East Bridgford St Peter's C. of E. Academy

Online Safety Policy

(to protect users from risks associated with being online)

Incorporating Digital Systems & Acceptable Use

(rules & guidelines for the appropriate use of digital resources)

"Together in Achievement"

Date Governor Approved:	March 2025
Review Date:	March 2026

Contents

1. Scope

This Online Safety Policy outlines St Peter's C of E Academy's commitment to safeguarding all members of our school community online, in line with statutory guidelines (see Appendix 1) and best practices. It:

- Sets expectations for the safe and responsible use of digital technologies in learning, administration, and communication.
- Defines roles and responsibilities for the implementation and oversight of the policy.
- Is regularly reviewed in collaboration with stakeholders, considering online safety incidents, evolving technologies, and emerging trends in digital behaviour.
- Provides guidance for staff on responsible digital technology use, ensuring they protect themselves, the school, and help safeguard learners in the digital world.
- Outlines how the school prepares learners to use online technologies safely and responsibly.
- Establishes clear procedures for identifying, reporting, responding to, and recording the misuse of digital technologies and online safety incidents, including available external support.
- Is supplemented by acceptable use agreements for different members of the school community.
- Is provided to all staff during induction and is published on the school website.
- Applies to all members of the school community (staff, learners, volunteers, parents, carers, visitors, and community users) who access or use school digital systems, both within and outside the school. It also governs the use of personal digital technology on school premises (where permitted).

2. Monitoring arrangements

The school will monitor the impact of this policy through:

- Logs of reported incidents (see Appendix 2)
- Monitoring of internet activity
- Internal network activity data
- Feedback from pupils, staff, and parents/carers

This policy will be reviewed annually by the Headteacher and shared with the governing board at each review. The review (such as the one available here) will be supported by an annual risk assessment that evaluates and reflects the evolving online risks faced by pupils. Given the rapid changes in technology and the associated risks, regular reassessment is crucial.

2.1 Our Commitment to Online Safety

St Peter's C of E Academy is committed to:

- Implementing robust processes to safeguard pupils, staff, volunteers, and governors online.
- Identifying and supporting pupils who may be at greater risk of online harm.
- Delivering an effective and proactive approach to online safety, empowering the entire school community to use technology responsibly, including mobile and smart devices (referred to as 'mobile phones').
- Establishing clear procedures to identify, intervene, and escalate online safety incidents as necessary.

2.2 The Four Key Categories of Online Risk

Our approach to online safety is based on addressing the following four categories of risk:

- Content – Exposure to illegal, inappropriate, or harmful material, such as:
  - Pornography
  - Fake news
  - Racism
  - Misogyny
  - Self-harm and suicide content
  - Antisemitism
  - Radicalisation and extremism
- Contact – Harmful online interactions, including:
  - Peer pressure
  - Commercial advertising
  - Adults posing as children or young adults to groom or exploit individuals for sexual, criminal, financial, or other purposes
- Conduct – Personal online behaviour that may cause or increase the risk of harm, such as:
  - Creating, sharing, or receiving explicit images (including consensual and non-consensual sharing of nudes, semi-nudes, and pornography)
  - Online bullying
  - Sharing other explicit or harmful content
- Commerce – Financial and commercial risks, including:
  - Online gambling
  - Inappropriate advertising
  - Phishing scams
  - Financial fraud

3. Roles and responsibilities

3.1 The Governing Board

The governing body is responsible for approving the Online Safety Policy and reviewing its effectiveness.

The designated governor for Online Safety, Mrs. Johnson, will:

- Hold regular meetings with the Headteacher, Mr. Tomlinson
- Receive and review reports of online safety incidents
- Monitor the implementation of the policy and its effectiveness

Additionally, the governing body will support the school in engaging parents, carers, and the wider community in online safety initiatives.

3.2 Headteacher's Role in Online Safety

Mr. Tomlinson (**Headteacher and DSL**) and Mrs. Gibbens (**Deputy Head Teacher and DSL**) hold **lead responsibility** for online safety in school. Key responsibilities include:

- Ensuring that **all staff understand** this policy and consistently implement it across the school.
- Working with the **governing board** to review this policy annually, ensuring that procedures and implementation are regularly updated, and providing regular reports on online safety.
- Collaborating with **Infotechdirect Ltd (our technical provider)** to ensure appropriate **filtering and monitoring systems** are in place.
- Working with **Infotechdirect Ltd** and other support staff to address **online safety issues and incidents** as needed.
- Managing **all online safety incidents** in line with the school's **Child Protection Policy**.
- Ensuring that **online safety incidents** are **logged and handled appropriately** (**see Appendix 2**).
- Ensuring that **incidents of cyberbullying** are **logged and addressed** in accordance with the **School Behaviour Policy**.
- Promoting **awareness and commitment** to online safety education **within the school and wider community**.
- Liaising with **curriculum leaders** to ensure that the **online safety curriculum** is **planned, progressive, embedded, and evaluated**.
- Liaising with the **local authority, other agencies, and MAT** as required.
- Conducting **annual risk assessments** to evaluate and address the **online risks faced by pupils**.
- Providing **regular safeguarding and child protection updates**, including online safety training, to all staff **at least annually** to ensure they have the necessary skills and knowledge to safeguard effectively.

This list is **not exhaustive** and may be updated as needed.

3.3 Responsibilities of External Digital Systems Providers

The school is responsible for ensuring that external contractors comply with all online safety measures required to meet the school's obligations. The provider must follow and implement the Online Safety Policy and procedures.

At St Peter's C of E Academy, our network and digital services are provided by Infotechdirect Ltd, who are responsible for:

- Implementing appropriate security protection measures, including filtering and monitoring systems* on school devices and networks. These measures are reviewed and updated at least annually to ensure their effectiveness in safeguarding pupils from harmful or inappropriate online content and contact, including terrorist and extremist material.
- Infotechdirect Ltd monitor alerts and where appropriate notifies Mr. Tomlinson.
- Examples of filtering categories which are blocked include drug abuse, hacking, illegal or unethical sites, discrimination, explicit violence, extremist groups, child sexual abuse, terrorism, abortion, other adult materials, gambling, nudity and risque, pornography, dating,

weapons sales, drugs, alcohol, tobacco, lingerie and swimwear, sports huntine and war games.
- Ensuring that the school's digital systems are secure and protected against viruses and malware, with regular updates to maintain security.
- Continuously monitoring and mitigating digital system vulnerabilities.
- Blocking access to potentially dangerous websites and, where possible, preventing the download of harmful files.
- Logging online safety incidents (see Appendix 2) and ensuring they are managed appropriately in line with this policy.
- Ensuring that cyberbullying incidents are addressed appropriately in accordance with Aspire's Child Protection and Behaviour Policies.

This list is not exhaustive and may be updated as necessary.

3.4 Staff Responsibilities for Online Safety

All staff are responsible for ensuring that:

- They stay informed about current online safety matters, trends, and the school's Online Safety Policy and practices.
- They have read, understood, and signed the Staff Acceptable Use Agreement (Appendix 6).
- They immediately report any suspected misuse or online safety concerns to Mr. Tomlinson or Mrs. Gibbens for investigation and action, in line with school safeguarding procedures.
- All digital communications with learners and parents/carers are conducted professionally and only via official school systems.
- Online safety principles are embedded into all aspects of the curriculum and other school activities.
- Learners understand and follow the Online Safety Policy and Acceptable Use Agreements, develop strong research skills, and adhere to plagiarism and copyright regulations.
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where permitted) and enforce current school policies regarding these devices.
- In lessons where internet use is pre-planned, learners are guided to suitable websites, and processes are in place to handle any unsuitable material encountered.
- They follow correct procedures when requesting bypasses to filtering and monitoring systems for educational purposes, ensuring Infotechdirect Ltd is alerted in advance.
- When conducting live-streaming or video-conferencing lessons, they adhere to national safeguarding guidance and local safeguarding policies and follow the Aspire MAT Virtual Meeting Policy.
- They maintain a zero-tolerance approach to cyberbullying, sexual harassment, discrimination, and online abuse, recognising that child-on-child abuse, including sexual violence and harassment, can occur online. Any incidents must be dealt with in line with school policy.
- They model safe, responsible, and professional online behaviour both in and outside of school, including when using social media.
- They are aware of the risks associated with AI tools, recognising that these technologies are still developing. If new AI tools are used within the school, staff must conduct a risk assessment before implementation.

This list is not exhaustive and may be updated as necessary.

3.5 Learners

3.5.1 Learner responsibilities

- **Are responsible for using the school's digital technology systems** in accordance with the Learner Acceptable Use Agreement (Appendix 4) and the Online Safety Policy. This includes personal devices, as outlined in Appendix 3. Teachers should refer to and remind students of these standards during IT lessons.

- **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 practices** when using digital technologies outside of school and recognise that the school's Online Safety Policy applies to their actions outside of school if they are related to school membership.

3.5.2 Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum in line with National Curriculum computing programmes of study and guidance on relationships education, relationships and sex education (RSE) and health education.

All schools are required to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

Pupils will receive online safety education as part of the curriculum, covering key aspects at different stages:

Key Stage 1 (KS1)

Pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact online.

Key Stage 2 (KS2)

Pupils will be taught to:

- Use technology safely, respectfully, and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respecting others online, even when anonymous.
- The rules and principles for staying safe online, how to recognise risks, harmful content, and contact, and how to report concerns.
- How to critically assess online friendships and sources of information, including understanding the risks associated with interacting with people they have never met.
- How information and data are shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others, including in digital contexts.
- How to respond safely and appropriately to unfamiliar adults they may encounter online or in person.
- How to critically evaluate AI-generated content, including identifying fake news and misinformation.

The safe use of social media and the internet will also be integrated into other subjects where relevant. Teaching about safeguarding, including online safety, will be adapted where necessary to support vulnerable children, victims of abuse, and pupils with SEND.

To help prevent **cyberbullying**, we will ensure that pupils:

- Understand what cyberbullying is and how to respond if they experience or witness it.
- Know how and where to report incidents and feel encouraged to do so, whether they are the victim or a witness.
- Engage in discussions about cyberbullying, including its causes, different forms, and consequences.

A structured and coordinated online safety education programme is provided through:

- **Purple Mash** computing scheme of work.
- **Classroom sessions** taught by **Infotechdirect Ltd**.
- **1Decision** PSHE & Safeguarding programme.
- **Assemblies and external speakers**, such as the **Year 6 social media police talk**.
- **Relevant national initiatives and events**, e.g. **Safer Internet Day** and **Anti-Bullying Week**.

3.5.3 IT facilities

Currently, the digital facilities available to pupils are:

- **30 laptops** stored in the library, available to pupils only under staff supervision.
- **8 children's iPads** stored in a lockable cupboard, available to pupils only under staff supervision

3.6 Parents/carers

Parents and carers play a crucial role in ensuring that their children understand the importance of using online services and digital devices responsibly.

Parents and carers are encouraged to support the school by:

- Reinforcing the online safety messages provided to learners in school.
- Understanding and supporting the school's guidelines on their children’s use of personal devices in school.

At **St Peter’s C of E Academy**, we actively work to help parents and carers understand these issues. This is communicated through:

- Publishing the **Online Safety Policy** on the school website.
- Providing parents and carers with a copy of the **Acceptable Use Agreement**.
- Sharing information about the **appropriate use of social media** concerning posts related to the school.
- Seeking parental permissions regarding **digital images** of their children.
- Offering **parent and carer information sessions**, including:
  - eSafety information in newsletters.
  - Up-to-date guidance via the school website.
  - Sharing national and local online safety campaigns and resources.

Parents and carers can find further guidance on keeping children safe online from the following organisations:

- UK Safer Internet Centre – *What are the issues?*
- Childnet – *Hot topics*
- Childnet – *Parent resource sheet*

If parents or carers have any **queries or concerns** regarding online safety, they should first contact **Mr. Tomlinson**. Concerns or queries about this policy can be raised with any member of staff or **Mr. Tomlinson**.

3.7 Visitors and members of the community

Visitors and community members who use the school's digital systems or internet will be made aware of this policy when relevant. They are expected to read and follow it, and, where appropriate, agree to the **Acceptable Use Terms** (see Appendix 6).

4. Acceptable use

All **pupils, parents/carers, staff, volunteers, and governors** are expected to adhere to a **Code of Conduct** regarding the acceptable use of the school's digital systems and the internet (**see Appendices 4 to 6**). **Visitors** will also be expected to read and agree to the school's acceptable use terms, where relevant.

The school's internet must be used **solely for educational purposes** or for fulfilling the duties of an individual's role.

To ensure compliance, we **monitor the websites** visited by pupils, staff, volunteers, governors, and, where applicable, visitors. Access to certain websites is restricted through filtering systems where appropriate.

The **Online Safety Policy** and **Acceptable Use Agreement** define acceptable digital use at **St Peter's C of E Academy**. These agreements are communicated and reinforced through:

- The **staff handbook**
- The **Computing, RSE and PHSE curriculum**
- **Communication with parents and carers**
- The **school website**
- Relevant **policies and standards**, including (but not limited to):
    - **Child Protection Policy**
    - **Child-on-Child Abuse Policy**
    - **Anti-Bullying Standard**
    - **Standard for Mobile Phones and Smartwatches**
    - **Staff Communication Standard**
    - **Visitors to School Standard**

5. Online Safety Incident Management

At **St Peter's C of E Academy**, we take all reasonable precautions to ensure online safety for all school users. However, we recognise that incidents may occur both inside and outside of school that could impact the school community and require intervention.

We will ensure:

- Clear **reporting routes** are in place, understood, and followed by all members of the school community. These routes align with safeguarding procedures, including the **whistleblowing, complaints, and managing allegations policies**.

- All members of the school community understand the importance of **reporting online safety issues and incidents**.
- Reports are addressed **as soon as practically possible** upon receipt.
- The **DSL(s)** and other responsible staff have the **appropriate skills and training** to handle online safety risks.
- If an incident involves **suspected illegal activity** or potential serious harm, it is escalated in line with **safeguarding procedures**.
- Any concerns about **staff misuse** will be reported to the **Headteacher**. If the concern involves the **Headteacher**, it will be referred to the **Chair of Governors, LADO, or the CEO of the Academy Trust**.

Investigating Suspected Misuse (Where No Illegal Activity Is Suspected)

If an incident does not involve suspected illegal activity, devices may be checked using the following procedures:

- **At least one senior staff member** must be involved to protect individuals in case of subsequent accusations.
- The investigation must be conducted using a **designated device**, which should:
    - Not be used by learners.
    - Be available for police inspection if illegal activity is later suspected.
    - Be used exclusively for the duration of the investigation.
- Staff conducting the investigation must have **appropriate internet access**, with sites and content **monitored and recorded** to ensure accountability.
- The **URL** of any concerning site must be recorded, along with a **description of the content**. Screenshots may also be taken, printed, signed, and attached to the report.
- Following the investigation, the **reviewing group** will determine whether further action is necessary. This may include:
    - **Internal response or disciplinary action**
    - **Involvement of the local authority or Multi-Academy Trust (MAT)**
    - **Referral to the police**

Handling Incidents Involving Indecent Images of a Child

If a staff member suspects that a device contains an **indecent image of a child (e.g., nude or semi-nude images)**, they must:

- **Not view the image.**
- **Confiscate the device immediately.**
- **Report the incident to the DSL (or equivalent).**
- The **DSL** will decide on the next steps in line with:
    - **DfE guidance on searching, screening, and confiscation**
    - **UKCIS guidance on sharing nudes and semi-nudes**

Supporting Those Involved in Online Safety Incidents

- Individuals reporting incidents should have **confidence that concerns will be taken seriously and handled effectively**.
- **Support strategies** (e.g., peer support) will be in place for those affected.
- **All incidents will be logged using CPOMs**.
- Staff will be aware of **external sources of support**, such as:
    - **Local authorities**
    - **Police**
    - **Professionals Online Safety Helpline**
    - **Reporting Harmful Content**
    - **CEOP (Child Exploitation and Online Protection Command)**

Communicating Outcomes and Learning from Incidents

Following an investigation, those involved will be **provided with feedback** on the outcome and any follow-up actions, as appropriate.
Where relevant (and anonymously), **learning from incidents** will be shared with:

- **The Online Safety Lead and DSLs** – for policy and curriculum updates.
- **Staff** – through regular briefings.
- **Learners** – through assemblies and lessons.
- **Parents/carers** – via newsletters, school social media, and the website.
- **Governors** – through safeguarding updates.
- **Local authorities or external agencies** – in line with best practices, such as the **Ofsted Review into Sexual Abuse in Schools and Colleges**, which advises close collaboration with **Local Safeguarding Partnerships**.

Searching Pupils' Devices

Any searches of pupils' devices will comply with:

- **The latest DfE guidance on** searching, screening, and confiscation.
- **UKCIS guidance on** sharing nudes and semi-nudes.
- **The school's Behaviour Policy**.

Complaints regarding the searching or deletion of inappropriate images/files on pupils' devices will be addressed through the **school's complaints procedure**.

Handling Online Misuse Proportionately

Most online safety incidents will involve **inappropriate**, rather than **illegal**, misuse. Such incidents should be **handled promptly and proportionately**, ensuring that:

- The **school community is aware** that the issue has been addressed.
- Pupil misuse is managed in line with the **Behaviour Policy**.
- Staff/volunteer misuse is managed through the **Disciplinary Procedure**.

6. Online Safety Training for Staff, Governors, and Volunteers

Staff Training

- **New staff members** will receive training as part of their induction on **safe internet use** and **online safeguarding issues**, including **cyberbullying** and the **risks of online radicalisation**.
- **All staff members** will receive refresher training at least **once per academic year** as part of their **safeguarding training**, with **additional updates** provided as necessary (e.g., via **emails, e-bulletins, and staff meetings**).

Through this training, all staff will be made aware that:

- **Technology plays a significant role** in many safeguarding and wellbeing concerns, and children are at risk of **online abuse**.
- **Children can abuse their peers online** through:
  - **Abusive, threatening, harassing, and misogynistic messages**.
  - **Non-consensual sharing** of indecent **nude or semi-nude images/videos**, particularly within chat groups.

    - **Sharing abusive images or pornography** with individuals who do not wish to receive such content.
- **Physical abuse, sexual violence, and initiation/hazing-type violence** can all have **an online element**.

Training Objectives

Staff training will help participants:

- **Recognise the signs and symptoms** of online abuse.
- **Support pupils** in identifying **risks and dangers** in online activity.
- **Encourage pupils** to make safe, informed decisions online while protecting their **short-term and long-term wellbeing**.

DSL and Deputy DSL Training

- The **Designated Safeguarding Lead (DSL) and Deputy DSLs** will complete **child protection and safeguarding training**—including **online safety**—**at least every two years**.
- They will also update their **knowledge and skills** on online safety at regular intervals, and at least **annually**.

Governor and Volunteer Training

- **Governors** will receive training on **safe internet use and online safeguarding issues** as part of their **safeguarding training**.
- **Volunteers** will receive appropriate **training and updates**, where relevant.

For further details, refer to the **Child Protection and Safeguarding Policy**.

7. Technology

At St Peter's C of E Academy, we are responsible for ensuring that the **school's digital infrastructure and network** are as safe and secure as reasonably possible. We also ensure that all **relevant policies and procedures** outlined in this document are **implemented and communicated** to all staff regularly. Every member of the school community is responsible for **online safety and data protection**.

7.1 Definitions

- **"digital systems"** – Includes all school-provided **hardware, software, and services**, such as the network infrastructure, desktop computers, laptops, tablets, phones, music players, and any **future technology** introduced. This also covers websites, web applications, and online services provided as part of the school's digital system.
- **"Users"** – Anyone **authorised** by the school to use the digital systems, including **governors, staff, pupils, volunteers, contractors, and visitors**.
- **"Personal use"** – Any **non-work-related** activity conducted using the school's digital systems.
- **"Authorised personnel"** – Employees designated by the school to **perform systems administration and/or monitor** digital facilities.
- **"Materials"** – Any **files or data** created using the digital systems, including documents, photos, audio, video, printed output, web pages, and content on social networking sites or blogs.

7.2 Access to School Digital Facilities and Materials

Infotechdirect Ltd manages access to the **school's digital systems and materials** for staff, including but not limited to:

- **Computers, iPads, tablets, and other devices**.
- **Access permissions** for specific programmes or files.

All staff are provided with **unique login credentials and passwords** to access the school's digital systems. **Infotechdirect Ltd** collaborates with St Peter's Academy to provide digital solutions and guidance, though additional costs may apply (e.g., broadband services).

7.3 School-Owned /Provided Devices

All staff must take **appropriate security measures** to protect their school-issued devices, including:

- **Using strong passwords** (at least **8 characters recommended**, including upper- and lower-case letters, numbers, and special characters).
- **Setting automatic screen locks** after a period of inactivity.
- **Not sharing devices** with family or friends.
- **Keeping operating systems updated** with the latest security patches (i.e. regularly installing updates provided by the operating system manufacturer (such as Microsoft, Apple, or Linux developers) to fix security vulnerabilities, improve performance, and protect against cyber threats like viruses, malware, and hackers.
- All school property, such as laptops, should be handled with **due care and responsibility**.

Infotechdirect Ltd will

- **Ensure hard drive encryption** to prevent unauthorised access if the device is lost or stolen.
- **Install and maintain** anti-virus and anti-spyware software.

Staff must use school-provided devices **exclusively for work-related purposes** and adhere to the **Acceptable Use Agreement** and **Data Protection Policy**. **Remote access** must follow the same security protocols as on-site use. **Confidential or protected information** must be handled with extreme caution, in compliance with data protection regulations.

If staff have concerns about the **security of their device**, they must consult **Infotechdirect Ltd** immediately.

7.4 Mobile Technologies

The school's **Acceptable Use Agreement** (Appendix 6) and **Standard for the Use of Mobile Phones and Smart Watches** (Appendix 3) outline expectations regarding mobile technology use.

7.5 Emails

- The school provides each staff member with a **work email address** for **all official communication**.
- Staff **must not** share their **personal email addresses** with parents or pupils.
- **Work-related materials** must not be sent using personal email accounts.
- Temporary email accounts **may be provided** for specific needs (e.g., home learning).
- Staff must ensure that email content is **professional and appropriate**, as improper statements may lead to legal claims for **discrimination, harassment, defamation, or breach of confidentiality**.
- Emails are subject to disclosure in **legal proceedings** or under the **Data Protection Act 2018**. Deleting an email does **not** guarantee permanent removal.
- **Sensitive or confidential information** sent via email must be **encrypted**.

- If an email is received in error, the recipient must **inform the sender and delete the email**. **Confidential content must not be disclosed or used**.

7.6 Personal Use of Digital Systems

Staff may use the school's digital systems for **occasional personal use**, provided that:

- It does **not occur during teaching time**.
- It constitutes **acceptable use**.
- It takes place when **no pupils are present**.
- It does **not interfere** with school operations or impact other staff/pupil access.

Restrictions:

- Staff **must not store personal files** (e.g., music, videos, or photos) on school digital systems.
- Personal use is subject to **digital monitoring activities** (see section **7.7**).
- Personal digital use (even outside school facilities) **can impact employment** (e.g., sharing personal details online where pupils/parents may see them).
- Staff must follow the **school's social media guidelines** (section 7.7) and **email usage policies** (section 7.5).

7.7 School Media Use

St Peter's C of E Academy recognises social media's role in education and personal life but expects **professional standards** in line with **DfE Teacher Standards.**

7.7.1 General Social Media Guidelines

- Personal information **must not** be published i.e. no private or sensitive details about students or staff. This includes:
  - Names, addresses, phone numbers, or email addresses
  - Photos or videos of individuals without consent
  - Personal opinions or confidential information
  - Any other data that could identify or compromise someone's privacy
- Staff and pupils receive education on **social media risks, privacy settings, data protection, and reporting procedures**.
- Reporting procedures for **social media concerns** are clearly outlined.
- Guidance is provided to **learners, parents, and carers** on appropriate social media use.

7.7.2 Expectations for Staff

- Staff **must not reference learners, parents, or colleagues** on personal social media.
- Discussions about **school-related matters** online are **prohibited**.
- Personal opinions must not be **attributed to the school**.
- Personal social media **security settings must be regularly reviewed**.
- Staff must act as **positive role models** in their social media activity.

7.7.3 Official School Social Media

- **Senior leadership** manages the official school social media account 'X', formerly Twitter.
- Posts and comments are **moderated and monitored** by leadership.
- Any **breaches** involving school social media may result in **disciplinary action**.

7.7.4 Monitoring Public Social Media

- The school may **monitor public online content** related to St Peter's C of E Academy.
- Concerns raised via social media will be **redirected to formal complaint procedures**.

7.8 Digital and Video Images

- The use of digital imaging technology follows **MAT policy guidance**.
- Learners receive education on **digital image risks and responsible sharing**.
- Staff and volunteers are informed of **students who cannot be photographed**.
- S**chool-owned devices** should be used for image capture unless explicitly permitted.
- Parents may take photos/videos at school events for **personal use only**, in line with **ICO guidance** (sharing on social media is prohibited).
- **Full names** will not be published alongside images.
- **Parental consent** is required for school photography use.

7.9 Digital Systems Monitoring and Compliance

The school reserves the right to **monitor** digital usage, including:

- Internet browsing history.
- Bandwidth consumption.
- Emails and phone calls.
- User access logs.

Only **authorised digital systems staff** may inspect, monitor, or disclose digital use, in compliance with the law. Monitoring ensures:

- Compliance with school policies.
- Protection of school operations and security.
- Prevention of cybercrime.

8. Data security

The school implements measures to protect the security of its computing resources, data, and user accounts. However, absolute security cannot be guaranteed. Staff, pupils, parents, and others using the school's digital systems must follow safe computing practices at all times.

8.1 Passwords

- All users must set strong passwords for their accounts and keep them secure.
- Users are responsible for the security of their passwords and accounts, as well as for setting appropriate access permissions for any files or accounts under their control.
- Staff or pupils who disclose their passwords or account details may face disciplinary action. Parents and volunteers who do so may have their access rights revoked.

8.2 Software updates, firewalls, and anti-virus software

- All school digital systems devices that support software updates, security patches, and anti-virus protection will be configured for automatic or scheduled updates.
- Our digital systems provider, Infotechdirect Ltd, manages remote updates and security patches.
- Users must not disable or bypass any administrative, physical, or technical safeguards implemented to protect school systems and data.
- Any personal devices connected to the school network must meet these security standards.

8.3 Data protection

All personal data must be processed and stored in compliance with data protection regulations and the school's Data Protection Policy.

8.4 Access to facilities and materials

- User access rights to school systems, files, and devices are strictly managed by Infotechdirect Ltd.
- Users must not attempt to access systems, files, or devices beyond their granted permissions. If they gain unintended access, they must report this immediately to Infotechdirect Ltd.
- Users must log out of systems and lock devices when not in use to prevent unauthorised access. At the end of each working day, systems and devices must be logged out and shut down completely.
- **Wi-Fi Access:**
    - School staff may use the **guest Wi-Fi** for personal use, subject to policy guidelines.
    - The **staff Wi-Fi** is strictly for educational and business purposes.
    - Visitors may be provided with a guest Wi-Fi password if internet access is necessary for their visit (e.g., accessing materials for presentations, lesson plans, or PTFA payment devices).

8.5 Encryption

- The school ensures that its devices and systems have an appropriate level of encryption.
- Staff may only use personal devices (including laptops and USB drives) to access school data, work remotely, or take personal data (such as pupil information) off-site **with prior authorisation from the Head Teacher**.
- Authorisation will only be granted if the personal device meets the encryption and security standards defined by Infotechdirect Ltd.

8.6 Secure Device Disposal

- School devices containing sensitive data mist be disposed of in a secure manner by a company that certifies data removal or destruction.

8.7 Data breach handling

- Any suspected data breaches must be reported to the DPO immediately (and within 24 hours), with Infotech notified thereafter

8.8 A1 and Deepfake Awareness

- Pupils will be taught to **identify AI-generated misinformation** as part of the **online safety curriculum**.
- Teachers must **verify AI-generated content** before using it for learning purposes.
- Staff are prohibited from creating or sharing **deepfake media** involving pupils or colleagues.
- Any AI-generated content used in school must be **fact-checked for accuracy**.

9. Links with other policies

This Online Safety Policy is linked to:

- **Child Protection and Safeguarding Policy**
- **Behaviour Policy**

- **Staff Disciplinary Procedures**
- **Data Protection Policy and Privacy Notices**
- **Acceptable Use Codes of Conduct** (Appendices 4–6)
- **Standard for Mobile Phones and Smart Watches** (Appendix 3)

Appendix 1: Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Data Protection Act 2018
- Computer Misuse Act 1990
- Human Rights Act 1998
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Freedom of Information Act 2000
- The Education and Inspections Act 2006

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Appendix 2: Online Safety Incident Report Log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 3: Standard for Mobile Phone and Smart Watches

Objectives

Our aim is that all users:

- Have a clear understanding of what constitutes misuse.
- Know how to minimise risk.
- Avoid putting themselves in compromising situations that could be misinterpreted and lead to possible allegations.
- Understand the need for professional boundaries and clear guidance regarding acceptable use.
- Are responsible for self-moderation of their behaviour.
- Are aware of the importance of promptly reporting concerns.

While we recognise that rigid regulations can be counterproductive, we promote an **agreement of trust** regarding the carrying and use of mobile phones within the school setting, which all users are expected to adhere to.

Personal Mobiles and Smart Watches

For Staff, Volunteers, Peripatetic Teachers, and Visitors

- Staff, volunteers, and visitors **must not** make or receive calls or texts during contact time with children. **Emergency contact** should be made via the school office.
- Staff must keep their phones on **silent or switched off and out of sight** (e.g., in a bag, drawer, or cupboard) during class time.
- Smart watches may be worn but **must have camera, messaging, and call services disabled** during the school day.
- Mobile phones must not be used in spaces where children are present (e.g., classrooms, playgrounds).
- Use of phones—including receiving/sending texts, emails, or messages on smart watches—is limited to **non-contact time when no children are present**, such as in the office areas, staff room, or empty classrooms.
- In exceptional circumstances (e.g., acutely ill relative), staff should inform the **Head Teacher**, and arrangements will be made for emergency calls via the school office.
- Personal mobile phones or smart watches should not be used to record or share images of children. Any photos taken by staff for **legitimate school purposes and with explicit permission from Mr. Tomlinson or Mrs. Gibbens, must be uploaded to the school system immediately** and **deleted from personal devices without delay.**
- Any concerns regarding mobile device usage should be reported to the **Head Teacher** immediately.

Mobile Phones for work related purposes

While mobile phones may be useful during **off-site activities**, staff must ensure:

- Mobile use remains **appropriate and professional** at all times.
- Mobile phones should only be used to contact parents during school trips outside of office hours and only when no landline is available. In these instances, dial 141 to withhold the caller's number. Wherever possible, all relevant communications should be made through the school office.
- Parents accompanying trips are informed that they must **not**:
    - Contact other parents (via calls, text, email, or social media) during the trip.
    - Use their phone/smart watch to take photographs of children.

- Any photos taken of children for **legitimate school purposes** (e.g., school trips) must be **uploaded to the school system immediately** and **deleted from personal devices without delay**.

Personal Mobiles and Smart Watches

We recognise that mobile phones and smart watches are part of everyday life for many children and can play a role in ensuring their safety. However, they can also be distracting and may facilitate bullying or inappropriate behaviour. Therefore:

- **Pupils are not permitted to have mobile phones at school**, unless they are in **Year 5 or 6** and have permission to walk home alone.
- These phones must be **switched off** and left in the **school office upon arrival**, to be collected at the end of the day. *(Phones are left at the owner's own risk.)*
- **Smart watches must not be brought to school.** If a child wears a smart watch, it **must not have any internet connection** while at school.

Tracking, Apple Airtags or equivalent (School Trips)

- **Tracking devices, such as Apple AirTags, must not be attached to pupils or their belongings** during school trips or residentials. This is a **safeguarding decision**.
- While tracking devices can enhance security in crowded places (e.g., festivals, theme parks), they must not be used for **surveillance** of children.
- School trips and residentials are **risk-assessed and supervised by experienced staff** to ensure safety

Volunteers, Visitors, School Stakeholder Committee Members, Peripatetic Teachers and Contractors

- All visitors, volunteers, and contractors must **follow the school's mobile phone and smart watch policy** while on the premises.
- Upon arrival, visitors will be **informed of these expectations**.
- While a smart watch may be **visible on an adult's wrist**, it must be in **silent mode** and **not used during the working day**, except to check the time.
- While we **discourage** parents and carers from using mobile phones on school premises, we recognise that this is difficult to regulate. **We ask that usage remains courteous and appropriate**.

Parents and Carers Taking Photos/Videos at School Events

- Parents and carers may take **photographs or videos** of school events (e.g., performances, sports days), **provided there are no parental objections or safeguarding concerns**.
- However, **photos or videos must not be published online** (e.g., on social media) if they contain images of **children other than their own**.

Appendix 4: Acceptable Use Agreement for Pupils

St Peter’s C of E Academy - My Online Safety Agreement

🌟 **I promise to use computers, iPads, and the internet safely and kindly!** 🌟

1. Staying Safe

🔹 I will ask an adult if I am unsure about a website.
🔹 I will never share my full name, address, or passwords online.
🔹 If something makes me feel worried or upset, I will tell a teacher straight away.

2. Being Kind Online

💬 I will always use kind words when talking to others.
🚫 I will not send messages that could hurt someone’s feelings.
📸 I will not take or share pictures of others without permission.

3. Looking After Devices

🖥️ I will take care of school computers, iPads, and equipment.
❌ I will not change settings or download anything without asking.
🔌 I will use the internet for schoolwork and fun learning.

4. Making Good Choices

✅ I will only go on websites my teacher says are safe.
❌ I will not play games or watch videos that are not allowed in school.
🔎 If I see something wrong or scary, I will tell an adult.

My Promise:

I understand these rules and will follow them to stay safe and happy online!

Appendix 5: Acceptable Use Agreement for Parents and Carers

Background

As part of our commitment to **online safety and safeguarding**, the school requires all **parents, pupils, and staff** to adhere to our **Acceptable Use Agreements**. This document promotes the **safe and responsible** use of digital technologies both in school and at home.

This agreement **does not require a signature**, but adherence to its guidelines is **non-negotiable and expected**.

The school takes **online safety very seriously** and actively promotes the **safe and secure** use of digital technologies and the internet. Pupils receive **regular lessons and assemblies** about online safety and general safeguarding.

Safeguarding

In accordance with school policy, as sanctioned by the **Governors** and the **Head Teacher**, **mobile phones and smart watches are not permitted for pupils in school**.

This decision is rooted in **safeguarding concerns**, as it mitigates risks such as:

- Unsupervised contact with individuals outside of school
- Access to inappropriate online content

Children are reminded of this policy during assemblies, and the school **appreciates parental support** in enforcing these guidelines.

Internet and Digital Systems Usage

- Parents **grant permission** for their child to access the **school's digital systems**, including the **internet**, in accordance with the school’s **Online Safety and Acceptable Internet Use Policy**.
- Parents acknowledge the **Online Safety and Anti-Bullying Policies** and agree to support their child in understanding the importance of using technology **safely and responsibly**, both in and out of school.

Devices in School

- If a **Year 5 or Year 6** pupil **must** bring a mobile phone to school for **independent travel** purposes, the device must be:
    - **Switched off** upon arrival
    - **Handed to the school office** for safekeeping
    - **Collected at home time**
- The **school is not responsible** for any **loss or damage** to devices.
- **Under no circumstances** should pupils access their **mobile phone or smart watch during the school day**. Devices **must not** be kept in pupils’ bags or coats.
    - **Failure to comply** will result in **confiscation** of the device. Parents will be notified and required to **collect it from the school office**.
- **Exceptions may be made** for medical purposes (e.g., diabetes monitoring apps), subject to prior discussion with the school.

Digital Watches

- **Step-counting digital watches** (without additional features) are **permitted**, as they encourage physical activity.
- However, if a step-counting watch includes **photo-taking, communication, or internet connectivity features**, the child will be asked to **leave it at home** or **hand it to their teacher** each day.

Tracking Devices on School Trips

- **Apple AirTags or similar tracking devices** must **not** be attached to pupils or their belongings during **school trips or residential visits**.
- While **tracking devices** provide an **extra layer of security**, they can also **compromise children’s privacy** if used for excessive surveillance.
- All school trips and residential visits are **risk-assessed** and **supervised by experienced staff** to ensure children's safety.
- The school **appreciates the trust and support of parents** in enabling children to **fully benefit from these valuable out-of-school experiences**.

Appendix 6: Acceptable Use Agreement for Staff and Volunteers

Introduction

New technologies have become integral to the lives of children and young people in today's society. Information and communication technologies (digital systems) are powerful tools that open up new opportunities for learning, collaboration, and creativity. These technologies also enable staff and volunteers to be more productive and efficient in their roles.

All users should have **safe and secure** access to the internet and digital technologies at all times.

Purpose of This Policy

This Acceptable Use Agreement ensures:

- That all staff and volunteers act as **responsible users**, prioritising online safety while using digital technologies for educational, personal, and recreational purposes.
- That school/academy systems and users are **protected from accidental or deliberate misuse** that could compromise security.
- That all adults are **protected from potential risks** when using technology in their professional roles.

The school will endeavour to provide **reliable access to digital technology** to support staff in their work and enhance pupils' learning experiences. In return, staff and volunteers are expected to use technology responsibly.

Internet and Digital Systems Acceptable Use Agreement

I understand that I must use the school's digital systems responsibly to protect my safety, the security of school systems, and other users. I recognise the value of digital technology in enhancing learning and will ensure that pupils benefit from its use.

Where possible, I will educate pupils in **safe digital practices** and embed online safety principles in my work with children.

Professional and Personal Safety

- I understand that **St Peter's C of E Academy** will **monitor** my use of digital technology and communication systems.
- The rules in this agreement **apply to my use of digital systems both in and outside of school**, including the transfer of personal data (digital or paper-based).
- School digital technology systems are **primarily for educational use**, and I will only use them for personal or recreational purposes within the school's policies.
- I will **not disclose my login credentials** to anyone or attempt to use another person's login details. I will take appropriate measures to keep my password secure.
- I will **immediately report** any illegal, inappropriate, or harmful content or incidents to the appropriate person.

Professional Conduct and Communication

- I will **not access, modify, or delete another user's files** without explicit permission.
- I will communicate **professionally and respectfully** with pupils, colleagues, and parents/carers, avoiding aggressive or inappropriate language.
- I will **only use official school communication systems** to contact pupils and parents/carers, ensuring that all communication is professional in tone and manner.

- I will ensure that I **only capture and publish images or videos of individuals with their permission**, following the school's policy on digital/video images.
  - I will **not use personal devices** to take images or videos unless explicitly permitted.
  - If publishing images (e.g., on the school website), I will ensure that individuals **are not identifiable by name or other personal information**.
- I will **not engage in online activities** that could compromise my professional responsibilities.

School and Aspire MAT Responsibilities for Safe Technology Use

Use of Personal Devices on School Premises

- When using **personal devices** (e.g., laptops, iPads, mobile phones) in school, I will adhere to this agreement as if using school-owned equipment.
- I will ensure my devices are **protected by up-to-date antivirus software** and free from malware.

Email and Internet Security

- I will **not open hyperlinks or attachments** in emails unless the sender is known and trusted. If I have concerns about the legitimacy of an email, I will verify before opening any attachments.
- I will **regularly back up my data** in accordance with school policies.

Content Restrictions and System Security

- I will **not attempt to access, download, or distribute illegal or inappropriate materials**, including but not limited to:
  - Child sexual abuse content
  - Criminally racist material
  - Pornographic content covered under the **Obscene Publications Act**
  - Material that could cause harm or distress to others
- I will **not attempt to bypass** the school's internet filtering or security systems.
- I will **not make large downloads or uploads** that could disrupt network performance.
- I will **not install software or alter computer settings** unless explicitly allowed by school policies.
- I will **not disable, damage, or interfere with school equipment** or the property of others.

Data Protection and Confidentiality

- I will handle **personal and sensitive data** with strict confidentiality, following school policies and **data protection regulations**.
- Any **digital personal data transferred outside the school network must be encrypted**.
- **Paper-based confidential information must be securely stored** in lockable storage.
- I understand that **pupil data is private and confidential** and will only disclose it when legally required or in accordance with school policy.

Reporting and Compliance

- I will **immediately report any faults, damages, or security concerns** regarding digital systems or equipment.

Use of the Internet for Professional and Personal Purposes

- I will **only use copyrighted materials with appropriate permissions** and will not download or distribute unauthorised copies (e.g., music, videos).

Responsibility and Consequences

I understand that:

- This **Acceptable Use Agreement applies to both my work at school and any use of school systems outside the premises**.
- If I **fail to comply**, I may face **disciplinary action**, which could include:
  - A formal warning
  - Suspension
  - Referral to **Governors and/or the Trust**
  - In cases of illegal activity, **police involvement**

Agreement Acknowledgment

I have read and understood this **Acceptable Use Agreement** and agree to comply with its guidelines when using:

- **School digital technology systems (both in and out of school)**
- **My personal devices when conducting school-related communications**

Signature: ________________________

Date: ________________________