided as part of Computing and/or PHSE lessons. The themes of these lessons are tailored to the age-range, technological experiences and practical applications of the individual year groups;
- Key online safety messages are reinforced as part of a planned programme of assemblies;
- Students are helped to understand the need for the Acceptable Use Policy and encouraged to adopt safe and responsible use of IT, the Internet and mobile devices (where appropriate to the year group) both within and outside school;
- Rules for the appropriate and safe use of IT systems are presented to children every time they access the network via PC or laptop;
- Staff are expected to act as good role models in their use of IT, the Internet and mobile devices.

The school will seek to provide information and awareness to parents and carers through:

- Letters, newsletters, pamphlets and the school website;
- Internet Safety talks;
- Reference to relevant online safety websites.

All staff members should ensure their own understanding of online safety issues is kept up to date through:

- Training sessions;
- Reference to relevant online safety websites;
- Online safety bulletin updates;
- Informal updates from the Computing leader or school technician.

Online Safety Curriculum

Online safety should be a focus in all areas of the curriculum and staff are expected to reinforce online safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet (e.g. using search engines), staff should be vigilant in monitoring the content of the websites the young people visit. In such cases, children should be guided as to appropriate search terms to use and any terms best avoided. Free searching of Google Images should not be encouraged or expected by teachers.
- Students should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of Digital Image and Work

The school will inform and educate users about the risks associated with posting material online and will implement policies to reduce the likelihood of the potential for harm:

- During online safety sessions, students will be educated about the issues of consent and the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- Staff are allowed to produce digital media (photos/video/audio) of students to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of that media (see Data Security Policy & Acceptable Use Agreement).
- Care should be taken when producing digital media that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute digital media of others without their consent.
- Parents are encouraged to not film school events such as sports days, fetes and school plays and instead enjoy the spectacle. Parents will be given time to take photos provided doing so will not cause a disturbance to others and there are no issues with relation to copyright.
- Parents must not post photos taken at a school event of pupils, other than their own children, on social networking sites.
- Under the terms of the Data Protection Act 1998 and the General Data Protection Regulations, parents, friends and family members can take images of their children and friends participating in school activities for family and personal use. If a recording is not for personal use (e.g. with a view to selling the video) then consent of other parents whose children may be on film would be required. Without this consent, the aforementioned regulations would be breached.

Online Publishing

- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be published anywhere on any school website or digital attachment - particularly in association with photographs & video.
- Parents will be requested to provide consent for the use of their child's image on any public forum (such as the school website). Where barriers may prevent informed consent (e.g. parents with low English language skills), additional support will be provided.
- A student's work can only be published with the permission of the student.
- Consent is not required where either individuals cannot be identified or they form part of a large crowd at a public event.
- Parental consent can be withdrawn or changed at any time in writing.
- Students should only publish material to approved, educationally-related websites, with the authorisation of their parent or teacher (where the material does not contravene other restrictions regarding student content).
- Students should only publish material that is:
    - not copyrighted;
    - their own work (or with permission of the owner);
    - not offensive or embarrassing to another individual;
    - approved by a member of staff.

Online Activities

- **Forums** and other such discussion **groups** will not be made available to students unless they are moderated by a responsible person or organisation and are directly linked to an educational activity. In such circumstances, access should be restricted to class-level accounts with teachers retaining the relevant usernames and passwords.
- Students will not access **social networking sites**, for example Facebook.
- Children should use only regulated, educational **chat** environments. This use will be supervised and the importance of chat room safety emphasised.
- Student use of personal **messaging services** (for example, 'WhatsApp') is not permitted.
- A risk assessment will be carried out before students are allowed to use a new technology in school.
- Use, by students, of **video conferencing** systems should only take place under staff supervision and for focussed educational tasks.
- Students should not be permitted to **register** themselves on external sites without parental consent. Teachers may, however, create 'class' accounts where educationally relevant without parental consent.
- The school may register students on external websites where the school has an active, approved subscription for educational purposes and the risks & benefits have been adequately considered.

Communication

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure.
- Users need to be aware that email communications may be monitored by automated systems reporting to the eLearning coordinator and school technician.
- Users must immediately report, to the nominated person, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students/parents (email, text message, eLearning platform, chat, etc.) must be professional in tone and content. These communications may only take place on official school systems. Staff may use their personal mobiles to contact parents, but should avoid this where possible. Personal email addresses, text messaging, public chat, social networking programmes must not be used for these communications. The only exception to this rule would be if, while on a school trip, a staff member has pressing need to contact a parent via text using their own or a school device.
- In general, staff should not communicate directly with parents using their individual staff email account. All email communications between teaching staff and parents should be via the school office or year group email accounts. Specific school roles (SLT, SENCo, Office staff) may use their individual staff accounts in the interests of expediency and confidentiality.
- Where required for educational tasks, whole class or group email addresses will be used at KS1, while students at KS2 and above may be provided with individual school email addresses. These accounts should be monitored by an adult and only active when required.
- Students will be taught about email safety issues, such as the risks attached to the use of personal details. They will also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Responding to Incidents

It is hoped that all members of the school community will be responsible users of IT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or (very rarely) deliberate misuse.

Apparent or actual misuse that appears to involve illegal activity will be reported immediately to the police for further investigation. Examples of illegal misuse include:

- child sexual abuse images;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material;
- other criminal conduct, activity or materials.

Incidents of misuse will be dealt with as soon as possible and in a proportionate manner. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as outlined in the Acceptable Use Policy.

Monitoring and Review

The monitoring of online safety is the responsibility of everyone and, yet the Computing leader and the Leadership Team will take a lead on this.

Policy Date: November 2021

Review Date: November 2022