Fairfield Primary School

Online Safety Policy

Created/Revised:	February 2026/ September 2026
By:	N Steel
Review Details:	Updates Annually
Review Date:	September 2026
Next Review:	September 2027
Approved by Governing Body:	September 2026

Fairfield Primary School Online Safety Policy

1. Introduction and Aims

Fairfield Primary School recognises that technology plays an essential role in children's education, communication and social development. The school is committed to ensuring that all pupils, staff, governors, volunteers and visitors use digital technologies safely, responsibly and respectfully.

This policy supports statutory safeguarding responsibilities outlined in:

- Keeping Children Safe in Education (KCSIE)
- The Education Act 2002 (safeguarding duties)
- UK GDPR and Data Protection Act 2018
- Prevent Duty guidance
- DfE cyber-security standards for schools
- DfE "Teaching Online Safety in Schools" guidance

Online safety is considered a safeguarding issue, and concerns will be treated in line with the school Child Protection and Safeguarding Policy.

2. Scope of Policy

This policy applies to:

- Pupils
- Staff and supply staff
- Governors and volunteers
- Parents and carers (where school systems are used)
- All school digital infrastructure and personal devices used on site

It covers:

- School IT systems and devices
- Remote learning platforms
- Social media use
- Personal devices in school
- Data security and cyber-security
- Online behaviour inside and outside school where safeguarding risks arise

3. Roles and Responsibilities

Governing Body

The governing body will:

- Ensure effective safeguarding including online safety
- Monitor implementation of filtering, monitoring and cyber-security measures
- Ensure staff training is regularly reviewed

Schools are expected to ensure appropriate filtering and monitoring systems are in place and regularly reviewed as part of safeguarding responsibilities.

Headteacher

The headteacher will:

- Ensure this policy is implemented
- Ensure safeguarding procedures include online safety
- Support staff training and compliance
- Ensure safe curriculum delivery

Designated Safeguarding Lead (DSL)

The DSL will:

- Take lead responsibility for online safety safeguarding issues
- Understand filtering/monitoring systems and risks
- Manage online safety incidents
- Liaise with external agencies where needed

KCSIE requires DSLs to understand filtering and monitoring arrangements and staff training responsibilities.

IT / Network Manager (OneIT)

Responsible for:

- Network security
- Filtering and monitoring
- Cyber-security compliance
- Incident response

- Regular system reviews

All Staff

Staff must:

- Model safe online behaviour
- Follow acceptable use policies
- Report safeguarding concerns immediately
- Undertake annual online safety and cyber-security training

Cyber-security standards emphasise staff training, password security and reporting incidents.

4. Education and Curriculum

Online safety is embedded within:

- Computing curriculum
- PSHE / RSHE
- Relationships education
- Safeguarding education

DfE guidance emphasises equipping pupils with knowledge to use the internet safely as part of the wider curriculum.

Teaching will address risks grouped under the 4Cs framework:

- Content
- Contact
- Conduct
- Commerce

These categories are widely used within safeguarding guidance. The school recognises that pupils increasingly encounter artificial intelligence (AI) technologies, including generative AI tools. Pupils will be taught to critically evaluate online content, including AI-generated content, misinformation, disinformation and manipulated media. Staff and pupils are expected to comply with the school's AI Policy, which sets out expectations for the safe, ethical and responsible use of AI technologies.

5. Acceptable Use of Technology

The school maintains Acceptable Use Agreements (AUAs) for:

- Staff
- Pupils
- Visitors

These cover:

- Responsible internet use
- Communication standards
- Data protection
- Device security

Cyber standards recommend having an acceptable use policy shared annually with all users.

6. Filtering, Monitoring and Security

The school ensures:

- Age-appropriate filtering systems
- Active monitoring for safeguarding risks
- Regular effectiveness reviews
- Appropriate balance to support learning

Schools must do “all that they reasonably can” to limit exposure to harmful online risks through filtering and monitoring systems.

Additional security measures include:

- Secure passwords and authentication
- Secure storage of devices
- Data protection compliance
- Incident reporting procedures

Filtering and monitoring arrangements are reviewed regularly to ensure they remain effective, proportionate and appropriate to the safeguarding needs of the school. The Governing Body receives assurance regarding the effectiveness of filtering and monitoring systems in line with statutory guidance.

7. Remote Learning and Online Communication

Where remote education occurs:

- Staff communicate only through approved platforms
- School accounts must be used
- Personal contact details must not be shared
- Parents are informed of platforms used

Safeguarding procedures must remain consistent during remote learning.

8. Social Media

Staff:

- Must not contact pupils via personal social media
- Must maintain professional boundaries
- Should follow the staff code of conduct

Pupils:

- Are taught responsible digital citizenship
- Should report online concerns promptly

9. Mobile Phones and Personal Devices

Fairfield Primary School:

- Restricts pupil mobile phone use on site
- Requires secure storage where permitted
- Provides guidance for staff device use

10. Data Protection and Privacy

The school complies with:

- UK GDPR
- Data Protection Act 2018

This includes:

- Secure handling of personal data
- Parental consent where appropriate
- Secure online consent systems

11. Reporting Concerns

All online safety concerns should be reported immediately to:

- DSL or Deputy DSL
- Senior leadership team

Concerns may include:

• Cyberbullying
• Grooming risks
• Inappropriate content exposure
• Data breaches
• Radicalisation concerns
• Online sexual harassment
• Sharing of nude or semi-nude images

Clear reporting routes must exist for pupils, staff and parents. Concerns involving the sharing of nude or semi-nude images will be managed in accordance with current UKCIS guidance and the school's safeguarding procedures.

12. Working with Parents and Carers

The school will:

- Provide guidance on online safety
- Signpost support resources
- Encourage parental supervision
- Share advice on parental controls

Parents should understand safe online environments and supervise age-appropriate internet use.

13. Staff Training

Training will include:

- Safeguarding updates
- Cyber-security awareness
- Filtering/monitoring awareness

- Data protection

Staff should receive regular training aligned with national cyber-security expectations.

14. Monitoring, Review and Evaluation

This policy will be:

- Reviewed annually
- Updated in line with statutory guidance
- Evaluated through safeguarding audits

15. Links to Other Policies

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Staff Code of Conduct
- Data Protection Policy
- Remote Learning Policy
- ICT Acceptable Use Policy
- AI Policy