ST. PETER AT GOWTS
CofE PRIMARY SCHOOL
Unlocking the potential in all, empowering a community of hope.

St Peter at Gowts Church of England Primary School

Policy	**Online Safety**
Date adopted	**June 2023**
Date reviewed	**September 2025**

1. Introduction

Online safety is of paramount importance at St Peter at Gowts CE Primary School. As the online world evolves, so do the harms and risks facing children. This policy reflects the latest statutory guidance, including Keeping Children Safe in Education (KCSIE) 2025, Working Together to Safeguard Children (2023), DfE Teaching Online Safety in Schools (2019), the Data Protection Act 2018 and UK GDPR, and the Prevent Duty Guidance (2023). Our school adopts a whole-community approach, ensuring all staff, pupils, governors, parents, and volunteers understand their responsibilities to keep children safe online.

2. Aims and Objectives

- To safeguard pupils when using technology both in and outside of school.
- To ensure appropriate filters and monitoring systems are in place and regularly reviewed.
- To educate pupils, staff, and parents about online risks, including those emerging from new technologies.
- To respond effectively to any online safety incident, following statutory safeguarding procedures.
- To foster a whole-school culture where online safety is everyone's responsibility.

3. Key Guidance and Legislation

This policy reflects:

- Keeping Children Safe in Education (KCSIE) (2025)
- Working Together to Safeguard Children (2023)
- Online Safety Act (2023)
- DfE Teaching Online Safety in Schools (2019)
- Data Protection Act 2018 and UK GDPR
- Prevent Duty Guidance (2023)

KCSIE 2025 highlights the need for schools to:

- Recognise the impact of **emerging technologies** such as AI chatbots, deepfakes, and algorithm-driven content.
- Address risks associated with **livestreaming, harmful online challenges and hoaxes**.
- Strengthen responses to **child-on-child abuse** in online contexts.
- Maintain **appropriate filtering and monitoring systems**, with clear leadership oversight.

4. Roles and Responsibilities

4.1 Governing Body

- Ensure the school has appropriate filtering and monitoring systems.
- Review online safety policies annually.

- Receive regular safeguarding reports including online safety data.

4.2 Headteacher and Senior Leadership Team (SLT)
- Embed online safety within the school's safeguarding approach.
- Oversee risk assessments for digital technologies and online platforms.
- Ensure staff are trained to recognise and respond to online risks.

4.3 Designated Safeguarding Lead (DSL)
- Take lead responsibility for online safety concerns.
- Review filtering/monitoring reports weekly and respond to flagged activity.
- Ensure online safety incidents are recorded and reported via CPOMS or equivalent.
- Keep up to date with emerging online threats (e.g. AI misuse, sextortion scams, harmful online challenges, and hoaxes).

4.4 Staff
- Model safe, responsible online behaviour.
- Report online safety concerns immediately to the DSL.
- Deliver online safety teaching as part of the curriculum.
- Maintain professional boundaries when communicating with pupils online.

4.5 Pupils
- Follow the school's Acceptable Use Policy (AUP).
- Report anything online that makes them feel worried or unsafe.
- Use school technology respectfully.

4.6 Parents and Carers
- Support the school's approach to online safety.
- Encourage safe online behaviour at home.
- Engage with resources and information provided by the school.

5. Education and Training
5.1 Pupils
- Critical thinking skills to evaluate online content.
- Recognising techniques used for persuasion and misinformation.
- Understanding the risks of sharing personal information, images, and livestreaming.
- Awareness of cyberbullying, child-on-child abuse online (including online sexual harassment), and reporting routes.
- Understanding harmful online challenges and hoaxes and how to respond safely.
- Understanding AI risks (deepfakes, manipulated images, algorithmic influence).

5.2 Staff
- Annual safeguarding and online safety training (with updates throughout the year).
- Guidance on managing incidents such as sexting, harmful online challenges, hoaxes, and online harassment.
- Training on appropriate professional conduct online.

5.3 Parents
- Understand the risks of online gaming, social media, harmful challenges, and new technologies.
- Recognise the signs of online harm and how to respond.
- Set up appropriate parental controls and filtering at home.

6. Filtering and Monitoring
Supported by Ark, our IT service provider, St Peter at Gowts CE Primary School uses the Securly filtering and monitoring system to:
- Block access to harmful or inappropriate material.
- Monitor pupils' online activity for signs of risk (e.g. concerning searches, harmful content).
- Generate immediate alerts for high-risk activity to the DSL.

The DSL and Headteacher review filtering and monitoring reports weekly and after any serious incident. Decisions relating to filtering changes are logged and signed off by the Headteacher.

7. Managing Online Safety Concerns
- Any online safety concern will be treated as a safeguarding concern.
- Concerns are reported to the DSL, logged on CPOMS, and actioned in line with child protection procedures.
- Where illegal content or criminal activity is suspected, the DSL will contact the police and relevant agencies (e.g. CEOP).
- Parents will be informed where appropriate.

Special consideration will be given to online sexual harassment, harmful challenges, and hoaxes, with responses aligned to the school's child-on-child abuse procedures.

8. Mobile Devices and Smart Watches
Pupils are not permitted to use mobile phones or internet-enabled smart watches during the school day. Devices brought to school must be handed in at the office and collected at the end of the day.

9. Monitoring and Review
This policy will be reviewed annually or earlier if:
- There is a significant online incident.
- KCSIE or other guidance is updated.
- New technology introduces potential risks.

10. Related Policies
This policy should be read alongside:
- Safeguarding and Child Protection Policy
- Behaviour Policy
- Data Protection Policy
- Anti-Bullying Policy
- Acceptable Use Policy (AUP)