St Peter's C of E (Aided) Primary School
Little Green Lane, Farnham, Surrey, GU9 8TF
☎: 01252 714115   Fax: 01252 721215
✉: info@stpeters-farnham.surrey.sch.uk
www.stpeters-farnham.surrey.sch.uk

Our Vision Statement

At St Peter's we have high expectations where everyone flourishes, achieves and succeeds within a safe, inclusive Christian community. We promote gospel values of independence, respect and empathy. Through an exciting curriculum, children are inspired to find joy as lifelong learners and active world citizens.

ONLINE SAFETY

Person Responsible:	Computing Subject Leader
Governor Committee:	Children & Learning
Review Period:	Every 3 year or in light of any new regulations
Status:	Statutory
Date Adopted:	Autumn Term 2023
Next review:	Autumn Term 2026
Ratified by Governors:	4 October 2023

This policy is to be read in conjunction with the following policies: Anti- Bullying, Teaching and Learning, SMSC, Safeguarding, Acceptable Use of Technology.

Introduction

The use of computers and computer systems is an integral part of the National Curriculum and knowing how they work is a key life skill. In an increasingly digital world there now exists a wealth of software, tools and technologies that can be used to communicate, collaborate, express ideas and create digital content. It is vital that pupils are able to take advantage of these technologies safely, and this policy defines the measures that St Peter's C of E Primary school takes to try to ensure online safety for all school members.

We are a primary school, and such children's access to the internet while on school premises is quite controlled. Computers and tablets are used under the direct supervision of staff in lessons, and access to social media such as Facebook, Snapchat and Gaming is prohibited on the school network. Children are not allowed to bring their own devices to school; any mobile phones required for journeys by pupils are kept at the school office during the day. Whilst this means that the risks of serious incident whilst at school are relatively low, this extremely important policy focusses on the following aims:

- To minimise the risks of harm (inappropriate or illegal content, or bullying) while pupils and staff are using the school's infrastructure,
- To ensure that pupils, staff and governors are aware of the risks of using online technology, and are equipped to recognise and deal with them,
- For staff to recognise incidents relating to the online safety of pupils, whether they occur at school or elsewhere, and know how to address them.

Scope of the Policy

This policy applies to all members of the school (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school's ICT systems, both in and out of the school.
It is linked to the Anti-bullying Policy, the Behaviour Policy, the Safeguarding Policy, the Computing Policy and the Acceptable Use of Technology Policy.

Roles and Responsibilities

Headteacher

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The headteacher and deputy headteacher 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.
- The Headteacher is responsible for ensuring that the Online Safety Coordinator, Computer Technician and the SMT receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- all digital communications with pupils / parents / carers should be 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
- in lessons where internet use is pre-planned 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.

Network Manager

The Network Manager is 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 Local 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 (if it has one), is applied and updated on a regular basis.
- 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 the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
- that monitoring software (Securus) is implemented and updated regularly.

Pupils
Are responsible for using the school 's digital technology systems in accordance with the Pupil Acceptable Use Agreement.

Online Safety Coordinator

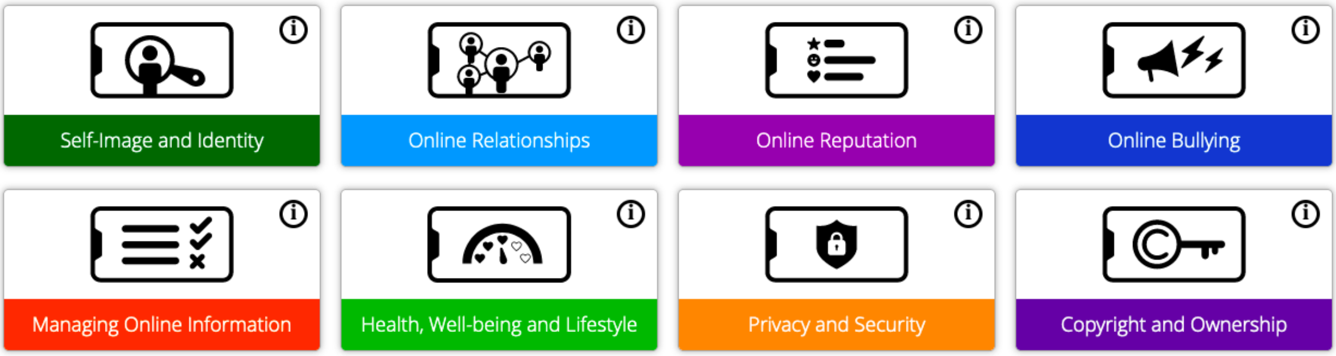
- To facilitate the training of staff in matters of online safety
- To investigate incidents on behalf of the headteacher
- To liaise with the headteacher to ensure that online safety incidents are recorded in the headteacher's log.

Policy Statements

Education of Pupils
Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore 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. At St Peter's this is accomplished by:

- A planned online safety curriculum is provided as part of the Computing Curriculum, based on the Project Evolve. All year groups are taught 8 different strands throughout the year. The strands are:



- Key online safety messages are reinforced in assemblies and pastoral activities
- Pupils are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned 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 young people visit and ensure that the children use search engines designed for children (e.g. swiggle.org.uk).

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 / regulation of the children's on-line 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: (select / delete as appropriate)

- Curriculum activities
- Letters, newsletters, web site
- Offering an evening briefing on online safety every other year.

Education and Training – Staff/Volunteers

- Formal online safety training will be made available to staff.
- All new staff should receive online safety briefing as part of their induction programme, to ensure that they fully understand the school 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 process.
- The Online Safety Coordinator will receive regular updates through attendance at external training events 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 Online Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authorities.
- Participation in school / academy training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – School infrastructure / equipment, filtering and monitoring

For the purposes of the Online Safety Policy, technical infrastructure and equipment includes the school servers (admin and curriculum), desktop computers in offices and classrooms, laptops and netbooks for use by pupils, the school's iPads, laptops provided to teachers, class cameras, printers and all components of the school's network.

- The School technical systems will be managed in ways that ensure that the school meets recommended technical requirements outlined in Local Authority guidance
- There will be regular reviews and of the safety and security of school technical systems, involving the Network Manager, Headteacher, and Data Manager.
- Servers, wireless systems and cabling are securely located, and physical access is restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every (insert period).
- The "master / administrator" passwords for the school ICT system, used by the Network Manager are available to the Head Teacher or other nominated senior leader and kept in a secure place.

- The school business manager (Fiona Hopkins) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users, using Smoothwall, which is provided as part of our broadband service. Illegal content (child sexual abuse images) is filtered by actively employing the Internet Watch Foundation CAIC list.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The Network Manager regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. Any inappropriate use is reported to the Headteacher.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Where Supply Teachers are employed on a daily basis, they use a specific 'Supply' account which provides them limited access to the school systems.
- Pupils do not access school systems from home, and do not take school equipment home.
- Staff and pupils are not allowed to downloading executable files or install programmes on school devices; this is the responsibility of the Network Manager. The only exception to this, are the Laptops allocated to teachers for their own use for schoolwork (use of these devices is detailed in the acceptable use policy, and the data protection policy).

Bring Your Own Device (BYOD)

Increasingly, staff and governors bring their own Smartphones and tablets into school. At this time, pupils are excluded from this, and must leave any such device at the office for the duration of the school day. Whilst they are on school premises these staff-owned devices may be connected to the school network, and as such are protected by the school network's filtering system. Staff are encouraged to use their own devices for personal matters only, and to use school equipment exclusively for school business. However, there are occasions where it is necessary to use a personal device (e.g. when on a school trip). This topic is covered in more detail the Acceptable Use of Technology Policy, and in the Data Protection Policy, and the following points relate online safety:

- Any staff-owned devices on school premises will be protected by a password, and be locked when not in use
- Pupils will not be allowed to use staff-owned devices under any circumstances
- Staff will not use their own devices to take photographs of pupils under any circumstances.

Personal Data and digital and video images

Access to personal data can be a contributor to online security, bullying and other illegal activity. The Data Protection Policy contains more detail on this topic, but the following statements refer particularly to online safety.

Staff must ensure that they

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- Access to school data from home is done by using Microsoft's Office 365 cloud-based products; Sharepoint and Onedrive.
- 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.

- Obtain written permission from parents or carers 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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases 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 these must not be shared, distributed or published outside the school premises without the permission of the headteacher. Those images should only be taken on school equipment, the personal equipment of staff must not be used for such purposes.
- Care should be taken when taking digital / video images 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 photograph
- Pupil's work can only be published with the permission of the pupil and parents or carers.
- No reference should be 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 should not be attributed to the school /academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

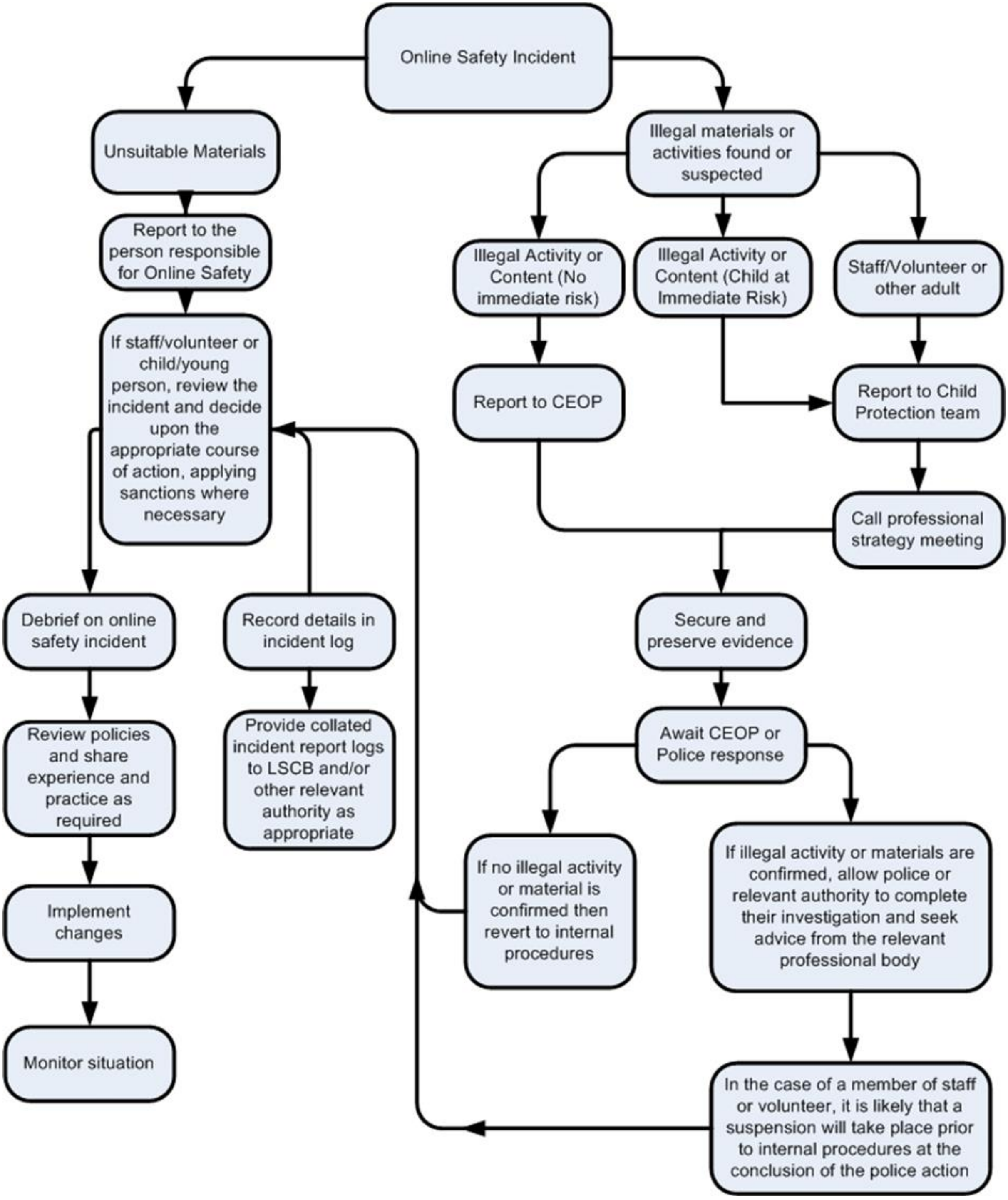
Responding incidents of misuse

Illegal Incidents
If there is any suspicion that the web site(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 for responding to online safety incidents and report immediately to the police. Whilst this scenario is extremely unlikely to occur in school, given the constraints in place, it is included in the policy for completeness.

Other Incidents
The following are more likely online safety incidents which could occur at St Peter's or to pupils at St Peters.

- Viewing inappropriate material
- Predation and grooming
- Requests for personal information
- Viewing incitement sites
- Bullying and threats
- Misuse of computer systems – inappropriate searching
- Publishing of personal information.

Online Safety Incident


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

If the incident happens on school premises, use the right-hand side of the diagram above, then the following procedure must be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority
  - Police involvement and/or action
- If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.