Online Safety Policy

Reviewed for the 2025–26 school year

Approved by:	Full Governing Body	**Date:** 24th March 2026
Last reviewed on:	Spring 2026	
Next review due by:	Spring 2027	

Purpose of this policy
This policy explains how the school keeps pupils safe when technology or online activity is involved. It sets the standard for what adults must do, what pupils are taught, how concerns are passed on and how the school responds when something goes wrong.

Schedule for approval, monitoring and review

Area	Position
Approved by	Governing body
Operational monitoring	Senior leaders, DSL and Online Safety Lead; reviewed through the year and after any serious incident
Filtering and monitoring review	At least annually, with more frequent review where incidents, alerts, curriculum changes or new risks make this necessary
Reporting to governors	Termly through safeguarding reporting, with immediate escalation where a serious issue requires governor awareness
Formal policy review	Annually and sooner if law, guidance, technology, local risk or school practice changes
External agencies likely to be involved when required	Children's social care, police, Prevent, LADO, CEOP, the local authority and other relevant safeguarding partners

1. Status of this policy

Online safety is part of safeguarding. The school treats online concerns with the same seriousness as offline concerns. Depending on the issue, the response may sit within safeguarding, behaviour, staff conduct, information security, or more than one of these at the same time.

This policy should be read alongside the Child Protection and Safeguarding Policy, Behaviour Policy, Staff Code of Conduct, low-level concerns procedures, Data Protection Policy, acceptable use arrangements and any published arrangements for pupil mobile phones and personal devices.

The school will apply this policy in line with current statutory guidance, including Keeping Children Safe in Education, Working Together to Safeguard Children, the DfE filtering and monitoring standards, guidance on searching, screening and confiscation, guidance on sharing nudes and semi-nudes, and any other relevant safeguarding or education guidance in force at the time.

2. Scope

This policy applies to pupils, staff, volunteers, governors, supply staff, contractors, visitors, parents and carers where their conduct affects pupils, staff, school systems or the wider life of the school.

It applies to school devices, school accounts, school networks, cloud systems, online platforms used for school business, school-owned images and data, and personal devices or accounts where their use affects safeguarding, behaviour, staff conduct, data protection or the reputation and safe running of the school.

3. Core principles

- The welfare of the child is paramount.
- A concern does not become less serious because it happened online, out of school or on a personal device.
- Staff must not wait until they are sure before acting. If something gives rise to concern, they must make a record and speak to the DSL or a deputy DSL without delay.
- Professional curiosity, clear records and prompt escalation are expected from all staff.
- Safeguarding responsibility cannot be diluted by informal custom, convenience or local habit.
- The school will use the least intrusive approach consistent with keeping children safe, preserving evidence and meeting legal duties.

4. What this policy is for

- Keep pupils and adults safe from online harm.
- Set a clear working standard for safe, lawful and professional use of technology.
- Make sure concerns are noticed, recorded and passed on without delay.
- Reduce the risk of uneven practice between staff, classes or phases.
- Teach pupils how to keep themselves and others safe online in a way that matches their age and understanding.
- Use review, incidents and emerging patterns to strengthen practice over time.

5. Categories of online risk

The school recognises that online harm may sit within one or more of the following categories:

- Content: exposure to illegal, inappropriate or harmful material, including pornography, violent material, extremist content, self-harm material, misinformation, disinformation and manipulated or AI-generated content.
- Contact: being contacted by others in ways that are exploitative, abusive, coercive, sexualised, intimidating or deceptive.
- Conduct: online behaviour by a child or adult that causes harm, increases risk or breaches expected standards.
- Commerce: fraud, scams, grooming linked to money, coercive financial requests, phishing, gambling and other financial exploitation.

6. Safeguarding position

The school recognises that online harm can include child-on-child abuse, sexual harassment, sexual violence, harmful sexual behaviour, grooming, criminal exploitation, coercive control, bullying, prejudice-based abuse, radicalisation, blackmail, image-based abuse, sharing nudes and semi-nudes, and exposure to illegal or harmful content.

Any concern that may indicate abuse, exploitation, significant harm, a pattern of unsafe behaviour, or risk to a vulnerable pupil must be treated as a safeguarding concern and managed accordingly.

Where professional judgement is needed in relation to harmful sexual behaviour, staff will use recognised safeguarding tools and the school will draw on the Brook Traffic Light Tool where appropriate. Such tools support judgement; they do not replace DSL decision-making.

7. Roles and accountabilities

Governing body

- The governing body holds leaders to account for the safe and lawful implementation of this policy.
- Governors will assure themselves that filtering and monitoring arrangements are in place, are reviewed at least annually and match the school's age range, systems and risks.
- Governors will receive regular safeguarding information, including online safety themes, patterns and actions taken.

Headteacher and senior leaders

- Senior leaders are responsible for making sure this policy is understood, implemented and enforced.
- Leaders will ensure that staff training, reporting routes, technical controls and curriculum provision are in place, understood and applied in practice, not left to individual preference.
- Leaders will act on weaknesses identified through incidents, audits, staff feedback or safeguarding review.

Designated Safeguarding Lead

- The DSL has lead responsibility for safeguarding and child protection, including online safety.
- The DSL is the school's lead decision-maker for online safeguarding concerns and for referrals to external agencies.
- The DSL will oversee the quality of recording, identify patterns, support staff, review the needs of vulnerable pupils and ensure that concerns are followed through properly.

Online Safety Lead

- The Online Safety Lead supports the DSL, but does not replace or override the DSL's safeguarding authority.
- The Online Safety Lead will coordinate curriculum planning, contribute to staff training, review patterns, work with technical staff and support policy review.
- Where the Online Safety Lead reviews filtering or monitoring information, any safeguarding concern must be passed to the DSL or a deputy DSL without delay and recorded in line with safeguarding procedures.

Technical staff and service providers

- Technical staff must keep systems secure and up to date, maintain suitable filtering and monitoring, control access properly, and report concerns or weaknesses promptly.
- Technical decisions must reflect safeguarding need as well as operational convenience.
- Technical staff must not make unilateral decisions to relax filtering, disable monitoring or bypass agreed controls without clear authorisation.

All staff, volunteers and contractors

- All adults must follow this policy, the staff code of conduct and acceptable use expectations.
- All adults must use school-approved systems for contact with pupils and families unless a specific exception has been authorised.
- All adults must report concerns immediately, make a clear factual record and avoid private investigation beyond what is needed to secure immediate safety and pass information on.

Pupils

- Pupils will be taught and expected to use technology safely, respectfully and lawfully.
- Pupils must report anything that worries them or puts them or another child at risk.
- Pupils must follow the school's instructions on devices, accounts, images and online conduct.

Parents and carers

- The school will work with parents and carers as partners in keeping children safe.
- Parents and carers will receive clear information about risks, age restrictions, devices, apps and reporting routes.

- Where a concern affects a child's safety or wellbeing, the school will involve parents and carers unless doing so would place the child at additional risk.

8. Education and curriculum

Online safety education will be taught through the curriculum and reinforced through assemblies, pastoral work, safeguarding messages and everyday classroom practice.

Teaching will be planned for primary pupils, matched to age and stage, and adapted where children need repetition, simpler language, scaffolding or additional support.

- healthy and respectful online relationships
- privacy, passwords and account security
- consent, boundaries and pressure to share images or information
- grooming, exploitation, coercion and manipulation
- bullying, child-on-child abuse and how to get help
- misinformation, disinformation and manipulated or AI-generated content
- fraud, scams and requests for money or personal information
- how and where to report concerns in school and beyond school

Pupils with SEND or other vulnerabilities will receive adapted teaching, additional rehearsal and targeted support where required.

9. Staff training and professional conduct

- All staff will receive safeguarding and online safety training at induction and regular updates after that.
- Training will cover reporting routes, professional boundaries, filtering and monitoring awareness, image-based abuse, sharing nudes and semi-nudes, harmful sexual behaviour, misinformation and AI-related risks.
- Governors will receive training sufficient to discharge their safeguarding and monitoring responsibilities.
- Staff must maintain professional boundaries online at all times. Personal contact with pupils through private accounts, private messaging or informal platforms is not permitted unless there is a clear, recorded and authorised reason.

10. Filtering, monitoring and technical control

The school will maintain filtering and monitoring systems that meet its safeguarding needs, reflect pupils' age and stage, and are reviewed against current DfE standards.

Filtering and monitoring are safeguarding controls. They are not optional, and they are not treated as a purely technical matter.

- Filtering will block or reduce access to harmful and inappropriate content without unreasonably disrupting teaching and learning.

- Monitoring arrangements will be designed to pick up indicators of risk, misuse and safeguarding concern, not merely rule-breaking.
- Safeguarding leaders will review alerts, themes and patterns often enough to spot risk and act in time.
- Weaknesses, false assurance or repeated gaps in filtering and monitoring will be escalated and put right.
- Any decision to permit access to restricted material for a legitimate educational purpose must be time-limited, risk-assessed where necessary and approved through normal school processes.

11. Devices, accounts, communication and images

School devices and accounts

- School devices, systems and accounts must be used for school business in line with this policy and acceptable use expectations.
- Shared accounts must only be used where there is a clear operational reason and suitable oversight.
- Passwords, multi-factor authentication and access rights must be managed securely.

Personal devices

- Staff must not use personal devices or accounts to contact pupils except where there is explicit authorisation and no safe school-based alternative.
- Any pupil mobile phone or personal connected device brought onto site must be managed in line with the school's published arrangements, and those arrangements must be enforced consistently.
- A personal device does not create a private space exempt from school action where safeguarding, staff conduct, behaviour, crime or serious disruption is involved.

Images and recordings

- Staff must use school-approved devices for taking, storing or sharing pupil images unless an emergency makes this impossible and the reason is recorded and reported.
- The school will control how pupil images are taken, stored, used and published. It will follow its data protection arrangements and recorded parental preferences.
- Full names will not be published with pupil images unless there is a clear and lawful reason to do so.

Artificial intelligence and manipulated content

- The school recognises that AI tools and manipulated media can increase the risk of bullying, harassment, fraud, misinformation, sexualised abuse and reputational harm.
- Staff and pupils must not use AI tools, image generators or editing tools in a way that is unsafe, unlawful, deceptive, abusive or inconsistent with school rules.

- Any concern involving deepfakes, manipulated images, impersonation or AI-assisted abuse must be treated according to the level of harm involved and must not be dismissed as a prank.

12. Responding to concerns and incidents

All online concerns must be acted on. Staff must not ignore them, play them down, delay action or make side arrangements outside the school's reporting systems.

1. Make the situation safe. If there is an immediate risk of harm, take urgent action and involve the DSL or a deputy DSL at once.
2. Record the concern promptly and factually on CPOMS The record must be clear about what was seen, said, reported or found, and by whom.
3. Pass the information to the DSL or a deputy DSL without delay. Staff must not assume that someone else has already done this.
4. Preserve evidence where necessary. Staff must not forward, copy or share harmful material unless this is strictly necessary to safeguard a child and is permitted by relevant guidance.
5. Follow the DSL's direction on parent contact, device handling, search, confiscation, external referral and support for the child or children involved.
6. Review what happened and whether any wider action is needed, including support, sanctions, curriculum response, technical change or staff briefing.

Incidents involving nude or semi-nude images, sexualised content, serious harassment, coercion, exploitation or possible criminal behaviour must be handled in line with current statutory guidance and safeguarding procedures. Staff must not conduct informal investigations or create unnecessary copies of imagery.

Illegal content must not be treated as a routine behaviour issue. The DSL will determine the appropriate referral route, including police or other agencies where required.

13. Behaviour, sanctions and support

The school will respond to misuse of technology in a way that keeps children safe, maintains standards and takes account of the age, understanding and needs of the pupils involved.

Where a response is disciplinary, it will still be informed by safeguarding. Where a response is safeguarding-led, this does not prevent the school from applying sanctions where justified.

- Victims and affected pupils will be supported and kept safe.
- Sanctions will be proportionate, applied consistently and rooted in published school expectations.
- Access to technology may be restricted where necessary to reduce risk.
- Serious incidents may lead to safeguarding referral, suspension or exclusion where lawful and appropriate.

14. Working with parents and carers

- The school will provide regular information for parents and carers about online risks, age ratings, devices, apps and reporting routes.
- The school will explain its expectations clearly so families know what the school will act on, what should be reported and how concerns should be raised.
- Where a concern arises outside school but affects safety, behaviour or the orderly running of the school, the school will take it seriously and respond in line with its policies.

15. Data protection and information security

Personal data will be processed in line with UK GDPR, the Data Protection Act 2018 and the school's data protection arrangements.

Information security is part of online safety. Secure handling of personal information, controlled access, strong passwords, encryption where required, and prompt management of breaches are expected standards, not optional extras.

16. Monitoring, assurance and review

- Leaders will monitor incidents, themes, staff understanding, curriculum delivery and technical controls through the year.
- The school will review this policy at least annually and sooner where incidents, new guidance, new technology or local patterns indicate that change is needed.
- Reviews will focus on whether practice is working in reality, not simply on whether documents exist.
- Where inconsistency, delay or erosion of standards is identified, leaders will tighten systems, clarify expectations and check that the change has taken effect.