



# Fulbrook

## Online Safety Policy

<b>Issue No.</b>	<b>Author or Reviewer</b>	<b>Date Written or Reviewed</b>	<b>Date Approved by FES/PEAP</b>	<b>Date Approved by FGB</b>	<b>Next Review Date</b>
2	Deputy Head Teacher	March 2026		March 2026	March 2027

# Contents

- 1. Policy Statement ..... 3
- 2. Legislative and Statutory Guidance ..... 3
- 3. Scope..... 4
- 4. Roles and Responsibilities ..... 4
- 5. Filtering and Monitoring..... 7
- 6. Online Safety Education ..... 8
- 7. Use of Digital Technologies ..... 8
- 8. Social Media ..... 9
- 9. Remote Learning..... 9
- 10. Online Safety Incident Reporting..... 9
- 11. Data Protection..... 10
- 12. Monitoring and Review ..... 10
- Appendix A..... 11
- Appendix B ..... 11
- Appendix C ..... 11

# 1. Policy Statement

This Online Safety Policy sets out how Fulbrook school ensures the safe and responsible use of digital technologies by students, staff, governors, visitors and the wider school community.

The school recognises that digital technology plays a critical role in education, communication and everyday life. While the internet and digital services offer significant educational benefits, they also present safeguarding risks.

Online safety is therefore recognised as a core element of safeguarding and child protection.

Fulbrook school is committed to:

- protecting students from harm when using technology
- educating students to use technology safely and responsibly
- ensuring staff understand their safeguarding responsibilities
- implementing effective technical safeguarding measures

Online safety is embedded within the school's safeguarding culture and procedures.

# 2. Legislative and Statutory Guidance

This policy has been developed in accordance with relevant legislation and statutory guidance including:

- Keeping Children Safe in Education (KCSIE)
- Working Together to Safeguard Children
- Teaching Online Safety in Schools (DfE)
- DfE Filtering and Monitoring Standards for Schools and Colleges
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Education Act 2002 • The Prevent Duty

This policy should be read alongside the following school policies:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy

- Staff Code of Conduct
- Data Protection Policy
- Acceptable Use Agreements

### 3. Scope

Online safety encompasses the use of:

- Internet access
- Email systems
- Social media
- Online communication platforms
- Online learning platforms
- Mobile phones and personal devices
- Tablets, laptops and computers
- Gaming and interactive platforms
- Cloud-based services

The policy applies to technology used:

- on school premises
- during school activities off-site
- during remote learning
- when technology use impacts on the school or students

### 4. Roles and Responsibilities

#### Governing Body

The Governing Body is responsible for ensuring effective safeguarding arrangements including online safety.

The governing body will:

- ensure the school has an effective online safety policy
- review safeguarding including online safety annually
- ensure appropriate filtering and monitoring systems are in place
- receive safeguarding reports from the DSL
- ensure staff receive appropriate safeguarding training

A safeguarding governor will oversee safeguarding including online safety.

## Headteacher

The Head Teacher has overall responsibility for online safety.

The Head Teacher will ensure:

- online safety policies are implemented
- appropriate staff training takes place
- safeguarding incidents are managed effectively
- filtering and monitoring systems are effective

## Designated Safeguarding Lead (DSL)

The DSL has lead responsibility for safeguarding including online safety.

Responsibilities include:

- managing online safety incidents
- maintaining safeguarding records
- liaising with external safeguarding partners
- supporting staff with safeguarding concerns
- monitoring emerging online risks

## Online Safety Lead

Where appointed, the Online Safety Lead supports the DSL and manages day-to-day online safety arrangements.

Responsibilities include:

- monitoring developments in online safety
- supporting staff and students
- coordinating training and awareness
- reviewing filtering and monitoring effectiveness

## IT and Technical Staff

Technical staff maintain the security of school systems.

This includes:

- maintaining secure infrastructure
- implementing filtering and monitoring systems
- ensuring regular security updates
- maintaining antivirus and malware protection
- supporting safeguarding investigations where required

## Staff

All staff have a safeguarding responsibility.

Staff must:

- follow this policy and acceptable use agreements
- report concerns immediately to the DSL
- model safe technology use
- supervise students when using technology (via the use of Classroom Cloud monitoring system)

## Students

Students must use technology responsibly and follow the student acceptable use agreement.

Students will be taught how to:

- stay safe online
- protect personal information
- recognise online risks
- report concerns

## Parents and Carers

Parents and carers play an important role in supporting online safety.

The school will:

- provide guidance and advice
- share information on emerging risks
- work with parents when concerns arise

## 5. Filtering and Monitoring

The school implements appropriate filtering and monitoring systems in line with Department for Education standards.

These systems aim to:

- prevent access to illegal or harmful content
- identify safeguarding concerns
- protect students while enabling educational access

Filtering and monitoring arrangements are regularly reviewed by:

- the DSL
- school leadership

- technical staff

Safeguarding concerns identified through monitoring will be reported to the DSL immediately.

The school's filtering provider is: LGFL

The school's monitoring system provider is: Classroom Cloud

## 6. Online Safety Education

Online safety education is embedded within the curriculum, particularly within Computing, PSHE and Relationships Education.

Students are taught about:

- online relationships
- online bullying
- online reputation
- managing online information
- privacy and security
- copyright and ownership

Staff receive regular safeguarding and online safety training.

## 7. Use of Digital Technologies

Use of school technology is a privilege and must be conducted responsibly.

Users must:

- use systems for educational or professional purposes
- protect personal data
- respect copyright laws
- communicate respectfully online

Personal devices must only be used in accordance with school policies.

## 8. Social Media

The school may use social media platforms for communication with the school community.

Official accounts are managed only by authorised staff.

Staff must not communicate with students through personal social media accounts.

Images of students may only be shared where parental consent has been obtained. Any reference to students should be forename only.

## 9. Remote Learning

Where remote learning is used, staff must use approved platforms and school accounts.

Online lessons and meetings must:

- maintain professional standards
- protect student privacy
- follow safeguarding procedures

## 10. Online Safety Incident Reporting

All online safety incidents must be reported immediately to the Designated Safeguarding Lead.

Examples include:

- cyberbullying
- online grooming
- accessing inappropriate content
- sharing personal information
- extremist or illegal content

All incidents will be recorded in the school's safeguarding recording system, MyConcern.

Where appropriate the school may involve:

- local authority safeguarding teams
- police
- other appropriate safeguarding agencies

## 11. Data Protection

All personal data must be handled in accordance with:

- Data Protection Act 2018
- UK GDPR

Staff must ensure:

- data is stored securely
- only authorised individuals access data
- confidential information is protected

## 12. Monitoring and Review

This policy will be reviewed annually or sooner if required due to:

- changes in legislation
- new safeguarding risks
- technological developments

The governing body will receive updates on online safety arrangements.

## Appendix A

### Staff Acceptable Use Agreement

Staff must:

- use school ICT systems responsibly
- maintain professional boundaries online
- protect confidential information
- report safeguarding concerns

Failure to follow the agreement may result in disciplinary action.

---

## Appendix B

### Student Acceptable Use Agreement

Students agree to:

- use the internet safely
  - treat others respectfully online
  - protect personal information
  - report anything that makes them feel unsafe
- 

## Appendix C

### Online Safety Incident Flowchart

1. Concern identified by staff or student
2. Report immediately to Designated Safeguarding Lead
3. DSL assesses safeguarding risk
4. Incident recorded in safeguarding system, MyConcern
5. Appropriate action taken:

- pastoral support
  - behaviour procedures
  - safeguarding referral/CEOP referral
  - police involvement if required
6. Parents informed where appropriate
  7. Incident reviewed to inform future prevention