# ST PETER'S CEVC PRIMARY SCHOOL
# ONLINE SAFETY POLICY
## September 2026

## 1. Aims

At St Peter's CEVC Primary School, we recognise that technology and the internet are an integral part of children's lives. We are committed to ensuring that all pupils can learn, communicate and use technology safely and responsibly.

This policy aims to:

- Safeguard and promote the welfare of children online.
- Teach pupils how to stay safe, healthy and respectful in digital environments.
- Support staff and parents in promoting safe use of technology.
- Establish clear expectations for the use of digital technology.
- Ensure appropriate systems are in place to protect children from online harm.

Online safety is an essential part of safeguarding and all concerns will be managed in line with the school's Child Protection Policy.

---

## 2. Scope

This policy applies to:

- Pupils
- Staff
- Governors
- Volunteers
- Contractors
- Parents and carers
- Visitors using school technology or accessing school systems

The policy covers the use of:

- The internet
- Digital devices
- Online communication platforms
- Social media
- Artificial Intelligence (AI) tools
- School networks and systems

---

## 3. Roles and Responsibilities

### *Governing Body*

The Governing Body will:

- Approve and review this policy annually.
- Ensure appropriate safeguarding arrangements are in place.
- Monitor the effectiveness of filtering and monitoring systems.

### *Headteacher*

The Headteacher is responsible for:

- Ensuring this policy is implemented.
- Supporting a culture of online safety.
- Ensuring staff receive appropriate training.

### *Designated Safeguarding Lead (DSL)*

The DSL has lead responsibility for online safety and safeguarding online.

The DSL will:

- Respond to online safety concerns.
- Oversee filtering and monitoring arrangements.
- Work with technical providers to ensure systems remain effective.
- Ensure staff receive regular updates and guidance.
- Record and respond to incidents through safeguarding procedures.

### *Staff*

All staff will:

- Model safe and professional online behaviour.
- Teach online safety through the curriculum.
- Supervise children's use of technology.
- Report concerns immediately through safeguarding procedures.

### *Pupils*

Pupils are expected to:

- Use technology safely and responsibly.
- Follow the school's Acceptable Use Agreement.
- Report anything online that makes them feel worried, unsafe or uncomfortable.

### *Parents and Carers*

Parents and carers are encouraged to:

- Support children to use technology safely.
- Monitor online activity at home.
- Work in partnership with the school when concerns arise.

---

## 4. Teaching Online Safety

Online safety is taught throughout the curriculum and is embedded within:

- Computing
- PSHE and RSE
- Collective Worship and assemblies
- Safeguarding learning opportunities

Teaching will include:

- Keeping personal information safe.
- Healthy online relationships.
- Cyberbullying.
- Social media awareness.
- Online scams and misinformation.
- Responsible use of AI.
- Privacy and consent.
- Reporting concerns and seeking help.

Online safety education is delivered through Computing lessons, Project Evolve and PSHE/RSE learning.

---

## 5. Safeguarding and Reporting Concerns

Any online safety concern is treated as a safeguarding concern.

Staff must:

- Act immediately.
- Record concerns using school safeguarding procedures.
- Inform the DSL or Deputy DSL on the same day.

Examples may include:

- Cyberbullying
- Exposure to harmful content

- Online grooming
- Child-on-child abuse
- Sharing inappropriate images
- Online harassment
- Extremist content
- AI-generated harmful content

The school will work with external agencies where necessary, including children's social care and the police.

---

## 6. Filtering and Monitoring

The school uses filtering and monitoring systems to help protect pupils online.

These systems are regularly reviewed and aim to:

- Block harmful and inappropriate content.
- Monitor potential safeguarding concerns.
- Support pupils' safe access to educational resources.

No filtering system can provide complete protection. Active supervision by staff remains essential.

The DSL has strategic responsibility for filtering and monitoring arrangements.

---

## 7. Mobile Phones, Devices and Social Media

### *Pupils*

Pupils may only bring mobile phones to school where permission has been given by parents and the school (see mobile phone policy).

Phones must be handed to staff on arrival and collected at the end of the school day.

### *Staff*

Staff must follow the Code of Conduct regarding personal devices and communication.

Personal devices must not be used to communicate with pupils.

### *Social Media*

All members of the school community are expected to use social media responsibly.

Parents and carers should raise concerns directly with the school rather than through social media platforms.

Recording staff, pupils or other members of the school community without permission is not permitted.

---

## 8. Artificial Intelligence (AI)

The school recognises that AI technologies are increasingly part of children's lives.

Pupils will be taught:

- How AI can be used positively.
- How AI can generate inaccurate information.
- The risks associated with deepfakes and manipulated images.
- How to report concerns involving AI-generated content.

Staff may use approved AI tools to support professional practice but must never enter confidential or personal pupil information into AI platforms.

---

## 9. Data Protection and Cyber Security

All users of school systems must comply with the school's Data Protection Policy and Cyber Security procedures.

Staff will:

- Protect passwords.
- Use multi-factor authenticator for emails and other secure platforms.
- Use approved school systems.
- Store information securely.
- Report any suspected data breach immediately.

The school recognises that safeguarding concerns override concerns about sharing information where a child may be at risk of harm.

---

## 10. Monitoring and Review

This policy will be reviewed annually by the Headteacher/DSL.

The Governing Body will monitor its implementation and effectiveness through safeguarding updates and annual policy review.

---

## Key Contacts

**Designated Safeguarding Lead (DSL):** Sam Wilding

**Deputy DSL:** Vanessa Sullivan

**Safeguarding Governor:** Louise Cowan

**Computing Lead:** Andy Robertson

**PSHE/RSE Lead:** Alice Rassell