Woodloes Primary School

Online Safety Policy

Written by	S Byrne
Date	Autumn 2025
Date adopted by Governors	Autumn 2025
Date for policy renewal	Autumn 2026

This Online Safety Policy sets out a comprehensive policy for ensuring the safety of all members of the school community in their use of digital technologies. It aligns with statutory guidance from the Department for Education, including *Keeping Children Safe in Education* (KCSIE, 2024), and supports inspection requirements under the Ofsted *Education Inspection Framework* (EIF, 2023). It reflects the principles of the *UKCIS Education for a Connected World* framework and incorporates responsibilities and mechanisms for creating a safe digital environment in school.

1. Policy Statement and Purpose

1.1 Introduction

This policy recognises the commitment of Woodloes Primary School to safeguarding and promoting the welfare of children and young people. Online safety, also referred to as e-safety, forms an integral part of our safeguarding and child protection responsibilities.

The purpose of this policy is to:

- Protect pupils from risks and harm in an increasingly digital world.
- Provide clear expectations for safe and responsible use of technology.
- Define measures to educate, train and safeguard staff, pupils and families.

This policy should be read in conjunction with the school's Safeguarding and Child Protection Policy.

1.2 Aims and Objectives

The aims of this policy are to:

- Promote safe and responsible use of the internet and digital technologies.
- Ensure that pupils, staff, parents and carers understand the risks associated with digital activity.
- Outline procedures for preventing, identifying and responding to online safety incidents.
- Comply with statutory safeguarding responsibilities set out in KCSIE.

1.3 Scope

This policy applies to all members of the school community, including:

- Pupils
- Staff
- Volunteers
- Governors
- Visitors

It covers:

- Use of school-provided and personally owned devices used on school premises.
- All school-based and remote/online learning activities.
- Digital communications involving members of the school community.

2. Legislative and Statutory Framework

2.1 Key Legislation

This policy is underpinned by the following legislation and guidance:

- *Children Act 1989 & 2004*
- *Education Act 2002*
- *Keeping Children Safe in Education* (DfE, 2025)
- *The Prevent Duty* (DfE, 2015)
- *Data Protection Act 2018 / UK GDPR*
- *Human Rights Act 1998*
- *Communications Act 2003*
- *Malicious Communications Act 1988*
- *Equality Act 2010*
- *Online Safety Act* (when in force)
- *Working Together to Improve School Attendance* (DfE, 2024) – now statutory as referenced in *KCSIE 2025.*

2.2 Guidance and Frameworks

This policy supports the following guidance:

- *Keeping Children Safe in Education (DfE, 2025)*
- *Teaching Online Safety in Schools (DfE, 2019)*
- *Education for a Connected World framework (UKCIS, 2020)*
- *Searching, Screening and Confiscation (DfE, 2022)*
- *Guidance on managing sexual violence and harassment (as outlined in KCSIE 2025 Part Five)*
- *Ofsted Education Inspection Framework (EIF, 2023)*

3. Roles and Responsibilities

3.1 School Standards Committee (SSC)

The SSC is responsible for:

- Ensuring the online safety policy is reviewed annually and is compliant with current legislation and guidance.
- Holding school leaders to account for effective implementation of online safety education and measures.
- Ensuring the school has appropriate filtering and monitoring systems (KCSIE, 2025).

3.2 Headteacher

The Headteacher is responsible for:

- Leading a whole-school approach to online safety.
- Ensuring staff training is undertaken and curriculum provision is in place.
- Supporting the Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Leads (DDSL) in handling incidents related to online safety.
- Reporting concerns to the SSC and external agencies when necessary.

3.3 Designated Safeguarding Lead (DSL)

The DSL holds responsibility for:

- Leading and coordinating the school's safeguarding responses to online concerns.
- Keeping up to date with trends and threats in online safety and disseminating information to staff.
- Liaising with external agencies, including the police or children's social care, for serious incidents.
- Maintaining an overview of online safety education and risk assessments.

3.4 Staff

All staff must:

- Read and understand the online safety policy and Staff Acceptable Use Agreement.
- Model safe online behaviour and respond immediately to concerns.

- Teach and support pupils to develop safe online practices.
- Report all safeguarding and online concerns to the DSL/DDSL.

3.5 Pupils

Pupils are expected to:

- Understand and follow the school's Pupil Acceptable Use Agreement.
- Use digital technologies safely, responsibly and respectfully.
- Report online concerns to a trusted adult.

3.6 Parents and Carers

Parents and carers should:

- Work in partnership with the school to reinforce safe online behaviour at home.
- Engage with online safety information shared by the school.
- Model appropriate online conduct and support the school's digital rules.

4. Education and Training

4.1 Online Safety Education for Pupils

Our curriculum is informed by the *Education for a Connected World* framework and includes:

- Age-appropriate learning about privacy, online relationships, cyberbullying, fake news, password safety, image sharing, online reputation and more.
- Pupils are also taught to recognise and critically evaluate misinformation, disinformation and conspiracy theories, reflecting the expanded "content risk" categories set out in *Keeping Children Safe in Education (2025)*. Lessons include recognising credible information sources, understanding how false content spreads, and knowing how to report harmful or misleading material.
- Opportunities to reflect on the impact of digital life on mental health and wellbeing.
- Regular updates and safety messages through PSHE, assemblies and enrichment activities such as Safer Internet Day.

4.2 Staff Training

All staff receive:

- Annual safeguarding and child protection training, which includes online safety elements.

- Regular updates via briefings or Professional Development Days on emerging risks and school procedures.
- Specific CPD for staff with wider responsibilities, such as Computing Leads or pastoral leads.

Training includes awareness of emerging technologies such as generative AI and the associated safeguarding considerations highlighted in KCSIE (2025).

4.3 Parent/Carer Support and Engagement

To build the capacity of our parent community, we:

- Share newsletters, website updates and guidance materials to support digital parenting.
- Host parent events and workshops linked to online safety issues.
- Share referrals to services such as CEOP, NSPCC, ThinkUKnow, Internet Matters and UK Safer Internet Centre.

5. Acceptable Use Policies

5.1 Staff Acceptable Use Agreement

Staff Acceptable Use Agreement covers:

- Expectations for professional use of digital tools and platforms.
- Appropriate conduct on social media and electronic communication.
- Data protection, device use and safeguarding responsibilities.

5.2 SSC/Visitors

All governors, volunteers and visitors who access school systems must agree to basic terms covering:

- Restricted access to pupil data and systems.
- No unauthorised use of photos, videos or recording equipment.
- Proper conduct when using network/wireless systems.

6. Technology and Filtering

6.1 Infrastructure and Filtering

The school ensures:

- Age-appropriate, robust web filtering and monitoring systems are in place to block harmful or inappropriate content.
- Regular audits of the filtering system.
- Monitoring logs are reviewed regularly by the DSL

- Systems meet the expectations set out in *KCSIE (2025)* and guidance from the UK Safer Internet Centre (2025 updates).

Filtering and monitoring systems are reviewed regularly to ensure they meet the expectations outlined in *KCSIE (2025)*. The school also considers the Department for Education's *Generative AI: Product Safety Expectations (2025)* when assessing emerging technologies, ensuring that any use of artificial intelligence or adaptive software is appropriately risk-assessed and monitored to safeguard pupils.

6.2 Device Security and Management

All school devices:

- Are password protected and only contain authorised software.
- Have up-to-date security including antivirus protection.
- Are managed securely through an inventory and appropriate remote management tools.

Remote learning platforms are secure and user access is managed centrally.

7. Monitoring and Responding to Incidents

7.1 Recognising Online Safety Concerns

Online safety concerns may include:

- Cyberbullying and online harassment.
- Exposure to harmful content (e.g. extremist, pornographic or violent material).
- Grooming or sexual exploitation.
- Sexting (youth-produced sexual images).
- Identity theft or financial scams.

Staff are trained to identify early warning signs and report concerns promptly.

7.2 Reporting Systems

We ensure:

- Clear routes are available for pupils to report anything they see or experience online.
- Concerns are recorded on our safeguarding log and reviewed by the DSL.
- Anonymous reporting routes can be used where needed.

All staff are aware of how to escalate concerns through safeguarding procedures.

7.3 Incident Management

On discovery of an incident, the following steps are taken:

- Report to DSL/DDSL immediately.
- DSL/DDSL assesses the incident and takes safeguarding action, including external referrals if necessary.
- School supports any affected pupils and involves parents.
- Where appropriate, devices may be confiscated, and police informed.

8. Remote Learning and Online Communication

8.1 Remote Learning Platforms

Our chosen platforms (e.g. Microsoft Teams) are:

- Secure, monitored and used in line with our Remote Learning Policy.
- Accessed only by school-approved accounts.
- Guided by e-safety charters for use by staff and pupils.

8.2 Live Streaming and Video Conferencing

Where staff conduct virtual lessons:

- Staff and pupils adhere to agreed protocols for safe lessons.
- Cameras may be on or off based on guidance.
- Lessons are monitored or recorded to ensure professional practice.

8.3 Communication with Pupils and Parents

Staff must:

- Only use school-provided email addresses and communication platforms.
- Never communicate with pupils through personal devices or accounts.
- Keep professional boundaries at all times.

Parents are informed of expectations and contacts used by the school.

9. Mobile and Smart Technologies

9.1 Mobile Phones

The use of mobile phones:

- Pupils must not use mobile phones during the school day
- Staff mobile phone use is restricted to non-contact times and must follow the Code of Conduct.
- Misuse will result in confiscation and parental contact.

9.2 Wearable and Smart Devices

Wearables and internet-connected devices such as smart watches must:

- Not be used to access content or recording features during the school day.
- Be used in line with school policy to protect privacy and learning.

10. Social Media

10.1 Use by Pupils

Pupils are taught:

- To critically evaluate information shared on social media.
- About privacy settings, blocking/reporting, and safe interaction.
- That using social media to harm others (e.g. name-calling or sexting) is a serious offence.

10.2 Use by Staff and SSC

Staff and SSC:

- Must maintain professional standards and not interact on social media with current pupils.
- Should use privacy settings and exercise caution when posting.
- Must not bring the school into disrepute through online actions.

10.3 Use by the School

We use social media for communication and celebration in line with our social media strategy:

- Accounts are managed by designated staff and access is restricted.
- Photos or content are shared with explicit consent.
- School avoids using identifiable names alongside pupil photographs.

11. Data Protection and Privacy

11.1 Data Collection and Storage

Through adherence to the Data Protection Policy, we ensure:

- Only necessary data is collected and retained in compliance with UK GDPR.
- Security protocols are in place for storing and transferring data.
- Staff are trained in data protection obligations.

11.2 Pupil Privacy

We protect pupil privacy by:

- Requiring parent/carer consent for images or videos to be shared publicly.
- Encouraging children to consider their digital footprint.
- Ensuring that pupils understand the risks of oversharing online.

12. Policy Review and Evaluation

12.1 Review Cycle

Reviews will also take account of updates to national guidance, including *KCSIE (2025)* and any subsequent DfE publications relating to online safety, filtering, monitoring or the use of artificial intelligence in schools.

12.2 Evaluation

The policy will be evaluated through:

- Audits of filtering/monitoring logs.
- Pupil and staff voice.
- Incident data tracking and lessons learned.
- SSC meetings.

---

13. Related Policies

This policy should be read alongside the following:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Data Protection Policy
- PSHE and RSHE Curriculum Policy
- Remote Learning Policy

References

- Department for Education (2025). *Keeping Children Safe in Education.*
- Department for Education (2019). *Teaching Online Safety in Schools.*
- UK Council for Internet Safety (UKCIS) (2020). *Education for a Connected World Framework.*

- Department for Education (2022). *Searching, Screening and Confiscation.*
- Department for Education (2024). *Working Together to Improve School Attendance.*
- Department for Education (2015). *The Prevent Duty.*
- Ofsted (2023). *Education Inspection Framework.*
- Department for Education (2025). *Generative AI: Product Safety Expectations for Education Settings.*

This document represents Woodloes Primary School's commitment to the safety and wellbeing of all pupils in an increasingly digital environment.