# Online Safety Policy

## St Mary's Church of England Primary School and Nursery

| | | | |
|---|---|---|---|
| **Approved by:** | LGB | **Date:** | Sept 2022 |
| **Last reviewed on:** | Sept 2023 | | |
| **Next review due by:** | Sept 2024 | | |

**Introduction**

This policy refers to and encompasses the use of computers, internet technologies and other forms of electronic communications by children and staff at St Mary's C of E Primary School and Nursery.

It highlights the need to educate children about the benefits and risks of using information communication technologies (ICT) and details the safeguards that are in place to enable children and staff to use ICT safely. This document also makes explicit, the conditions regarding: mobile technologies; data protection; communication; social media and cloud storage.

This policy has been written by the School, building on the South West Grid for Learning (SWGfL) Policy and government guidance. It has been made available to parents and staff via the school website and approved by the Governing Body.

**Context and Background**

The Technologies

ICT in the 21st Century has an all-encompassing role in the lives of children and adults. New Internet and online technologies are enhancing communication and the sharing of information.

Current and emerging Internet and online technologies used in school and in many cases used outside of school by children include:

- The Internet
- Email
- Instant messaging
- Web based voice and video calling
- Online chat rooms
- Online discussion forums
- Social networking sites
- Blogs
- Podcasting
- Video broadcasting sites
- Music and video downloading
- Technology, including mobile phones with camera and video functionality
- Smart phones with email, messaging, apps and Internet access.

**A Whole School Approach To The Safe Use Of ICT**

We aim to create a safe ICT learning environment for pupils by supporting them to develop a strong awareness of the type of dangers that exist when using the Internet and linked technology, and proactively teaching them how to manage these.

**Roles And Responsibilities**

The following section outlines the Online Safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the governors receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor. The role of the Safeguarding Governor will include:

- regular meetings with Online Safety Lead and monitoring of Online Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to the Local Governing Body

Headteacher and Senior Leaders

- The Headteacher has a duty of care in ensuring the safety (including Online Safety) of members of the school community, though the day-to-day responsibility for Online Safety.

- The Headteacher and at least one other member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff – see the flowchart on dealing with Online Safety incidents included in a later section "Responding to incidents of misuse".
- The Headteacher and Senior Leaders are responsible for ensuring that the relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to colleagues who take on important monitoring roles.

Technical staff

Technical Staff are responsible for ensuring:

- that the school's / technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required Online Safety technical requirements and any Trust / other relevant body Online Safety Policy / guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy in which passwords are regularly changed.
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

that they keep up-to-date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant.

- that use of the network / Internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and Online Safety Coordinator for investigation.
- that monitoring software / systems are implemented and updated as agreed in school policies.

Teaching And Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of Online Safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy and Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher / action / sanction
- all digital communications with pupils / parents / carers are on a professional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and Acceptable Use Policies pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- lessons where the Internet is used are pre-planned so that pupils are 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.

Designated Safeguarding Lead (DSL)

The DSL should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Pupils

Pupils

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- need to understand the requirement to avoid plagiarism and uphold copyright regulations

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the School's Online Safety Policy covers their actions out of school if related to their membership of the school.

Parents / Carers

Parents / carers play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school's Online Safety website page and information about national and local Online Safety campaigns or literature. Parents and carers will be encouraged to support the school in promoting good Online Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and online pupil records
- their children's personal devices in the school where this is allowed.

**Policy Statements**

**Education – Pupils**

The education of pupils in Online Safety is an essential part of the school's Online Safety provision. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience. Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages across the curriculum. The Online Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities. It will be provided in the following ways:

- A planned Online Safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Key Online Safety messages should be reinforced as part of a planned programme of assemblies and PSHE activities.
- Pupils should be taught to be critically aware of the content they access online, in all lessons.
- Pupils should be supported to build resilience to radicalisation by having access to a safe environment for debating controversial issues and being supported to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use of communications technologies both within and outside school.
- Staff should act as good role models in their use of digital technologies, the Internet and mobile devices.
- In lessons where Internet use is pre-planned, it is best practice that pupils 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 pupils are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the children visit.

**Education – Parents / Carers**

Many parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the Internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, the Online Safety page on the school's website
- Parent/carers Online Safety workshops
- High profile events e.g. Safer Internet Day
- Reference to relevant websites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers www.thinkuknow.co.uk

**Education & Training – Staff / Volunteers**

It is essential that all staff receive Online Safety training and understand their responsibilities as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Online Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the Online Safety training needs of all staff will be carried out regularly
All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify Online Safety as a training need within the Performance Management / Appraisal process.
- The Computing Leadership Team will receive regular updates through attendance at external training events e.g. from SWGfL / LA / other relevant organisations and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff team meetings / INSET days.
- The Computing Leadership Team or other nominated person will provide advice or training to individuals as required.

**Training – Governors**

Governors should take part in Online Safety training. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation e.g. SWGfL.
- Participation in school training or information sessions for staff or parents.

**Technical – infrastructure / equipment/ filtering and monitoring**

Ensure as far as is reasonably possibly, that policies and procedures approved within this policy are implemented. This will include ensuring that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- Users are responsible for the security of their username and password.
- The "administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated Senior Leader and kept in a secure place e.g. school safe.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and Internet use is logged and regularly monitored.
- The Online Safety Lead is responsible for termly audits of filtering logs.
- All filtering issues should be reported immediately to Online Safety Lead who will consult technical support if necessary.
- The school has provided differentiated user-level filtering whereby the staff can enter their personal SWGfL login to disable the filter for teaching materials.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.

Use of digital and video images

- The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the GDPR). To respect everyone's privacy and in some cases for protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims but must follow school policies concerning the sharing, distribution and publication of those images. Such images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images, to ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

**Data Protection**

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018, The Partnership Trust's Data Protection and Freedom of Information policy and TBMPT Privacy Notice which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy (see The Partnership Trust's Data Protection and Freedom of Information policy)
- It is registered as a Data Controller for the purposes of the General Data Protection Act (GDPR)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- take responsibility for the security of their username and password and do not allow other users to access systems using their logon details.

- immediately report any suspicion or evidence that there has been a breach of security.
- change their passwords at regular intervals.

When personal data is stored on any portable computer system, memory stick or any other removable media:
- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

**Disposal Of Data**
This is carried out in line with The Partnership Trust's Record Retention policy.

**Communications**
When using communication technologies the school considers the following as good practice:
- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school or on school systems e.g. by remote access.
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems.
- Pupils should be taught about Online Safety issues such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

**<u>Social Media - Protecting Professional Identity</u>**
The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:
- Ensuring that personal information is not published
- Providing training including: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

**School staff should ensure that:**
- No reference is made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions are not be attributed to the school or The Partnership Trust
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official school social media accounts are established there should be:
- A process for approval by Senior Leaders
- Clear processes for the administration and monitoring of these accounts involving at least two members of staff
- A code of behaviour for users of the accounts including:
  - -systems for reporting and dealing with abuse and misuse.
  - - Understanding how incidents may be dealt with under school disciplinary procedures.

**Personal Use:**

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites.

**Monitoring of Public Social Media:**

- As part of active social media engagement it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process
- The school's use of social media for professional purposes will be checked regularly by the Headteacher and Senior Leadership Team to ensure compliance with the school policies.

**Illegal Incidents**

If there is any suspicion that the website/s concerned may contain child abuse images or if there is any other suspected illegal activity, refer to the right hand side of the flowchart in Appendix 1 for responding to Online Safety incidents and report immediately to the police.

# Appendix 1 - E-Safety Reporting Flowchart