Temple Ewell Church of England Primary School

Online Safety Policy

Policy written – February 2026

To be reviewed – February 2027

AQUILA
Diocese of Canterbury
Academies Trust

1. Introduction

Temple Ewell CEP School is committed to a whole-school approach to online safety and safeguarding that protects and educates pupils, staff, volunteers and governors in their use of technology.

Technology is now embedded within children's lives. We recognise that online activity can present both significant educational opportunities and safeguarding risks, including child-on-child abuse, exploitation, financial harm and exposure to harmful content.

As of 2026, the provisions of the UK Online Safety Act are fully implemented. While online platforms now have strengthened duties under Ofcom regulation, schools retain a statutory safeguarding responsibility to educate, monitor and respond to online harm.

This policy aligns with:

- Keeping Children Safe in Education (KCSIE) 2024
- DfE Filtering and Monitoring Standards
- UKCIS guidance on sharing nudes and semi-nudes
- The Prevent Duty

Our approach is proactive rather than reactive. We explicitly address:

- Artificial intelligence (AI) and synthetic media
- Deepfake and manipulated imagery
- Algorithm-driven content exposure
- Online scams and financial exploitation
- Digital wellbeing and resilience

Online safety is embedded within our safeguarding culture and curriculum.

2. Aims

› Through this policy we ensure that:

- Robust safeguarding systems protect pupils from online harm
- Online safety education is progressive, explicit and current
- Emerging risks (AI misuse, scams, algorithm influence) are addressed
- Clear reporting and escalation procedures are in place
- Filtering and monitoring systems are effective and proportionate

› In line with KCSIE, we address four areas of risk:

Content – exposure to harmful or illegal material, including AI-generated or manipulated content
Contact – harmful interaction, grooming, coercion or exploitation
Conduct – unsafe online behaviour, including image sharing or harassment
Commerce – scams, gambling, phishing, money mule recruitment and financial exploitation

3. Roles and responsibilities

3.1 The School Governing Body

Governors will:

- Review this policy annually
- Receive an annual filtering and monitoring impact report
- Ensure safeguarding training includes AI and emerging risks
- Hold leaders accountable for online safety implementation
- Ensure provision is adapted for vulnerable pupils

Online safety is a standing safeguarding priority.

3.2 Senior Leaders

- Ensure consistent implementation of this policy
- Understand filtering and monitoring systems
- Ensure emerging risks are reflected in curriculum and practice
- Oversee staff training

3.3 The designated safeguarding lead

The DSL has lead responsibility for online safety.

This includes:

- Monitoring trends in online incidents
- Escalating AI-generated or manipulated imagery immediately
- Ensuring filtering systems flag concerns appropriately
- Delivering staff training
- Reporting digital safeguarding patterns to governors
- Reviewing risk assessments annually

Any AI-generated or manipulated content involving pupils or staff will be treated as a safeguarding concern and investigated under child-on-child abuse procedures where applicable.

3.4 ICT Support Provider (BCTEC)

The school's ICT support provider will:

- Ensure filtering and monitoring systems meet DfE Filtering and Monitoring Standards
- Review filtering provision at least annually in partnership with the DSL and senior leaders

- Ensure systems are updated to respond to emerging risks (e.g., AI content, bypass methods)
- Provide regular reports to support safeguarding monitoring
- Maintain network security, antivirus protection and cyber-security compliance
- Escalate any technical safeguarding concerns immediately to the DSL

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers will:

- Assist with the consistent implementation of this policy by agreeing with and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use.
- Read and understand this policy.
- Agree with and follow the Staff Code of Conduct which outlines what we expect from staff in relation to use of mobile and smart technology, social media, and acceptable online communication with students.
- Work with the DSL to ensure that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Update parents around what their children are being asked to do online, including the sites they may be asked to access and who, if anyone, their child should be interacting with from the school online.
- Recognise and report safeguarding concerns involving AI-generated or manipulated content.

This list is not intended to be exhaustive.

3.6 Parents

Parents and carers will:

- Support the school's online safety expectations at home
- Engage with information shared about emerging risks (AI, scams, algorithm influence)
- Monitor children's access to personal devices outside school
- Encourage safe and respectful online behaviour
- Report concerns about online harm to the school promptly so safeguarding procedures can be followed.

4. Educating pupils about online safety

Online safety is taught through:

- Relationships & Health Education

- Computing curriculum
- Our Purple Mash Online Safety Scheme of Work
- Assemblies and themed events (e.g., Safer Internet Day)
- Digital Leaders programme

Purple Mash provides a structured, age-appropriate progression covering:

- Privacy and personal information
- Password security
- Online relationships
- Cyberbullying
- Digital footprint
- Misinformation
- Online scams
- Responsible use of AI tools

By the end of KS2 pupils will understand:

- That AI can generate images, text and video that may not be real
- What deepfakes are and why they can be harmful
- How algorithms influence the content they see
- How scams target young people (gaming scams, fake giveaways, phishing)
- The concept of digital footprints and cyber-vetting
- How to report concerns confidently

Digital resilience education supports pupils to manage:

- Screen time
- Online comparison
- Exposure to distressing content
- Algorithm-driven feeds

We adapt provision for SEND and vulnerable pupils.

5. Artificial Intelligence and Synthetic Media

The school recognises increasing safeguarding risks linked to generative AI tools.

Risks include:

- AI-generated sexual imagery
- Deepfake bullying
- Voice cloning
- Academic misuse

- Manipulated imagery used for harassment

Pupils are explicitly taught:

- How AI tools work
- That AI can "hallucinate" or fabricate information
- That creating fake images of real people may be illegal
- That sharing manipulated images constitutes serious misconduct.

AI education is embedded within our Purple Mash online safety progression.

Any AI-generated imagery involving a real pupil will be escalated immediately to the DSL.

6. Educating Parents

Parents are supported through:

- Website guidance
- Newsletters
- Parent workshops
- Safer Internet Day communications
- Workshops now include:
- AI-generated content awareness
- Deepfake risks
- Online scams and financial exploitation
- Algorithm influence
- Age assurance under the Online Safety Act

7. Filtering and Monitoring

The school uses schoolsbroadband.net filtering and monitoring systems.

The DSL:

- Reviews daily monitoring reports
- Analyses incident trends
- Reports patterns to governors annually

Filtering provision is reviewed at least annually in line with DfE standards.

Monitoring data is used proactively to inform curriculum planning.

8. Cyber-Bullying

We recognise that cyberbullying now includes:

- AI-generated harassment
- Manipulated imagery
- Large chat group abuse
- Misogynistic or extremist messaging

Cyberbullying may occur both inside and outside school hours and will be addressed where it impacts pupil wellbeing or school life.

All incidents are recorded on Bromcom and escalated appropriately.

9. Devices in School

All pupils hand in mobile phones at the start of the school day.

The school recognises risks from:

- Smartwatches
- Bluetooth sharing
- AirDrop
- Wearable devices

Misuse will be addressed proportionately in line with safeguarding procedures.

10. Acceptable use of the internet in school

All pupils, staff and governors sign acceptable use agreements (Appendix 3).

Use of the internet must be for educational purposes only.

The school monitors usage.

11. Purple Mash Acceptable Use Expectations

As Purple Mash is our core digital learning platform, pupils agree to:

- Use Purple Mash respectfully
- Not share login details
- Not use 2Email or sharing tools inappropriately
- Not create or upload harmful or manipulated content
- Use AI tools ethically in line with school guidance
- Report any concerning content immediately

Purple Mash usage is monitored by staff.

12. Responding to Misuse

Incidents involving:

- Illegal content
- AI-generated harm
- Sexual imagery
- Financial exploitation

Will be escalated to the DSL immediately and managed in line with safeguarding procedures.

Police involvement will occur where appropriate.

All incidents will be recorded on Bromcom in line with safeguarding procedures.

13. Training

All staff receive annual safeguarding training including:

- AI and deepfake recognition
- Scam awareness
- Algorithm-driven harm
- Online financial exploitation
- Child-on-child digital abuse

Staff self-audit (Appendix 1) now includes AI awareness.

14. Monitoring and Review

Online safety incidents are categorised to identify trends such as:

- AI misuse
- Scam exposure
- Peer harassment
- Inappropriate searches

An annual digital safeguarding review informs policy updates.

15. Links with Other Policies

- Child Protection & Safeguarding
- Behaviour
- Staff Code of Conduct
- Data Protection
- Anti-Bullying
- Prevent