



Online Safety Policy

December 2025

Approved by:	FGB
Date:	December 2025
Review due:	December 2027 or earlier if guidance changes

Introduction

Great Steeping Primary School is committed to safeguarding pupils in both the physical and digital environments. This policy outlines our approach to online safety, including the safe use of technology, social media, and digital communication, and aligns with our Anti-Bullying and GDPR policies.

Scope

This policy applies to:

- Pupils, staff, governors, volunteers, and contractors
- Use of school and personal devices
- Internet, email, social media, and remote learning platforms

Leadership and Governance

- **Online Safety Leader:** Miss Emma Dunkin
- **Named Governor for Online Safety:** Allison Sunley

The governing body ensures this policy is reviewed regularly and remains responsive to emerging risks. The headteacher oversees implementation and ensures incidents are addressed promptly.

Roles and Responsibilities

Headteacher

- Ensures staff training is current and appropriate
- Oversees incident management

Online Safety Leader

- Maintains awareness of emerging risks
- Leads risk assessments and liaises with external agencies
- Engages with parents and the wider community

IT Technical Support

- Maintains antivirus and filtering systems
- Ensures secure password protocols
- Updates operating systems and monitors device security

All Staff

- Understand and follow this policy
- Report concerns to the Online Safety Leader or Headteacher

Risk Management

A live risk assessment is maintained and shared with staff and IT support. Risks include:

- Access to inappropriate content
- Data breaches
- Online bullying and exploitation
- Device theft or misuse

Safeguarding and Extremism

We actively monitor for signs of:

- Exposure to extremist content
- Peer-on-peer sexual abuse and harassment
- Harmful sexual behaviour online
- Mental health concerns linked to online activity

Staff are trained to identify and respond to these risks, and referrals are made to appropriate authorities when necessary.

Online Safety Education

Pupils are taught:

- Responsible internet use
- Cyberbullying awareness

- Copyright and data protection
- Safe social media behaviour

Staff will receive yearly training on the filtering and monitoring systems in school, unless there are significant changes to any of these systems in between these times. New members of staff will have initial training with IT support as part of their induction. Staff receive annual training on online safety.

Social Media Use

Staff

- Must not befriend pupils or ex-pupils under 18
- Should not post about the school unless sharing official content
- Must not identify themselves as school staff without authorisation

Pupils

- Must not access social media in school unless directed by a teacher
- Inappropriate comments or behaviour will be reported and may result in disciplinary action

Parents

- Must not use social media during school visits
- Must not post images or comments that breach GDPR or school policy

Acceptable Use

- Pupils are supervised online and taught safe practices
- Filtering and monitoring systems are in place at router level
- Personal storage devices require permission and encryption
- Multi-factor authentication is used by all staff
- Passwords must be kept secure and not shared

Device Use

- Staff iPads are password-protected and erased after failed attempts

- Pupil iPads are filtered and monitored via a Fortigate appliance in school
- Mobile phones must be silent and out of sight during school hours
- KS2 pupils may bring phones if walking alone, but must store them securely

Email and Communication

- Only approved email and Teams accounts may be used
- Communication must remain professional
- Pupils must not arrange meetings with online contacts

Examining Electronic Devices

Authorised staff may search and examine devices if:

- There is a risk to safety
- A school rule has been broken
- The device may contain evidence of an offence

Data may be erased if it poses harm or disrupts the school environment.

Monitoring and Filtering

We use a two-level filtering/monitoring system:

- Router-level filtering
- Log360 internet monitoring

This applies to any device on the school network, including visitor/staff personal devices.

Filtering is stricter for pupils than staff and is reviewed regularly.

Reporting and Response

If you have any queries, or wish to escalate a concern, you can contact:

- Online Safety Leader: Miss Emma Dunkin
- Named Governor for Online Safety: Allison Sunley
- IT Technician: Josh Carlton

Infotechdirect Ltd

07540667382

Josh.Carlton@infotechdirect.co.uk

All concerns are reported to the DSL / DDSL and investigated in line with the Child Protection and Safeguarding Policy. This includes incidents occurring off-site or on personal devices.

Review and Evaluation

This policy is reviewed every two years or following a significant incident. Feedback from staff, pupils, and parents informs updates.