FEDERATION OF GORING AND STOKE ROW CHURCH OF ENGLAND PRIMARY SCHOOLS

DIGITAL TECHNOLOGY, ONLINE SAFETY AND ACCEPTABLE USE POLICY

Policy reviewed and agreed by:	Teaching, Learning and Inclusion Committee
Date:	March 2026
Next review:	March 2028

Contents

1. Aims

The Federation of Goring and Stoke Row Church of England Primary Schools is committed to safeguarding and promoting the welfare of children. Technology is a central part of modern life and education, and safeguarding must reflect this.

This policy aims to:

- Ensure robust processes are in place to safeguard pupils, staff, volunteers and governors online
- Deliver an effective whole-school approach to online safety
- Empower and educate the school community in safe technology use
- Establish clear mechanisms to identify, report, intervene and escalate concerns
- Protect school systems and data from misuse or security breaches
- Identify and support pupils who may be at greater risk of harm online

2. Legislation and Guidance

This policy is informed by:

- Keeping Children Safe in Education (KCSIE)
- Teaching Online Safety in Schools (DfE)
- Searching, Screening and Confiscation (DfE)
- UKCIS guidance on sharing nudes and semi-nudes
- Prevent Duty guidance
- Relationships and Health Education statutory guidance
- Education Act 1996 and 2011
- Equality Act 2010
- Data Protection legislation (GDPR and Data Protection Act 2018)

This policy should be read alongside:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Data Protection Policy
- Complaints Procedure

3. The Four Categories of Online Risk

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

Content

Exposure to illegal, inappropriate or harmful content, including pornography, racism, misogyny, extremism, self-harm, suicide content, fake news and radicalisation.

Contact

Harmful interaction with others online, including grooming, coercion, exploitation, peer pressure and adults posing as children.

Conduct

Online behaviour that causes or increases risk of harm, including cyber-bullying, harassment, sharing explicit images, and abusive behaviour.

Commerce

Online gambling, scams, phishing, inappropriate advertising and financial exploitation.

4. Roles and Responsibilities

4.1 Governing Board

The Governing Board will:

- Monitor implementation of this policy
- Ensure appropriate filtering and monitoring systems are in place
- Review filtering and monitoring provision at least annually
- Ensure online safety is embedded within safeguarding
- Receive regular reports on online safety incidents
- Ensure staff receive annual safeguarding and online safety training
- Ensure online safety education is adapted for vulnerable pupils and those with SEND
- Ensure an annual online safety risk assessment is completed

4.2 Headteacher

The Headteacher is responsible for:

- Ensuring consistent implementation of this policy
- Overseeing filtering and monitoring systems
- Authorising device searches
- Taking disciplinary action where appropriate

4.3 Designated Safeguarding Lead (DSL)

The DSL:

- Takes lead responsibility for online safety
- Manages and logs online safety incidents
- Oversees filtering and monitoring effectiveness
- Works with IT providers to maintain secure systems
- Delivers staff training and updates
- Reports regularly to SLT and governors
- Conducts annual online safety risk assessments
- Liaises with external agencies where necessary

4.4 Staff and Volunteers

All staff and volunteers must:

- Read, understand and implement this policy
- Model responsible digital behaviour
- Embed online safety within teaching
- Respond appropriately to reports of online harm
- Maintain professional conduct online
- Report safeguarding concerns immediately
- Understand that online abuse and peer-on-peer harm can occur

4.5 Parents and Carers

Parents/carers are expected to:

- Support the school's approach to online safety
- Encourage safe technology use at home
- Inform the school of online safety concerns

- Follow the Parent Code of Conduct
- Ensure children understand acceptable use expectations

5. Filtering and Monitoring

The school ensures:

- Harmful and inappropriate content is blocked
- Filtering does not unreasonably impact learning
- Monitoring systems meet safeguarding needs
- Systems are reviewed at least annually
- Clear roles are assigned for filtering oversight

The DSL works closely with IT providers to maintain effective safeguards.
Users should not expect privacy when using school systems.

6. Acceptable Use of School Systems

School systems are primarily for educational and professional purposes.
Users must not:

- Access illegal, harmful or inappropriate content
- Attempt to bypass filtering systems
- Install unauthorised software
- Share passwords
- Access others' accounts
- Use aggressive or discriminatory language
- Engage in gaming, gambling or shopping without permission

Monitoring may take place at any time.

7. Mobile Devices

7.1 Pupils

Pupil mobile phone use is governed by school rules. Devices must not be used during the school day unless explicitly permitted.

7.2 Personal Devices

Where personal devices are permitted:

- They are brought at the owner's risk
- The school accepts no liability for loss or damage
- Devices must be password protected
- Must remain on silent
- Must follow all school rules

8. Staff Use of Devices Outside School

Staff must:

- Use strong passwords (minimum 8 characters including upper/lower case, numbers and symbols)
- Ensure encryption of hard drives
- Enable automatic screen locking
- Install anti-virus protection
- Keep systems updated
- Not share work devices with family
- Store and transfer personal data securely

Work devices must be used solely for professional purposes.

9. Social Media

9.1 Official School Accounts

- Must be approved by SLT

- Must be monitored regularly
- Must be managed by at least two adults
- Must use professional tone
- Must respond to queries within 24 hours (or next working day)

9.2 Professional Conduct

Staff must:

- Maintain professional boundaries
- Not engage with pupils via personal accounts
- Not damage the school's reputation
- Not share confidential information
- Use disclaimers where appropriate

9.3 Parents and Pupils

Offensive or defamatory comments about the school will be addressed in line with behaviour or complaints procedures.

10. Cyber-Bullying

Cyber-bullying is repetitive, intentional harm carried out via electronic communication.
It may include:

- Threatening messages
- Sharing images without consent
- Impersonation
- Exclusion
- Harassment

The school will:

- Educate pupils about prevention
- Log incidents
- Follow safeguarding and behaviour procedures
- Involve police where necessary

11. Searching, Screening and Confiscation

The Headteacher or authorised staff may search and confiscate electronic devices where there are reasonable grounds to suspect:

- A safeguarding risk
- Presence of inappropriate or illegal material
- Evidence of an offence

If indecent images of a child are suspected:

- Staff will not view the image
- The device will be confiscated
- The DSL will be informed immediately
- Police involvement will be considered

All searches follow DfE guidance.

12. Artificial Intelligence (AI)

AI tools are increasingly accessible.
Risks include:

- Deepfake images
- AI-generated bullying
- Misinformation
- Academic dishonesty

The school will:

- Educate pupils about responsible AI use
- Risk assess AI tools before implementation

- Treat AI misuse in line with behaviour policy

13. Online Safety Education

Online safety is taught through:

- Computing curriculum
- PSHE
- Relationships and Health Education
- Safeguarding curriculum

Pupils are taught to:

- Keep personal information private
- Recognise and report risks
- Critically evaluate online content
- Understand respectful online behaviour

Teaching is adapted for vulnerable pupils and those with SEND.

14. Safeguarding Vulnerable Pupils

We recognise that some pupils are more vulnerable online.
Online safety teaching and intervention will be personalised where necessary.

15. Reporting and Responding to Concerns

All concerns must be reported immediately to the DSL.
The school will:

- Log incidents formally
- Assess risk
- Take proportionate action
- Inform parents where appropriate
- Involve external agencies where required

Illegal content will be reported to police.

16. Incident Logging

All online safety incidents are:

- Recorded formally
- Reviewed for patterns or trends
- Reported to SLT and governors as appropriate

17. Training

All staff:

- Receive online safety training at induction
- Receive annual safeguarding updates
- Receive regular updates throughout the year

DSL training includes enhanced online safety training at least every two years.
Governors receive safeguarding and online safety training.

18. Annual Risk Assessment

An annual online safety risk assessment will consider:

- Emerging technologies
- AI developments
- Incident trends
- Filtering effectiveness
- Pupil voice

This ensures the policy remains current.

19. Breaches of Policy

Failure to comply may result in:

- Withdrawal of access
- Behaviour sanctions
- Disciplinary procedures
- Referral to Governors or Local Authority
- Police involvement where necessary

The school may act where out-of-school online behaviour impacts the school community.

20. Agreement

Access to school systems is conditional upon agreement to this policy.

Separate signature agreements may be issued for:

- Staff and volunteers
- Parents/carers
- Pupils (age-appropriate versions)