Oldswinford C.E. Primary School

Online Safety Policy

Believe, Achieve and Shine Brighter Together

Written: Sept 2026

Approved by Governors:

1. Introduction

The DfE's Keeping Children Safe in Education (KCSIE) requires schools to ensure that children are safeguarded from potentially harmful and inappropriate online material. An effective whole-school approach to online safety empowers a school to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

KCSIE requires that online safety is a running and interrelated theme whilst devising and implementing the school's whole-school approach to safeguarding. This includes considering how online safety is reflected in all relevant policies, the curriculum, staff training, the roles and responsibilities of the designated safeguarding lead, and parental engagement.

KCSIE recognises four categories of online risk:

- **Content:** being exposed to illegal, inappropriate, or harmful content, including pornography, fake news, misinformation, disinformation, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact:** being subjected to harmful online interaction with other users, including peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial, or other purposes.
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm, including making, sending, and receiving explicit images (consensual and non-consensual sharing of nudes and semi-nudes), sharing explicit images, and online bullying.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing, and financial scams.

This policy outlines the school's commitment to safeguarding its community online, setting out the roles, responsibilities, and procedures that ensure a safe digital environment for all.

2. Purpose

This policy aims to:

- Safeguard all members of the school community from online harm.
- Ensure the school meets its statutory obligations under KCSIE, the DfE's Digital and Technology Standards, and other relevant legislation.
- Establish clear roles, responsibilities, and reporting procedures for online safety.
- Provide a framework for educating pupils about safe and responsible online behaviour.
- Ensure effective filtering and monitoring systems are in place.
- Support parents and carers in keeping children safe online.

3. Scope

This policy applies to all members of the school community, including staff, pupils, governors, volunteers, parents and carers, visitors, and community users who have access to and are users of school digital systems, both in and out of school. It also applies to the use of personal digital technology on the school site where permitted.

The school will address online safety incidents that occur outside school where they affect members of the school community, in accordance with the behaviour policy and anti-bullying policy.

4. Legal and Regulatory Framework

Legislation

- Children Act 2004 (Section 175, Education Act 2002)
- Data Protection Act 2018 and UK GDPR
- Education Act 2011
- Online Safety Act 2023
- Counter-Terrorism and Security Act 2015 (Prevent Duty)
- Equality Act 2010
- Computer Misuse Act 1990
- Sexual Offences Act 2003
- Voyeurism (Offences) Act 2019
- Malicious Communications Act 1988
- Communications Act 2003 (Section 127)
- Protection from Harassment Act 1997

Statutory and Non-Statutory Guidance

- DfE 'Keeping Children Safe in Education'
- DfE 'Working Together to Safeguard Children'
- DfE 'Meeting Digital and Technology Standards in Schools and Colleges'
- DfE 'Generative Artificial Intelligence (AI) in Education'
- DfE 'Mobile Phones in Schools'
- DfE 'Searching, Screening and Confiscation'
- UK Safer Internet Centre 'Appropriate Filtering and Monitoring Definitions' (2025)
- ICO Age Appropriate Design Code (Children's Code)
- UKCIS 'Sharing Nudes and Semi-Nudes: Advice for Education Settings'
- UKCIS 'Education for a Connected World' Framework

Related School Policies

- Child Protection and Safeguarding Policy
- Behaviour Policy and Anti-Bullying Policy
- Cyber Security Policy
- Filtering and Monitoring Policy
- Artificial Intelligence Policy
- Social Media and Mobile Technologies Policy
- Electronic Devices: Searching, Screening and Confiscation Policy
- Data Protection Policy
- Mobile Phone Policy
- Acceptable Use Agreements (staff and pupils)
- Staff Code of Conduct

- PSHE / RSE Curriculum Policy

5. Policy Development and Review

Item	Detail
Policy approved by:	Governing Body
Date approved:	
Implementation monitored by:	Headteacher
Monitoring frequency:	At least once per year
Governor reports frequency:	At least once per year
Next review date:	Sept 2027 or earlier if needed.
External support agencies:	Local Authority safeguarding team, police, CEOP, network provider

This policy will be reviewed annually, or more frequently in light of significant technological developments, new threats, changes to legislation or guidance, or following a serious online safety incident. The review will be informed by:

- Logs of reported online safety incidents.
- Filtering and monitoring reports.
- Internal network activity monitoring data.
- Feedback from pupils, parents and carers, and staff (e.g. through surveys).
- Outcomes of the annual filtering and monitoring review.
- The school's annual online safety risk assessment.

6. Roles and Responsibilities

6.1 Headteacher and Senior Leaders

- The headteacher has overall duty of care for ensuring the safety, including online safety, of all members of the school community, fostering a culture of safeguarding.
- Day-to-day responsibility for online safety is held by the Designated Safeguarding Lead (DSL) as defined in KCSIE.
- Senior leaders must be aware of procedures for handling serious online safety allegations against staff.
- Senior leaders are responsible for ensuring the DSL, Online Safety Lead receive suitable training.
- Senior leaders will receive regular monitoring reports from the DSL.
- Senior leaders will work with the responsible governor, the DSL, and the IT provider on all aspects of filtering and monitoring.

6.2 Governing Body

KCSIE states that governing bodies should ensure there are appropriate policies and procedures in place to safeguard and promote children's welfare, including online safety. Governors are responsible for:

- Approval of this policy and review of its effectiveness.
- Appointing a governor with specific responsibility for online safety.
- Receiving regular, anonymised reports of online safety incidents.
- Ensuring the filtering and monitoring provision is reviewed and recorded at least annually, involving the SLT, DSL, IT provider, and the responsible governor, in line with the DfE Filtering and Monitoring Standards.
- Receiving cyber security training to enable oversight of the school's compliance with the DfE Cyber Security Standards.
- Supporting the school in engaging parents and the wider community in online safety.

6.3 Designated Safeguarding Lead (DSL)

KCSIE states that the DSL should take lead responsibility for safeguarding and child protection, including online safety, and understanding the filtering and monitoring systems in place. The DSL will:

- Hold lead responsibility for online safety within their safeguarding role.
- Receive regularly updated training on online safety risks, including AI-related risks.
- Meet regularly with the online safety governor to review incidents and filtering/monitoring logs.
- Attend relevant governing body meetings.
- Receive and handle reports of online safety incidents, making referrals to relevant agencies and ensuring all incidents are recorded.
- Liaise with the IT provider on matters of online safety and safeguarding.
- Recognise the additional risks that children with SEND face online and ensure appropriate support.

6.4 Online Safety Lead

Where appointed, the Online Safety Lead will work closely with the DSL to:

- Support the day-to-day management of online safety.
- Receive and log reports of online safety incidents.
- Contribute to the development and review of online safety policies.
- Support the delivery of online safety education across the curriculum.
- Coordinate pupil digital champion or ambassador programmes.

6.5 IT Provider

IT Provider is responsible for:

- Maintaining the school's filtering and monitoring systems in line with the DfE's standards and the UK Safer Internet Centre definitions.
- Providing regular filtering and monitoring reports to the DSL and headteacher.
- Ensuring the technical infrastructure supports online safety.
- Advising on technical aspects of online safety and emerging risks.
- Supporting the annual filtering and monitoring review.

6.6 All Staff

- Reading, understanding, and adhering to this policy and the Acceptable Use Agreement.
- Completing online safety training at induction and attending regular updates.
- Reporting online safety concerns to the DSL or Online Safety Lead promptly.
- Modelling safe and responsible use of technology.
- Supervising pupils' use of technology during lessons and activities.
- Being aware of the online safety risks relevant to their pupils, including those with SEND.

6.7 Pupils

- Following the school's Acceptable Use Agreement.
- Reporting any online safety concerns to a trusted adult.
- Treating others with respect online, as they would face to face.
- Protecting their personal information online.

6.8 Parents and Carers

- Reading and supporting the school's online safety policies and Acceptable Use Agreement.
- Discussing online safety with their children at home.
- Reporting any online safety concerns to the school.
- Attending online safety awareness sessions provided by the school.
- Setting appropriate parental controls on home devices.

7. Education and Curriculum

7.1 Pupil Education

The school will deliver a planned programme of online safety education through the curriculum, including through PSHE, RSE, and computing, informed by the UKCIS Education for a Connected World framework. This will cover:

- Self-image and identity online.
- Online relationships and respectful behaviour.
- Online reputation and digital footprint.
- Online bullying, including cyberbullying.
- Managing online information, including misinformation, disinformation, and AI-generated content.
- Health, wellbeing, and lifestyle impacts of technology use.
- Privacy and security, including protecting personal data.
- Copyright and ownership of online content.
- The safe and responsible use of AI tools.
- How to report concerns and seek help.
- Age restrictions and why they exist.
- Sharing nudes and semi-nudes: the law and consequences.
- Radicalisation and extremism online (Prevent Duty).

7.2 Staff Training

All staff will receive online safety training at induction and at regular intervals, covering:

- The school's online safety policies and procedures.
- Recognising and responding to online safety concerns.
- The four categories of online risk (content, contact, conduct, commerce).
- Current and emerging online safety threats.
- AI-related risks, including deepfakes and AI-generated harmful content.
- Filtering and monitoring systems in place.
- Prevent Duty obligations.
- Professional conduct online and the use of personal devices.

7.3 Parent and Carer Engagement

The school will support parents and carers through:

- Regular communications about online safety, including through newsletters, the school website, and social media.
- Online safety information sessions and workshops if a particular need arises..
- Signposting to external resources and support services.
- Providing information about age-appropriate use of technology and parental controls.
- Sharing information about current online risks and trends.

8. Filtering and Monitoring

Full details of the school's filtering and monitoring arrangements are set out in the Filtering and Monitoring Policy. In summary:

- The school maintains filtering systems that meet the DfE's Filtering and Monitoring Standards and the UK Safer Internet Centre's 2025 definitions.
- Filtering is applied to all users, all school-owned devices, and all devices using the school broadband connection.
- Monitoring systems are in place to identify safeguarding concerns, with alerts escalated to the DSL.
- The filtering and monitoring provision is reviewed at least annually by the SLT, DSL, IT provider, and the responsible governor.
- Filtering systems address AI-generated content and generative AI tools in line with KCSIE.

See also the Filtering and Monitoring Policy for detailed responsibilities, standards, and procedures.

9. Mobile Phones and Personal Devices

In line with the DfE's guidance on mobile phones in schools, the school operates as a mobile-phone-free environment by default. Pupils must not access mobile phones at any point during the school day, including during lessons, break times, and lunchtimes.

More details are available in our Mobile Phone Policy.

10. Managing Online Safety Incidents

10.1 Reporting

All online safety incidents and concerns must be reported to the DSL (or deputy) as soon as possible. This includes:

- Concerns about a pupil's online activity, including out-of-school incidents.
- Disclosures from pupils about online experiences.
- Concerns about staff conduct online.
- Filtering or monitoring alerts.
- Any suspected illegal activity online.

Incidents must be logged on the school's safeguarding recording system: CPOMS.

10.2 Investigation and Response

When investigating an online safety incident:

- The DSL will make an initial assessment and determine the appropriate response.
- Where safeguarding concerns exist, the Child Protection and Safeguarding Policy will be followed.
- Evidence will be preserved, including URLs, screenshots and device records.
- The school will work with external agencies (police, local authority, CEOP) as appropriate.
- Affected individuals will be supported and provided with feedback on the outcome.

- Learning from incidents will be shared appropriately and anonymously with staff, pupils, parents, and governors.

10.3 Sharing of Nudes and Semi-Nudes

The school will follow the UKCIS guidance on sharing nudes and semi-nudes. Please see our separate policy for more details.

Key principles:

- Staff must never intentionally view, copy, print, share, store, or save such images.
- The device should be confiscated and referred immediately to the DSL.
- The DSL will assess the situation and determine whether a referral to the police or children's social care is required.
- Parents will be informed at an appropriate stage, unless doing so would place the child at greater risk.

10.4 Online Safety Concerns About Staff

Where an online safety concern is raised about a member of staff, the school will follow the procedures set out in KCSIE and the school's managing allegations procedures. This includes low-level concerns, which should be reported and recorded.

11. Safeguarding Specific Online Risks

11.1 Child Sexual Exploitation and Abuse (CSEA)

The school recognises that the internet can be used to facilitate CSEA. Staff will be trained to recognise the indicators and report concerns in line with the safeguarding policy.

11.2 Radicalisation and Extremism

Under the Prevent Duty (Counter-Terrorism and Security Act 2015), the school will ensure that filtering systems restrict access to extremist material and that pupils are educated to critically evaluate online content. Concerns about radicalisation must be reported to the DSL.

11.3 Online Bullying (Cyberbullying)

The school takes online bullying as seriously as face-to-face bullying. Online bullying will be addressed through the behaviour policy and anti-bullying policy. The school will educate pupils about the impact of online bullying and how to report it.

11.4 Artificial Intelligence Risks

KCSIE requires schools to address challenges posed by generative AI. The school will ensure that:

- Filtering and monitoring systems address AI-generated harmful content.
- Staff and pupils are educated about AI risks including deepfakes, AI hallucinations, and AI-generated inappropriate content.
- The Artificial Intelligence Policy is followed for all AI tool use.

11.5 Gaming and Gambling

The school will educate pupils about the risks associated with online gaming and gambling, including in-game purchases, loot boxes, exposure to strangers, and age-inappropriate content.

12. Acceptable Use

All staff, governors, and volunteers must sign an Acceptable Use Agreement before being granted access to school systems. Pupil-appropriate Acceptable Use Agreements will also be in place. These agreements set out the expectations for safe and responsible use of school technology.

Breaches of the Acceptable Use Agreement will be investigated and may result in disciplinary action (for staff) or sanctions under the behaviour policy (for pupils).

13. Use of Personal Devices and Cameras

13.1 Staff Personal Devices

Staff personal devices (phones, tablets, cameras) must not be used to take photographs or recordings of pupils unless explicitly authorised by the headteacher for a specific purpose.

Staff should not use personal devices to communicate with pupils or parents about school matters unless authorised through an approved school system.

13.2 Use of Cameras and Recording Devices

The use of cameras and recording devices in the school is governed by:

- Only school-owned devices should be used for photographing or recording pupils.
- Images must be stored securely and deleted when no longer needed.
- Consent must be obtained in line with the school's image consent policy.
- Cameras and recording devices (including smartwatches with camera capability) are not permitted in changing areas, toilets, or other sensitive areas.

14. Social Media

Full details are set out in the Social Media and Mobile Technologies Policy. In summary:

- Official school social media accounts must be authorised and monitored.
- Staff must not use personal social media to communicate with pupils.
- Staff must maintain professional boundaries online.
- Pupils will be educated about safe and responsible social media use.

15. Data Protection and Privacy

Online safety practices must comply with the Data Protection Act 2018 and UK GDPR. This includes:

- Ensuring that any online tools or platforms used comply with data protection requirements.
- Completing Data Protection Impact Assessments for new technologies.
- Protecting the personal data of all members of the school community.

- Responding to data breaches in line with the Data Protection Policy.

16. External Support and Resources

The school will make use of the following external support and resources:

- CEOP (Child Exploitation and Online Protection): ceop.police.uk
- UK Safer Internet Centre: saferinternet.org.uk
- Professionals Online Safety Helpline: saferinternet.org.uk/helpline
- Report Harmful Content: reportharmfulcontent.com
- Childline: 0800 1111 / childline.org.uk
- Internet Watch Foundation: iwf.org.uk
- NSPCC: nspcc.org.uk
- 360safe Self-Review Tool: 360safe.org.uk
- Local Authority safeguarding team: [Contact details]

17. Monitoring and Review

This policy will be reviewed at least annually, or more frequently in light of significant new developments, threats, or incidents. Changes will be communicated to all members of the school community.

The school will use the 360safe self-review tool (or equivalent) to support its annual review of online safety practices.