



REEDLEY PRIMARY SCHOOL

Online Safety Policy

Incorporating Keeping Children Safe in Education 2026

Document Control	
Policy owner	Headteacher, in consultation with the Designated Safeguarding Lead (DSL) and the Governing Body DSL/Online safety lead – Catherine Simmonds Filtering and Monitoring Lead – Catherine Simmonds Deputy DSL – Sarah Bell Back up DSLs – Ambreen Iqbal, Ashleigh Hume, Kerry Gorrell, Louise Cowell Headteacher – Sarah Bell Computing Lead – Carley Edwards
Approved by	Full Governing Body
Status	Statutory — reviewed at least annually and whenever KCSIE or related guidance is updated
Date of this version	01 09 2026
Date of last review	01 09 2026
Date of next review	01 09 2027
Version	1
Statutory basis	Keeping Children Safe in Education 2026 (KCSIE 2026); Working Together to Safeguard Children 2026; Online Safety Act 2023; UK GDPR; Data Protection Act 2018; Data (Use and Access) Act 2025; Filtering and Monitoring Standards; Cyber Security Standards for Schools and Colleges; Education Act 2011 (search and screening); Children's Wellbeing and Schools Act; Crime and Policing Act 2026

This policy takes effect from 1 September 2026, when KCSIE 2026 replaces KCSIE 2025. It should be read alongside the school's Child Protection and Safeguarding Policy, Behaviour Policy, Mobile Phone Policy, Anti-Bullying Policy, Acceptable Use Agreements, Data Protection Policy and Staff Code of Conduct. Where any conflict arises, the Child Protection and Safeguarding Policy takes precedence, as online safety is a core part of safeguarding rather than a stand-alone IT matter.

1. Introduction and Ethos

Reedley Primary School is committed to safeguarding and promoting the welfare of every child. This policy sets out how the school protects pupils, staff and the wider school community online, and how it responds when things go wrong. Online safety is treated as a core, integral part of the school's wider safeguarding responsibilities, not as a separate IT issue, and is addressed with the same rigour as any other safeguarding matter.

Technology is a significant factor in many safeguarding and wellbeing issues that children face, both inside and outside school. This includes child sexual abuse and exploitation, criminal exploitation, radicalisation, sexual harassment and sexual violence between children, bullying, and the growing range of harms associated with artificial intelligence (AI), including AI-generated ("deepfake") sexual imagery. Children can also be at risk from the use of AI chatbots and companion applications that simulate human relationships. This policy has been reviewed to reflect these evolving risks in line with KCSIE 2026.

This policy applies to all staff, governors, volunteers, pupils and visitors, and covers use of school systems, personal devices brought onto the premises, and, where the school's ability to safeguard is engaged, pupils' use of technology outside school (for example where online activity affects wellbeing or relationships within school).

2. Legal and Statutory Framework

This policy has been written with regard to the following legislation and statutory guidance, and will be updated as this framework changes:

- Keeping Children Safe in Education 2026 (KCSIE 2026), published by the Department for Education on 7 July 2026 and effective from 1 September 2026, replacing KCSIE 2025
- Working Together to Safeguard Children 2026
- The Online Safety Act 2023
- UK GDPR and the Data Protection Act 2018
- The Data (Use and Access) Act 2025, effective from January 2026
- The DfE Filtering and Monitoring Standards
- The DfE Cyber Security Standards for Schools and Colleges
- The Education Act 2011 (powers to search and, in limited circumstances, delete data from electronic devices)
- The Crime and Policing Act 2026 (regulated activity and volunteer supervision changes)
- The Children's Wellbeing and Schools Act

- The DfE's Generative AI: product safety expectations, and its policy paper on generative artificial intelligence in education
- Relationships Education, Relationships and Sex Education (RSE) and Health Education statutory guidance

KCSIE 2026 removes the previous condensed "Annex A" summary of Part One. From 1 September 2026, all staff — including catering, site, administrative and other staff who do not work directly with pupils — are required to read Part One of KCSIE 2026 in full, not a summary. This is recorded through staff induction and annual safeguarding training sign-off (see Section 4).

3. Scope and Definitions

For the purposes of this policy, online safety covers four categories of risk, updated in KCSIE 2026 to reflect the modern digital landscape (the "4Cs"):

Risk category	Description and KCSIE 2026 updates
Content	Being exposed to illegal, inappropriate or harmful material, including pornography, self-harm and suicide content, hateful or discriminatory material, and — newly listed in KCSIE 2026 — disinformation, misinformation and conspiracy theories.
Contact	Being subjected to harmful online interaction with other people, including adults or other children. KCSIE 2026 explicitly extends this to harmful interactions with generative AI applications that simulate human interaction, such as AI chatbots and companion-style systems.
Conduct	Personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending or receiving explicit images (sexting), or being persuaded to share personal information. KCSIE 2026 explicitly references images generated or altered using AI, including deepfakes and "deep nudes", within this category.
Commerce	Risks such as online gambling, inappropriate advertising, phishing and financial scams, including financially motivated sexual extortion (FMSE), where a child is coerced into sending an explicit image and then blackmailed.

The school also recognises the specific and serious harms of child sexual abuse material (CSAM), including AI-generated child sexual abuse material, and financially motivated sexual extortion. Staff are directed to guidance produced by the National Crime Agency's Child Exploitation and Online Protection (CEOP) education programme, in collaboration with the Internet Watch Foundation, for understanding and responding to these harms.

4. Roles and Responsibilities

4.1 Governing Body

The Governing Body has overall strategic responsibility for online safety and will:

- Approve this policy and review it at least annually, and sooner if national guidance changes
- Nominate a link governor for online safety and safeguarding, who receives regular reports
- Ensure that appropriate filtering and monitoring systems are in place and that their effectiveness is reviewed and evidenced at least once every academic year, in line with KCSIE 2026
- Ensure the school has regard to the DfE Cyber Security Standards for Schools and Colleges and treats data and cyber security as a core safeguarding matter, not solely an IT concern
- Ensure that all staff undertake safeguarding and online safety training, including training on filtering and monitoring responsibilities, on induction and at least annually thereafter

4.2 Headteacher

The Headteacher has overall day-to-day responsibility for online safety and will:

- Ensure this policy is implemented consistently across the school
- Ensure the Designated Safeguarding Lead (DSL) has sufficient time, funding, training and resources to fulfil their online safety responsibilities
- Nominate a named member of the Senior Leadership Team (SLT) with formal responsibility for filtering and monitoring systems
- Ensure that the school operates as a mobile phone-free environment by default, in line with KCSIE 2026 (see Section 8)
- Ensure that any use of generative AI tools by staff or pupils is properly risk-assessed with reference to DfE guidance on Generative AI: product safety expectations

4.3 Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for online safety as an integral part of the school's wider safeguarding arrangements. In line with KCSIE 2026, the DSL's job description explicitly includes understanding of the school's filtering and monitoring systems and processes. The DSL will:

- Keep up to date with emerging online risks, including AI-generated abuse imagery, deepfakes and financially motivated sexual extortion
- Work with the SLT member responsible for filtering and monitoring and with IT support to ensure systems are appropriate and effective
- Support staff with any online safety concerns and manage referrals to children's social care, the police, or the NCA's CEOP reporting service as appropriate

- Ensure that a shared, monitored system (such as a confidential mailbox) is in place so that concerns, including online safety concerns, are received and acted upon without delay when the DSL is unavailable
- Ensure that online safety incidents, including those involving AI-generated imagery, are recorded, monitored for patterns, and reported to governors
- Ensure that all online safety concerns are recorded on CPOMS and categorised appropriately to allow monitoring, oversight and trend analysis.

4.4 SLT Member Responsible for Filtering and Monitoring

KCSIE 2026 requires a named senior leader to hold formal responsibility for filtering and monitoring, working with the DSL and IT support — this can no longer sit solely with a technical team or an external provider. This role will:

- Lead the school's at-least-annual review of the effectiveness of filtering and monitoring systems
- Ensure that reviews include checks that filtering is working appropriately on all internet-connected devices in all relevant locations across the school
- Ensure a written record of these checks is kept and made available to governors and, where relevant, to Ofsted
- Ensure that filtering and monitoring arrangements take account of the use of generative AI tools in school, referring to the DfE's Generative AI: product safety expectations

4.5 IT Support / Network Manager

- Maintain and configure filtering and monitoring systems and carry out day-to-day technical checks
- Report technical safeguarding concerns (for example, filtering breaches or attempted circumvention) to the DSL and the responsible SLT member promptly
- Apply the DfE Cyber Security Standards for Schools and Colleges, including safeguards such as multi-factor authentication, secure backups and access management for systems holding safeguarding and pupil data
- Support staff and the DSL with the secure, time-limited retention of evidence where an online safety incident requires it

4.6 All Staff, Volunteers and Governors

Online safety is everyone's responsibility. From 1 September 2026, all staff — including those in catering, site, administrative and other non-teaching roles — must read KCSIE 2026 in full as part of induction and annual safeguarding training; the previous condensed summary (Annex A) has been withdrawn. All staff will:

- Model safe and responsible use of technology, and adhere to the Staff Acceptable Use Agreement (Appendix A)
- Understand how to recognise and respond to online safety concerns, including those relating to AI-generated imagery and financially motivated sexual extortion
- Understand their role in relation to filtering and monitoring: how to report a concern, who holds responsibility, and how concerns are escalated
- Report any concern about a child, another adult, or the school's own systems to the DSL (or deputy) without delay, following the school's Child Protection and Safeguarding Policy

4.7 Pupils

- Follow the Pupil Acceptable Use Agreement, appropriate to their age (Appendix B)
- Know how to recognise unsafe or unkind online behaviour and how to report it to a trusted adult
- Understand, in an age-appropriate way through the curriculum, that creating or sharing sexual images of a child — including images generated or altered using AI — is a form of abuse, whoever produces it and regardless of intent

4.8 Parents and Carers

Parents and carers play an essential role in supporting children's online safety at home. The school will reinforce the importance of talking to parents about children's access to online sites and apps when away from school, in line with KCSIE 2026, and will:

- Share this policy and age-appropriate online safety guidance via the school website and newsletters
- Provide information on parental controls, age ratings and safe use of AI tools and chatbots
- Signpost support such as the NSPCC, CEOP's Thinkuknow programme, and Internet Matters
- Communicate the school's mobile phone-free approach and expectations for devices brought onto or near the premises

5. Education and Curriculum

Online safety is embedded throughout the curriculum, not taught as a single, isolated lesson. It is delivered through Computing, Relationships, Sex and Health Education (RSHE), assemblies, and Personal, Social, Health and Economic (PSHE) education, and reflects the DfE's updated content risk categories, including disinformation and misinformation.

1. Pupils are taught age-appropriate lessons on staying safe online, recognising unsafe contact, and understanding that AI-generated images can look real and cause serious harm
2. Pupils are taught to think critically about what they see online, including how to recognise misleading or false information

3. Pupils are taught the school's expectations around kindness and respect online, linked to the Anti-Bullying and Behaviour Policies
4. Safer Internet Day and other national campaigns are used to reinforce key messages annually
5. Staff receive training annually, and on induction, that includes online safety, filtering and monitoring responsibilities, and how to recognise the signs of online harm, including AI-related risks
6. The school has Online Safety Ambassadors, made up of pupil volunteers from across the school, who meet regularly to discuss online safety issues and help ensure key messages are communicated to children in a meaningful and age-appropriate way.

6. Filtering and Monitoring

Reedley Primary School has appropriate filtering and monitoring systems in place across all internet-connected devices, in line with the DfE Filtering and Monitoring Standards and KCSIE 2026. The school uses Netsweeper filtering and monitoring systems, including real-time alerts through OnGuard, to identify and respond promptly to safeguarding concerns.

Filtering systems limit pupils' exposure to harmful online content; monitoring systems allow the school to identify safeguarding concerns raised through pupils' online activity on school devices and networks.

6.1 Governance and review

- The named SLT member responsible for filtering and monitoring, supported by the DSL and IT support, leads a formal review of the effectiveness of the school's filtering and monitoring systems at least once every academic year
- The review includes checks that filtering is working appropriately on all internet-connected devices in all relevant locations across the school site, and a written record of these checks is kept
- Governors receive a report on the outcome of the annual review and any resulting actions
- Filtering and monitoring provision takes account of the school's use of any generative AI tools, referring to the DfE's Generative AI: product safety expectations

6.2 Responding to alerts and breaches

- Monitoring alerts are reviewed promptly by the DSL (or deputy) and acted upon in line with the Child Protection and Safeguarding Policy
- Any attempt to bypass filtering, or any gap identified in filtering coverage, is reported to IT support and the responsible SLT member and addressed without delay
- Staff and pupils are reminded that filtering is a safeguarding tool, not a substitute for vigilance, professional curiosity, and good relationships with children

7. Artificial Intelligence (AI)

KCSIE 2026 significantly expands guidance on AI-related safeguarding risks. Reedley Primary School recognises both the educational opportunities and the safeguarding risks associated with generative AI, including AI chatbots, image generators and AI-powered learning tools.

7.1 Safe use of generative AI in school

- Any use of generative AI tools by staff for planning, marking or administration, or by pupils for learning, is risk-assessed before adoption, with reference to the DfE's Generative AI: product safety expectations
- Staff must not input personal, sensitive or safeguarding information about pupils, families or colleagues into public generative AI tools
- Pupil use of generative AI tools is supervised and age-appropriate, and forms part of the school's filtering and monitoring arrangements
- Staff receive guidance on the safeguarding, ethical, data protection and intellectual property considerations of using AI in an educational setting

7.2 AI-generated abuse, deepfakes and nudes/semi-nudes

In line with KCSIE 2026, the school treats the making or sharing of nude or semi-nude images of a child as abuse regardless of how the image was produced, including where it has been digitally altered or wholly generated using AI (sometimes described as "deepfakes" or "deep nudes"). This applies equally where a child creates such an image of themselves or of another child, or of an adult impersonating a child, and whether or not the child understood the seriousness of what they were doing.

- Any concern about AI-generated or manipulated sexual imagery involving a child is treated as a child protection concern and reported immediately to the DSL
- Staff do not view, forward, download or print any such image; concerns are reported and escalated in line with searching, screening and confiscation guidance and the Child Protection and Safeguarding Policy
- The DSL refers appropriately to children's social care and/or the police, and may draw on NCA-CEOP and Internet Watch Foundation guidance on understanding and responding to AI-generated child sexual abuse material
- Where financially motivated sexual extortion (FMSE) is suspected — where a child is coerced into sharing an image and then blackmailed — the DSL follows NCA-CEOP guidance for education settings and treats this as an urgent safeguarding matter

8. Mobile Phones and Personal Devices

In line with KCSIE 2026, Reedley Primary School operates as a mobile phone-free environment by default. Pupils do not have access to personal mobile phones during the school day, including

lessons, time between lessons, breaktimes and lunchtimes, except where an individual exception has been agreed (for example, for a medical or safeguarding reason).

- Any pupil who brings a mobile phone or smart device to school for a specific reason (such as travel to and from school) must hand it in at the school office / class teacher at the start of the day and collect it at the end of the day, in line with the school's Mobile Phone Policy
- Staff personal mobile phone use is governed by the Staff Code of Conduct and Acceptable Use Agreement; staff do not use personal devices to take photographs or videos of pupils.
- Visitors, volunteers and parents/carers are made aware of the school's expectations regarding mobile phone and camera use on the premises. Personal mobile phones should only be used in designated staff areas unless specific permission has been granted.

9. Cyber Security

KCSIE 2026 makes clear that cyber security is a core safeguarding responsibility, not solely a technical matter, because schools hold sensitive personal data, including safeguarding records, and a cyber-attack can pose an immediate risk to a child's safety and wellbeing. Reedley Primary School has regard to the DfE's Cyber Security Standards for Schools and Colleges and will:

- Maintain up-to-date anti-malware protection, firewalls and secure, regularly tested backups of critical systems and safeguarding data
- Require multi-factor authentication and strong password practices for access to school systems, particularly those holding pupil and safeguarding information
- Ensure that access to safeguarding records (including CPOMS or equivalent systems) is restricted to authorised staff on a need-to-know basis
- Have a clear incident response plan in the event of a cyber-attack or data breach, including immediate escalation to the Headteacher, DSL and Data Protection Officer
- Provide staff training on phishing, cybercrime and safe data-handling practices, recognising that young people themselves may be drawn into cybercrime without understanding its full implications

10. Data Protection

The school processes personal data, including safeguarding information, in accordance with UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025. Data protection law is never used as a reason to delay or avoid sharing information where there is a concern about a child's safety or welfare; appropriate information sharing to keep children safe always takes precedence.

- Safeguarding and child protection records, including those relating to online safety incidents, are stored securely and access is restricted to those with a legitimate need

- The school's Data Protection Policy and Privacy Notices set out further detail on how personal data is collected, used, stored and shared
- Staff are reminded that images, videos or personal information relating to pupils must only be captured, stored and shared using approved school systems

11. Reporting and Responding to Online Safety Concerns

Any concern about a child's safety online — whether relating to content, contact, conduct, commerce, AI-generated imagery, cyberbullying or any other online harm — is treated with the same seriousness as any other safeguarding concern and follows the same reporting route.

- Any pupil, member of staff, parent or visitor with a concern reports it immediately to the DSL or a Deputy DSL
- Where the DSL is unavailable, concerns should be reported to the Deputy DSL or one of the Backup DSLs to ensure the concern is received and acted upon without delay.
- All online safety concerns will be recorded on CPOMS and categorised appropriately to allow monitoring, oversight and trend analysis.
- The DSL assesses the concern, records it appropriately, and determines next steps, which may include referral to children's social care, the police, or reporting to the NCA's CEOP service (www.ceop.police.uk) for concerns about online sexual abuse or grooming
- Where illegal content (such as suspected CSAM) is discovered, staff must not attempt to view, copy, print, share, store or forward it; the DSL and Headteacher isolate the device where safe to do so and contact the police and/or CEOP immediately
- Incidents are logged, reviewed for patterns and trends, and reported to governors as part of the school's regular safeguarding reporting

Staff should never investigate an online safety concern themselves beyond what is necessary to establish immediate safety. Concerns are a matter for the DSL, working with external agencies as appropriate.

12. Working with Parents and the Wider Community

The school recognises that most children's online activity takes place outside school, and reinforces the importance of open conversations between parents and children about online sites, apps and games. The school will:

- Provide regular online safety updates and guidance to parents, including on AI-related risks, through newsletters, the school website, and parent workshops
- Encourage parents to raise any online safety concern, including any concern about another child or family, with the DSL

- Work with external partners, including the local authority, police, and organisations such as the NSPCC and Internet Watch Foundation, where needed

13. Monitoring, Evaluation and Review

- This policy is reviewed at least annually by the DSL and Headteacher, and approved by the Governing Body
- It is reviewed immediately following any significant change to statutory guidance, such as the publication of a revised edition of KCSIE, or following a serious online safety incident
- The effectiveness of filtering and monitoring systems is formally reviewed and recorded at least once every academic year, as set out in Section 6
- Online safety incident logs are analysed periodically to identify trends and inform staff training and curriculum priorities

Appendix A: Staff Acceptable Use Agreement (Summary)

- I will only use school systems, devices and accounts for professional purposes and in line with this policy
- I will not share my login details with anyone else, and will report any suspected compromise of my account immediately
- I will not take, store or share images or videos of pupils on personal devices
- I will not input personal, sensitive or safeguarding information about pupils, families or colleagues into public generative AI tools
- I will report any online safety concern, filtering or monitoring gap, or suspicious content immediately to the DSL
- I understand that my use of school systems may be monitored and that this policy applies on and off the school site where using school equipment or accounts

Appendix B: Pupil Acceptable Use Agreement (Summary — age-appropriate versions to be used in practice)

- I will only use the internet and school devices for learning, with an adult's permission and supervision
- I will tell a trusted adult straight away if I see something online that upsets or worries me, or if someone online asks me to do something I'm not comfortable with
- I will be kind and respectful online, just as I am expected to be in school
- I will not share personal information, photos or videos of myself or others without permission
- I understand that creating or sharing a nude or partly-nude picture of a child, including one made using AI, is never allowed and is a form of abuse

Appendix C: Useful Contacts and Resources

Organisation	Purpose
CEOP (Child Exploitation and Online Protection)	Report concerns about online grooming or sexual abuse: www.ceop.police.uk
Internet Watch Foundation (IWF)	Reports and helps remove child sexual abuse material online: www.iwf.org.uk
NSPCC	Safeguarding advice and support: 0808 800 5000
Childline	Support for children and young people: 0800 1111
Report Harmful Content	Support for reporting harmful online content: reportharmfulcontent.com
Professionals' Online Safety Helpline (UK Safer Internet Centre)	Advice for school staff: 0344 381 4772

This policy should be read alongside the school's Child Protection and Safeguarding Policy, Behaviour Policy, Mobile Phone Policy, Anti-Bullying Policy, Staff Code of Conduct, Data Protection Policy and Acceptable Use Agreements, all of which are available from the school office or website.