



Online Safety Policy

Created: Spring 2026

Next Review: Autumn 2027

1. Introduction and Scope

This policy applies to all members of the St Peter's community (including staff, pupils, volunteers, parents/carers, and visitors) who have access to the school's technology or who interact with pupils online.

Our policy is built upon the **Education for a Connected World** framework and statutory guidance from **Keeping Children Safe in Education (KCSIE)**. It operates in conjunction with our Child Protection, Behaviour, and Data Protection policies.

2. Our Approach: The 5 Cs

To ensure our staff and families have a clear, practical understanding of online risks, we categorise potential harms using the **5 Cs**. This framework mirrors the language used in our **Online Safety Curriculum**, ensuring consistency between what pupils are taught and how staff safeguard them.

1. **Content:** Risk of being exposed to illegal, inappropriate, or harmful material (e.g., pornography, fake news, racist or hate speech).
2. **Contact:** Risk of being subjected to harmful online interaction with others (e.g., grooming, peer-to-peer cyberbullying).
3. **Conduct:** Risk of personal online behaviour that increases the likelihood of, or causes, harm (e.g., sending non-consensual nude images/sexting, bullying others).
4. **Commerce:** Risks such as online gambling, inappropriate advertising, phishing, or financial scams.
5. **Cybersecurity (Conspiracy):** Risks involving data theft, hacking, and the spread of misinformation/disinformation.

3. Curriculum and Education

At St Peter's, we do not just filter the internet; we teach children to be resilient users of it.

- **Curriculum Framework:** We deliver a robust, age-appropriate curriculum aligned with the 'Education for a Connected World' framework.
- **Delivery:** As detailed in our **Online Safety Curriculum**, lessons are taught explicitly in every year group (6 lessons per year).
- **Focus:** Topics progress from foundational knowledge in Early Years to advanced digital resilience in KS2, covering privacy, reputation, and critical thinking.

4. Use of Personal Devices

Mobile Phones (Pupils)

- **General Rule:** Pupils are generally not permitted to have mobile phones on school premises.
- **Exception (Year 5/6):** Pupils in Year 5 or 6 who walk home alone may bring a mobile phone for safety on their journey.
- **Procedure:** Upon arrival, the phone must be switched off and handed immediately to the school office (or class teacher, as per site procedure) for secure storage. It can be collected at the end of the school day.
- **Breach:** If a pupil is found with a phone in class, it will be confiscated and returned only to a parent/carer.

Smartwatches and Wearables

- **Not Allowed:** Smartwatches (including Apple Watches, V-Tech watches, or any device capable of taking photos,

recording audio, or receiving messages) are **not permitted** in school.

- **Rationale:** These devices present a safeguarding risk regarding data protection, distraction, and the potential for unmonitored communication.
- **Fitbits/Activity Trackers:** Simple activity trackers that do **not** have cameras, microphones, or communication features are permitted.

5. Staff and Professional Conduct

- **Staff Devices:** Personal phones and smartwatches must not be used during teaching time or in areas where pupils are present. They should be stored securely.
- **Social Media:** Staff are advised to keep personal social media profiles private and must not accept "friend requests" from current pupils or recent leavers.
- **Photography:** Only school-owned devices/cameras are to be used for photographing or recording pupils.

6. Spotting the Signs

Staff should remain vigilant to signs that a child may be at risk online. These changes in behaviour can often be subtle:

- **Emotional:** appearing withdrawn, upset, or angry after using a device.
- **Secretive:** switching screens or closing apps when an adult approaches; being secretive about who they are talking to.
- **Social:** spending significantly more or less time online/gaming; unexpected changes in friendship groups.
- **Physical:** tiredness or lack of concentration due to late-night device use.

7. Reporting Incidents

- **Safeguarding Concerns:** Any concern involving grooming, sexual abuse, or radicalisation must be reported immediately to the **Designated Safeguarding Lead (DSL)** and logged on [Insert System, e.g., CPOMS/MyConcern].
- **Inappropriate Content:** If illegal content (e.g., child sexual abuse images) is discovered on a device, staff must **not** view it further or forward it. Secure the device immediately and contact the DSL.
- **Cyberbullying:** Incidents will be dealt with under the school's Anti-Bullying and Behaviour Policy.

Recommended Resources for Staff & Parents

Here is a list of high-quality, trusted resources to support your policy and curriculum.

For Staff (Curriculum & Training):

- **Project Evolve:** Free digital literacy toolkit that maps directly to the "Education for a Connected World" framework.
- **LGfL (London Grid for Learning):** Excellent resources on critical thinking and fake news (Cybersecurity).
- **Barefoot Computing:** Great for integrating safety into computational thinking.

For Parents & Families:

- **Internet Matters:** Very user-friendly guides on how to set parental controls on specific apps (TikTok, Roblox, etc.) and broadband.
- **Common Sense Media:** Reviews of games and movies from a child-suitability perspective.
- **Ask The Awkward (CEOP):** Helps parents handle difficult conversations with their children about online relationships.
- **NSPCC Net Aware:** Up-to-date guide on the latest social networks pupils are using.

