



St. Peter's C.E.
Primary School
and Nursery



"...The fruit of the spirit is...

love, peace, kindness, gentleness, joy, patience, goodness, faithfulness, self-control"

Galatians 5:22-23

ST. PETER'S CE PRIMARY SCHOOL & NURSERY EDMOND

Online Safety Policy

This policy applies to all members of our school community (including staff, pupils, volunteers, parents and carers and visitors) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Date created: September 2023

Next review date: September 2024

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of St. Peter's CE Primary School & Nursery to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of our school community (including staff, children, governors, volunteers, parents and carers and visitors) who have access to and are users of school digital systems, both in and out of school. It also applies to the use of personal digital technology on the school site (where allowed).

St. Peter's CE Primary School & Nursery will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Policy development, monitoring and review

This Online Safety Policy has been developed by the Senior Leadership Team made up of:

- Headteacher
- Designated Safeguarding Lead (DSL) and Deputies
- Online Safety Lead (OSL)
- Governors

Schedule for development, monitoring and review

This Online Safety Policy was approved by the school governing body on:	12 October 2023
The implementation of this Online Safety Policy will be monitored by:	Senior leadership team
Monitoring will take place at regular intervals:	Half-termly
The governing body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2024
Should serious online safety incidents take place, the following external persons/agencies should be informed:	LA safeguarding officer Police

Process for monitoring the impact of the Online Safety Policy

School will monitor the impact of this policy using:

- logs of reported incidents
- Filtering and monitoring logs
- internal monitoring data for network activity
- surveys/questionnaires of:
 - children
 - parents and carers
 - staff

Aims

This Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours

- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how our school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels
- is published on the school website

Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within our school.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, and as the Designated Safeguarding Lead, holds day-to-day responsibility for online safety as defined in Keeping Children Safe in Education.
- The headteacher and DSLs are 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 Designated Safeguarding Leads, Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher 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.
- The headteacher will receive regular monitoring reports from the Designated Safeguarding Leads / Online Safety Lead.
- The headteacher will work with the responsible Governor, the Designated Safeguarding Leads (DSLs) and IT service providers in all aspects of filtering and monitoring.

Governors

Governors are responsible for the approval of this Online Safety Policy and for reviewing the effectiveness of the policy and will do so by asking the questions posed in the UKCIS document [“Online Safety in Schools and Colleges – questions from the Governing Body”](#).

This review will be carried out by the governing body whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead

- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training) is taking place as intended
- ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually (this review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) in line with the [DfE Filtering and Monitoring Standards](#)
- reporting to the governing body
- receiving basic cyber-security training to enable the governors to check that the school meets the [DfE Cyber-Security Standards](#)

The governing body will also support our school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safety Lead (DSL)

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role
- receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensure that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/committee meetings
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded
- provide (or identify sources of) training and advice for staff/governors/parents/carers/ learners
- liaise with local authority technical staff, pastoral staff and support staff (as relevant)
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Lead

The Online Safety Lead will:

- work closely with the Designated Safeguarding Lead (DSL)
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing this policy
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
 - content

- contact
- conduct
- commerce

Curriculum Leads

Curriculum Leads will work with the DSL and OSL to develop a planned and coordinated online safety education programme.

This will be provided through:

- a discrete programme
- PSHE and RSHE programmes
- a mapped cross-curricular programme
- assemblies and pastoral programmes
- relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#).

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of our current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement
- they immediately report any suspected misuse or problem to the DSL for investigation/action, in line with our school safeguarding procedures
- all digital communications with learners and 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
- children understand and follow this Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners 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
- there is a zero-tolerance approach to incidents of online bullying, sexual harassment, discrimination, hatred etc.
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media

IT Provider

Our IT Provider (Telford & Wrekin) is responsible for ensuring that:

- they are aware of and follow our school Online Safety Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack

- the school meets (as a minimum) the required online safety technical requirements as identified by the [DfE Meeting Digital and Technology Standards in Schools & Colleges](#) and guidance from the local authority
- there is clear, safe, and managed control of user access to networks and devices
- 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
- the use of technology in our school is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring systems are implemented and regularly updated

Children

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- 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 and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use online services and devices in an appropriate way.

Our school will take every opportunity to help parents and carers understand these issues through:

- publishing our school Online Safety Policy on the school website
- providing them with a copy of our pupils' acceptable use agreement
- seeking their permissions concerning digital images, cloud services etc
- holding parents'/carers' evenings, distributing newsletters, informing via our school website/Twitter feed and sharing information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support school staff in reinforcing the online safety messages provided to children in school.

Acceptable use

St. Peter's CE Primary School has defined what it regards as acceptable/unacceptable use and this is shown in our acceptable use agreements (attached).

Acceptable use agreements

Our Online Safety Policy and acceptable use agreements define acceptable use at our school. The acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook

- Computing lessons
- communication with parents/carers
- school website

Please see also our Mobile & Smart Technology Policy.

Reporting and responding

Our school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside school (with impact on the school) which will need intervention. School will ensure:

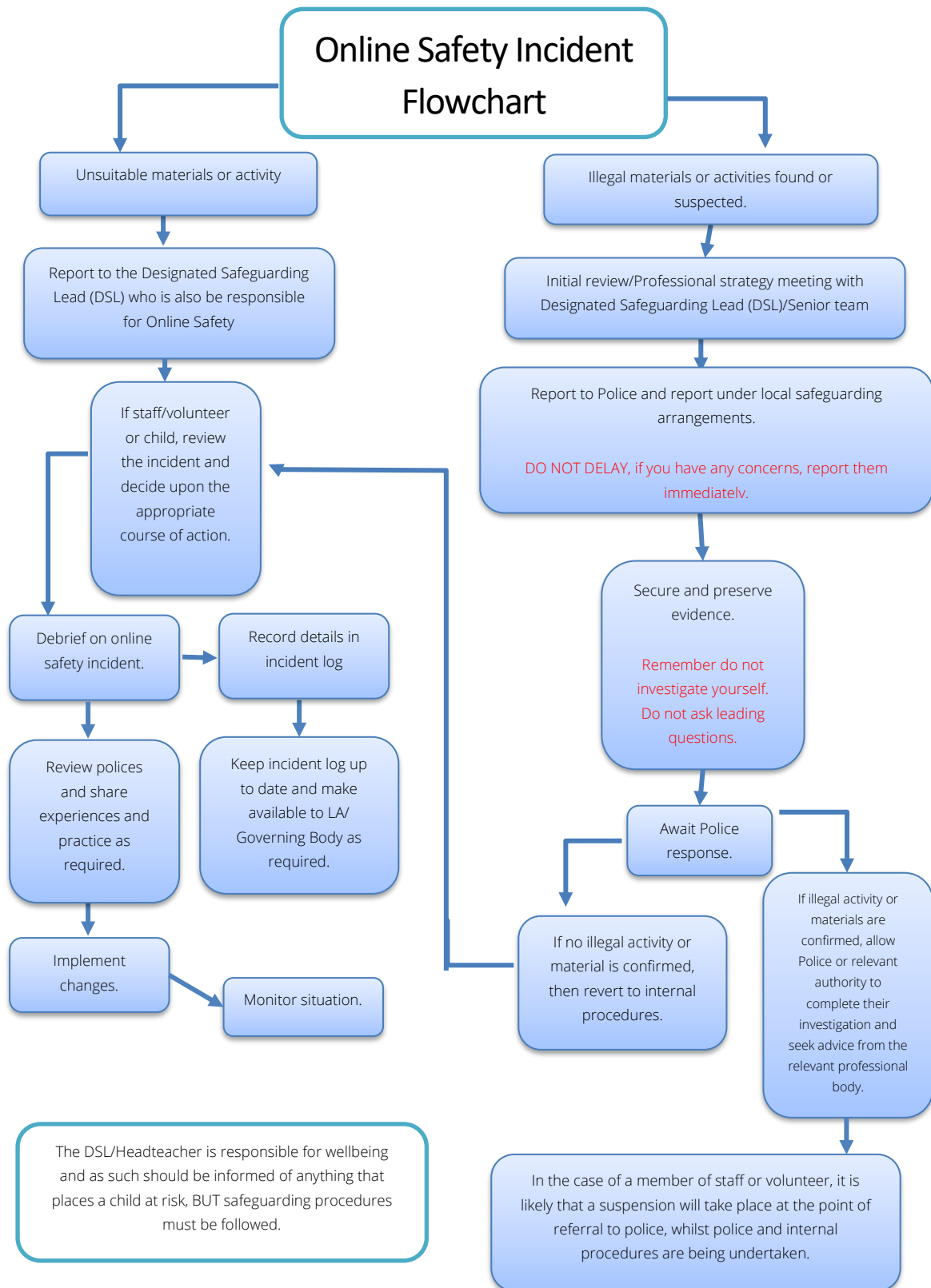
- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of our school community are aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident will be escalated through our agreed school safeguarding procedures, this may include
 - Non-consensual images
 - Self-generated images
 - Terrorism/extremism
 - Hate crime/ Abuse
 - Fraud and extortion
 - Harassment/stalking
 - Child Sexual Abuse Material
 - Child Sexual Exploitation Grooming
 - Extreme Pornography
 - Sale of illegal materials/substances
 - Cyber or hacking [offences under the Computer Misuse Act](#)
 - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- where there is no suspected illegal activity, devices may be checked using the following procedures:
 - at least two senior members of staff will be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
 - the procedure will be conducted using a designated device that will not be used by pupils and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). The same device will be used for the duration of the procedure.
 - the relevant staff will have appropriate internet access to conduct the procedure, but the sites and content visited will be closely monitored and recorded (to provide further protection).
 - the URL of any site containing the alleged misuse will be recorded and the nature of the content causing concern described. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed and signed.

- once this has been completed and fully investigated staff will judge whether this concern has substance or not. If it does, then appropriate action will be taken and may include the following:
 - internal response or discipline procedures
 - involvement by local authority
 - police involvement and/or action

It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively. We will ensure that:

- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents are logged securely
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; [Professionals Online Safety Helpline](#); [Reporting Harmful Content](#); [CEOP](#).
- those involved in the incident are provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
 - staff, through regular briefings
 - children, through assemblies/lessons
 - parents/carers, through newsletters/website
 - governors, through regular safeguarding updates
 - local authority/Local Safeguarding Partnership, as relevant

School will make the flowchart overleaf available to staff to support the decision-making process for dealing with online safety incidents.



School actions

It is more likely that school will need to deal with incidents that involve inappropriate rather than illegal misuse. Any incidents will be dealt with as soon as possible in a proportionate manner, and members of the school community will be made aware that incidents have been dealt with (as relevant). It is intended that incidents of misuse will be dealt with through our normal Behaviour/Disciplinary procedures (see Behaviour & Relationships policy and Disciplinary Policy & Rules).

Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating children to take a responsible approach. The education of pupils in online safety is therefore an essential part of our online safety provision. Children need our help and support to recognise and avoid online safety risks and develop their resilience.

Online safety is a focus in all areas of the curriculum and staff regularly reinforce online safety messages across the curriculum. Our online safety curriculum is broad, relevant and provides progression, and is taught in through the [Education for a Connected Work Framework by UKCIS/DCMS](#) and the [SWGfL Project Evolve](#). Lessons are matched to need, are age-related and build on prior learning. They are context-relevant with agreed objectives leading to clear and evidenced outcomes. Our teaching also incorporates relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#). Our online safety curriculum is accessible to learners of different ages and abilities such as those with additional learning needs or those with English as an additional language. Children 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. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.

Staff are expected to act as good role models in their use of digital technologies, particularly when using the internet and/or mobile devices. In lessons where internet use is pre-planned, we aim to ensure that children are guided to sites checked as suitable for their use in advance, however processes are in place for dealing with any unsuitable material that is found in internet searches. On the rare occasions that pupils are allowed to freely search the internet, staff are vigilant in supervising them and monitoring the content of the websites they visit.

Staff/volunteers

All staff receive online safety training and understand their responsibilities, as outlined in this policy. Training is offered as follows:

- a planned programme of formal online safety and data protection training is made available to all staff. This is regularly updated and reinforced. An audit of the online safety training needs of all staff is carried out regularly.
- the training is an integral part of our school's annual safeguarding and data protection training for all staff
- all new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements
- the Online Safety Lead and Designated Safeguarding Lead 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 Designated Safeguarding Lead/Online Safety Lead will provide advice/guidance/training to individuals as required.

Governors

Governors take part in online safety training/awareness sessions, which are offered in several ways such as:

- attendance at training provided by the local authority or other relevant organisation
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training is made available to the governor with responsibility for Online Safety. This includes:

- Cyber-security training
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

Families

Our school seeks to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- their children, who are encouraged to pass on to parents the online safety messages they have learned in lessons
- letters, newsletters, website
- high profile events / campaigns e.g. [Safer Internet Day](#)

Technology

Our school, in partnership with Telford & Wrekin IDT, is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. We ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering & Monitoring

Our school filtering and monitoring provision is agreed by senior leaders, governors and our IT Service Provider (Telford & Wrekin IDT) and is regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours. Our DSL has lead responsibility for safeguarding and online safety and our IT service provider has technical responsibility. Our filtering and monitoring provision is reviewed annually by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of our IT Service Provider. Checks on the filtering and monitoring system are carried out by our IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or new technology is introduced.

Filtering

Through our IT service provider, Telford & Wrekin IDT, we meet the filtering and monitoring requirements as follows:

- Internet Filtering Provision: Smoothwall – This blocks access to any of the material listed on the SWGfL testing site (including child sexual abuse content, terrorism content, adult content and offensive language).
- If necessary, school will seek advice from, and report issues to, the SWGfL [Report Harmful Content](#) site.

Monitoring

Our school has monitoring systems in place to protect the school, systems and users:

- We monitor all network use across all our devices and services using Senso classroom monitoring software. Senso's filter cloud not only benefits from extensive category-based libraries to block inappropriate websites, but also uses Artificial Intelligence to check the content of every website a student attempts to visit and will proactively include any inappropriate websites within the filtering libraries.
- Real-time monitoring reports/concerns are automatically sent to the DSL and urgently picked up, acted on and outcomes recorded. All users are aware that our network (and devices) are monitored.
- We have effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with our safeguarding policy and practice.

Technical Security

- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users are recorded by our IT service provider and are reviewed regularly by the DSL.
- password policy and procedures are implemented
- the security of usernames and passwords does not allow users to access the systems using log on details that are not their own.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all school networks and systems are protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in a secure place.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- servers, wireless systems and cabling are securely located and physical access restricted.

- appropriate security measures are in place to protect our server, firewall, router, wireless systems and devices from accidental or malicious attempts which might threaten the security of school systems and data. These are tested regularly. Our school infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines - Microsoft provide resilience within their Office 365 environment and T&W provide back-ups on everything else.
- T&W IDT are responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the DSL.
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them.
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network.
- staff members are not permitted to install software on school-owned devices without the consent of the DSL.
- removable media is not permitted unless approved by the DSL.
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place.
- guest users are provided with appropriate access to school WiFi based on an identified risk profile.

Mobile technologies

Our Mobile & Smart Technology Policy and school acceptable use agreements for staff and pupils outline the expectations around the use of mobile technologies.

Social media

Our school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to children through:

- ensuring that personal information is not published.
- asking parents/carers to give/refuse permission for children's photographs to be used on the school website/Twitter account.
- providing education/training including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for children and parents/carers.

School staff should ensure that:

- no reference is made in social media to learners, 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 attributed to the school.

- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, 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.

Monitoring of public social media

- as part of active social media engagement, we may pro-actively monitor the Internet for public postings about the school.
- when parents/carers express concerns about our school on social media we will urge them to make direct contact with us, in private, to resolve the matter. Where this cannot be resolved, parents/carers will be informed of the school complaints procedure.

Digital and video images

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

- when using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers will be made aware of those children whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes unless in exceptional circumstances, when permission from the headteacher must be sought in advance. Any images taken on personal devices will be deleted immediately after use.
- 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 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 children in the digital/video images.
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy.

- images will be securely stored in line with the school retention policy.

Online Publishing

Our school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Twitter feed

The school website is managed/hosted by T&W IDT. We ensure that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where pupil work, images or videos are published, their identities are protected, and full names are not published.

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

The school:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so.
- has paid the appropriate fee to the Information Commissioner's Office (ICO).
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it.
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed .
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule' supports this.
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice.
- has procedures in place to deal with the individual rights of the data subject.
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier.

- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors.
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data.
- [reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected.
- device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software.
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

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.
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school.
- only use encrypted data storage for personal data.
- will not transfer any school personal data to personal devices.
- 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, a secure email account (where appropriate), and secure password protected devices.

Outcomes



The impact of our Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff and pupils; and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g. online safety education, awareness, and training.
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors.

- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising.
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate.
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Acceptable Use Agreement (AUA) for KS1 pupils

To stay **SAFE online and on my devices**:

1. I only **USE** devices or apps, sites or games if I am allowed to
2. I **ASK** for help if I'm stuck or not sure; I **TELL** a trusted adult if I'm upset, worried, scared or confused
3. I look out for my **FRIENDS** and tell someone if they need help
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult
5. I **KNOW** that online people aren't always who they say they are and things I read are not always **TRUE**
6. Anything I do online can be shared and might stay online **FOREVER**
7. I don't keep **SECRETS**  unless they are a present or nice surprise
8. I don't have to do **DARES OR CHALLENGES** , even if someone tells me I must.
9. I don't change **CLOTHES** or get undressed in front of a camera
10. I always check before **SHARING** my personal information or other people's stories and photos
11. I am **KIND** and polite to everyone

✓

My trusted adults are:

_____ at school

_____ at home

Acceptable Use Agreement (AUA) for KS2 pupils

These statements can keep me and others safe & happy at school and home:

1. ***I learn online*** – I use school internet, devices and logins for school and homework, to learn and have fun. School can see what I am doing to keep me safe, even when at home.
2. ***I behave the same way on devices as face to face in the classroom, and so do my teachers*** – If I get asked to do anything that I would find strange in school, I will tell another teacher.
3. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. ***I am creative online*** – I don't just use apps, sites and games to look at things other people made or posted; I also get creative to learn or make things.
5. ***I am a good friend online*** – I won't share or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. ***I am not a bully*** – I know just calling something fun or banter doesn't stop it maybe hurting someone else. I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
7. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
8. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
9. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
10. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult.
11. ***If I make a mistake I don't try to hide it but ask for help.***
12. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
13. ***I know online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
14. ***I never pretend to be someone else online*** – it can be upsetting or even dangerous.
15. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
16. ***I don't go live (videos anyone can see) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

17. ***I don't take photos or videos or people without them knowing or agreeing to it*** – and I never film fights or people when they are upset or angry.
18. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
19. ***I say no online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
20. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
21. ***I follow age rules*** – 13+ games, apps and films aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.
22. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
23. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even if I delete it).
24. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
25. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
26. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
27. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, and I know which sites to trust, and how to double check information I come across. If I am not sure I ask a trusted adult.



I have read and understood this agreement. If I have any questions, I will speak to a

trusted adult: At school that might be _____

Outside school, my trusted adults are _____

I know I can also get in touch with [Childline](#)

Acceptable Use Agreement (AUA) for Staff & Governors

Background

We ask everyone involved in the life of St. Peter's Primary School & Nursery to sign an Acceptable Use Agreement (AUA), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUA is reviewed annually, and staff, governors and volunteers are asked to sign it when starting at the school and whenever changes are made. All staff (including support staff), governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in our full Online Safety policy.

If you have any questions about this AUA or our approach to online safety, please speak to Claire Medhurst, Headteacher.

What am I agreeing to?

1. I have read and understood St. Peter's Primary School's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay as outlined in the Online Safety policy.
2. I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best practice in this area. I have noted the section in our online safety policy which describes trends over the past year at a national level and in this school.
3. I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (whether by a child or an adult) and make them aware of new trends and patterns that I might identify.
4. I will follow the guidance in the Safeguarding and Online Safety policies for reporting incidents (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media).
5. I understand the principle of safeguarding as a jigsaw where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom.
6. I will take a zero-tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including bullying and sexual violence & harassment – I know that 'it could happen here.'
7. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.

I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting subject leaders and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).

I will follow best-practice pedagogy for online-safety education, avoiding scaring and other unhelpful prevention methods.

I will prepare and check all online sources and classroom resources before using for accuracy and appropriateness. I will flag any concerns about overblocking to the DSL.

I will carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and data protection.

During any periods of remote learning, I will not behave any differently towards students compared to when I am in school and will follow the same safeguarding principles as outlined in the main child protection and safeguarding policy when it comes to behaviour, ways to contact and the relevant systems and behaviours.

8. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.

9. I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE 2023, now led by the DSL. If I discover pupils may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay. Equally, if I feel that we are overblocking, I shall notify the school to inform regular checks and annual review of these systems.

10. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology both in and outside school, including on social media, e.g. by not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

11. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.

12. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in our full Online Safety policy. If I am ever not sure, I will ask first.

13. I agree to adhere to all provisions of the school's Cybersecurity and Data Protection Policies at all times, whether or not I am on site or using a school device, platform or network.

14. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after any devices loaned to me.

15. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.
16. I understand and support the commitments made by pupils/students and fellow staff, governors and volunteers in their Acceptable Use Agreements and will report any infringements in line with school procedures.
17. I understand that breach of this AUA and/or of the school's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature:

Name:

Role:

Date:
