



Pinewood Infant School & Foundation Unit ONLINE SAFETY POLICY

Autumn 2026

Approved by	Governing Body
Policy lead	Rachel Otter – Headteacher / DSL / Online Safety Lead
Assistant Online Safety Lead	Kellie Reilly
Date approved	Autumn 2026
Next review	Autumn 2027, or sooner where required

1. Development, Review and Monitoring

This Online Safety Policy has been developed by Rachel Otter, Headteacher, DSL and Online Safety Lead; Kellie Reilly, Assistant Online Safety Lead; teaching, support and technical staff; and governors. Consultation with the school community takes place through formal and informal meetings and relevant safeguarding and technical guidance.

Review arrangements

- The policy will be reviewed at least annually and normally during the Autumn term.
- The policy will also be reviewed following significant online safety or safeguarding incidents, significant changes to technology, changes to legislation or statutory guidance, significant changes to filtering and monitoring provision, or emerging online risks.
- The Governing Body will receive appropriate information about online safety, including relevant incident data, filtering and monitoring arrangements and the outcomes of annual reviews.

Filtering and monitoring annual review

Pinewood Infant School will review its filtering and monitoring provision at least annually. The review will involve the DSL, Online Safety Lead, relevant member(s) of the senior leadership team, IT support and the Online Safety Governor.

- the effectiveness and coverage of filtering and monitoring;
- alerts, incidents and concerns and how they have been responded to;
- whether provision remains appropriate for the age and developmental stage of pupils;
- the needs of pupils with SEND, communication needs and EAL;
- emerging technologies, including generative AI;
- known limitations, gaps or weaknesses in the current provision;
- whether staff and pupils know how to report concerns;
- actions required, timescales and the person responsible for completion.

The outcome of the review will be recorded and reported to governors. Technical arrangements will be checked with the school's managed IT provider so that policy wording accurately reflects the systems in use.

Scope of the policy

This policy applies to all members of the school community, including staff, pupils, governors, volunteers, parents/carers and visitors, who access or use school digital technology or school systems, both in and out of school.

The school will respond to online safety incidents in accordance with this policy and related safeguarding, behaviour, anti-bullying, acceptable use, data protection and disciplinary procedures. Where an incident takes place outside school but is linked to membership of the school, the school may take appropriate action in line with its published policies and legal duties.

2. Links to Other Policies and Safeguarding

This policy forms part of Pinewood Infant School's wider safeguarding arrangements and should be read alongside:

- Keeping Children Safe in Education 2026 (KCSIE 2026)
- Child Protection and Safeguarding Policy
- Staff, Pupil and Parent/Carer Acceptable Use Agreements
- Computing Policy
- Behaviour Policy
- Anti-Bullying Policy
- Mobile Phone Policy
- Remote Learning Policy, where applicable
- Device Loan Agreement
- Social Media Policy
- Data Protection Policy / Privacy Notices
- Cyber Security Policy and relevant IT procedures

Our commitment

Pinewood Infant School recognises that keeping children safe online is an integral part of safeguarding. Technology is part of everyday life, including for our youngest learners, and brings both educational opportunities and risks.

- Embedding online safety throughout safeguarding policies and daily practice.
- Maintaining effective, proportionate and age-appropriate filtering and monitoring on school systems and devices.
- Ensuring staff receive appropriate training and understand online risks, reporting routes and the systems used by the school.
- Providing age-appropriate online safety education so children begin to understand how to stay safe online, ask for help and develop digital resilience.
- Working with parents and carers to promote safe and responsible use of technology at home.
- Reviewing practice regularly in response to new and emerging online risks.

Online risk

The school recognises the four broad categories of online risk: Content, Contact, Conduct and Commerce. The school also recognises emerging risks associated with misinformation, disinformation, conspiracy theories, artificial intelligence, synthetic or manipulated media, online bullying and other harmful online behaviours.

Online safety education and safeguarding arrangements will be proportionate to the age and developmental stage of pupils. The school will not expose young children unnecessarily to adult terminology or examples; instead, it will teach developmentally appropriate concepts such as asking for help, keeping information private, recognising unsafe or upsetting content, and understanding that information found online is not always accurate.

3. Roles and Responsibilities

Governing Body

- Approve the Online Safety Policy and review its effectiveness.
- Seek assurance that appropriate filtering and monitoring arrangements are in place.
- Receive appropriate information about online safety incidents and the outcomes of filtering and monitoring reviews.
- Ensure that online safety is considered as part of wider safeguarding and risk management.

Headteacher / DSL / Online Safety Lead

- Provide strategic leadership for online safety within the school's safeguarding framework.
- Ensure online safety concerns are managed as safeguarding concerns where appropriate.
- Ensure the Assistant Online Safety Lead and relevant staff receive appropriate training.
- Oversee serious online safety allegations involving staff in accordance with safeguarding and allegations procedures.
- Ensure filtering and monitoring arrangements are appropriately governed and reviewed.

Assistant Online Safety Lead

- Take day-to-day responsibility for online safety issues and contribute to policy development and review.
- Provide advice and training to staff.
- Receive and record online safety concerns and incidents and ensure appropriate escalation.
- Work with the DSL, IT provider and governors on filtering and monitoring.
- Coordinate the annual filtering and monitoring review and track agreed actions.
- Keep up to date with relevant DfE, safeguarding, cyber-security and online-safety guidance.

IT / Technical Support

- Maintain appropriate technical security for school networks, devices and systems.
- Support secure account management, access controls, updates, anti-malware, firewall and other relevant protections.
- Support filtering and monitoring configuration, testing and review.
- Provide technical information and reports needed for safeguarding and governance.
- Support incident response and recovery following cyber-security incidents.

Teaching and Support Staff

- Maintain current awareness of online safety and follow this policy and the Acceptable Use Agreement.
- Complete required online-safety and safeguarding training.
- Report concerns promptly to the DSL, Online Safety Lead or other designated person.
- Use official school systems for professional digital communication with pupils and parents/carers.
- Supervise children's use of digital technology appropriately.
- Use only suitable, age-appropriate online resources.
- Do not investigate potentially illegal material themselves.
- Do not enter personal, confidential or sensitive school information into unapproved AI tools.

4. Pupils and Online Safety Education

Pupils

- Use school digital technology in accordance with the Pupil Acceptable Use Agreement and adult guidance.
- Tell a trusted adult if something online makes them feel worried, uncomfortable or unsafe.
- Understand that they should not share personal information without appropriate adult guidance.
- Follow age-appropriate online safety rules and ask for help when unsure.

Education

Online safety education is an essential part of the school's provision. It will be taught through Computing, PSHE, RSHE where appropriate, assemblies, stories, discussion, modelling and everyday classroom practice.

- The planned curriculum will be broad, relevant, progressive and regularly revisited.
- Online safety messages will be reinforced through assemblies and wider school activities.
- Children will be taught that online information may be inaccurate, misleading or untrue.
- Children will be taught to ask for help if they encounter something upsetting or inappropriate.
- Children will learn age-appropriate strategies for protecting personal information and communicating safely.
- Staff will model safe and responsible use of technology.
- Where internet use is planned, staff will use resources that have been checked as suitable.
- Online safety education will be adapted for pupils' age, developmental stage, SEND, communication needs and EAL.

Media literacy and misinformation

At an age-appropriate level, children will begin to understand that people can create, change and share information online. Staff will support children to question information, recognise obvious signs that something may not be true, and seek help from a trusted adult.

Parents and carers

- The school will provide online safety information through newsletters, the website, parent communications, workshops and appropriate campaigns.
- The school will signpost parents/carers to reliable advice and age-appropriate resources.
- Parents/carers will be encouraged to discuss online safety with their children and to report concerns where an online incident may affect a child's safety or wellbeing.

5. Filtering and Monitoring

Pinewood Infant School recognises that filtering and monitoring are important safeguarding measures which help protect children and staff from illegal, inappropriate and potentially harmful online content.

Filtering is preventative and aims to prevent access to inappropriate or harmful content. Monitoring is reactive and identifies potentially harmful activity through technical alerts, reports and appropriate manual supervision.

The school recognises that no filtering or monitoring system can be completely effective. Technical controls will therefore be combined with supervision, education, staff awareness and safeguarding procedures.

Filtering and monitoring arrangements

- Filtering and monitoring will be appropriate to the school's age range and safeguarding risk profile.
- Provision will take account of pupils' SEND, communication and EAL needs.
- The school will consider the safeguarding implications of generative AI and other emerging technologies.
- Filtering will aim to prevent access to illegal, inappropriate and harmful content, including relevant online harms and harmful AI-generated content where technically supported.
- Monitoring arrangements will generate alerts or reports for potentially harmful activity where supported by the school's systems.
- Staff will understand how to report technical or safeguarding concerns relating to filtering and monitoring.
- The school will document decisions about what is blocked or allowed where appropriate and will review the effectiveness of provision.
- The school will work with its managed IT provider to understand system capabilities, limitations and coverage.

Alerts, incidents and escalation

- Alerts and reports will be reviewed by appropriately trained and authorised staff.
- Where an alert indicates a possible safeguarding concern, it will be escalated to the DSL without delay.
- Online safety incidents will be recorded in accordance with school safeguarding and incident-recording procedures.
- Staff will not attempt to investigate suspected criminal or illegal material themselves.
- Filtering and monitoring weaknesses or false negatives/positives will be considered as part of ongoing review.

Annual review

The school's filtering and monitoring provision will be reviewed at least annually and following significant incidents, technology changes or emerging risks. The review will involve the DSL, Online Safety Lead, relevant SLT, IT support and the Online Safety Governor. Findings, actions and responsibilities will be recorded.

6. Technical Infrastructure, Cyber Security and Devices

Technical security

- School systems will be protected by appropriate firewalls, anti-malware and other security controls.
- Devices and software will be kept appropriately updated and security vulnerabilities will be addressed promptly.
- User access will follow the principle of least privilege wherever practicable.
- Accounts and permissions will be reviewed and removed promptly when no longer required.
- Multi-factor authentication will be used where appropriate and available for critical systems.
- Appropriate backups and recovery arrangements will be maintained for critical systems and data.
- Cyber-security arrangements will be reviewed regularly and benchmarked against current DfE and NCSC expectations.

Cyber-security awareness

- Staff will receive appropriate awareness training covering phishing, suspicious links, passwords, device security and reporting concerns.
- Staff will lock screens and secure devices when unattended.
- Suspected cyber attacks or data-security incidents will be reported without delay to the DSL/Headteacher and IT support in accordance with school procedures.
- Serious incidents may be escalated to relevant external agencies where required.

School devices

- School laptops and other devices will be used in accordance with school security procedures.
- Devices taken off site must be protected in accordance with the school's Security Handling and Data Protection arrangements.
- School devices must not be shared with unauthorised users.
- Staff leaving employment will have access removed in accordance with school procedures.

Personal devices and mobile phones

The use of mobile phones and personal devices by staff, pupils and visitors will be managed in accordance with the school's Mobile Phone Policy and Acceptable Use Agreements. The school will follow current statutory guidance on mobile phones in schools.

- Personal phones must not be used to photograph or record pupils unless specifically authorised under school procedures.
- Personal devices must not be used to communicate with pupils or parents/carers on behalf of the school.
- Staff personal devices will be kept out of sight and away from children's access when not in use.
- Visitors will follow the school's visitor and acceptable-use arrangements.

7. Digital Images, Personal Data and Communication

Digital and video images

- Staff will follow school procedures for taking, storing, using and publishing photographs and videos.
- Photographs and videos will only be taken using authorised school equipment or systems unless a specific exception has been approved.
- Current parental permissions and restrictions will be checked before images are published.
- Images will be selected carefully and used in accordance with safeguarding and data-protection requirements.
- Pupils' full names will not normally be published alongside photographs on the school website or public platforms.
- Parents/carers attending school events may take images for personal use where permitted, but should not publish images containing other children without appropriate permission.

Personal data

- Personal data will be processed in accordance with current data-protection legislation and the school's Data Protection Policy.
- The school will collect and retain only the personal data necessary for its functions and will retain it for no longer than necessary.
- Data will be accurate and kept up to date.
- Lawful bases and any relevant special-category conditions will be identified and documented.
- Appropriate security, access, storage, transfer and disposal arrangements will be maintained.
- Data breaches will be managed through the school's data-breach procedures, including consideration of ICO reporting requirements.

Generative AI and personal data

Staff must not enter personal, confidential or sensitive information relating to pupils, families or staff into publicly available or unapproved generative AI tools. Where the school approves an AI tool that processes personal data, appropriate data-protection, safeguarding and security checks must be completed before use.

A Data Protection Impact Assessment will be completed where required, including where a proposed technology involves high-risk processing of personal data.

Digital communication

- Official school communication systems will be used for professional communication with pupils and parents/carers.
- Digital communications must be professional in tone and content.
- Personal email addresses, personal messaging accounts and personal social-media accounts must not be used for school communication with pupils or parents/carers.
- Personal information about pupils, families or colleagues must not be shared on personal social-media platforms.

8. Social Media and Professional Identity

The school recognises that social media can create safeguarding, reputational, professional and data-protection risks. Staff are expected to maintain professional boundaries online.

- Staff must not make inappropriate references to pupils, parents/carers or colleagues on personal social-media accounts.
- Staff must not disclose confidential school information online.
- Staff should review privacy and security settings regularly.
- Where a personal account identifies a staff member as working at Pinewood, staff should make clear that personal views are their own where relevant.
- Official school social-media accounts must have appropriate approval, administration and monitoring arrangements involving at least two authorised staff where practicable.
- Concerns about online abuse, harassment or misuse involving the school community should be reported through the appropriate school procedure.

Personal use of social media

Reasonable personal use of social media is permitted where it does not interfere with professional duties, breach school policies, compromise confidentiality, bring the school into disrepute or create a safeguarding risk. Where personal online activity impacts on the school or a member of the school community, it may fall within the scope of school policies and relevant disciplinary procedures.

Children's use of social media

Pinewood is an infant school and recognises that many social-media platforms have age restrictions. The school will provide age-appropriate education about online communication and encourage parents/carers to follow platform age requirements and seek advice where they have concerns.

9. Artificial Intelligence (AI)

Pinewood Infant School recognises that artificial intelligence, including generative AI, is increasingly used in education and everyday life. The school will consider both the opportunities and risks associated with AI and will ensure that its use supports learning, safeguarding and wellbeing.

- AI tools used for school purposes must be appropriate for the intended use and comply with safeguarding, data-protection, copyright, acceptable-use and cyber-security requirements.
- Staff must use only AI tools approved by the school where school-related or personal information is being processed.
- Staff must not enter personal, confidential or sensitive information about pupils, families or staff into unapproved AI tools.
- AI-generated information must be checked for accuracy, bias and appropriateness.
- Professional judgement remains the responsibility of the member of staff; AI output must not be accepted uncritically.
- The school will consider the potential impact of AI on children's learning, wellbeing and development.
- Age restrictions and product terms must be followed.
- Concerns about harmful, inappropriate, misleading or manipulated AI-generated content must be reported.

Pupil-facing AI

Pupil-facing AI will only be introduced where appropriate safeguards are in place, including age-appropriate use, close supervision, suitable filtering and monitoring, appropriate product safety features and data-protection arrangements.

The school will consider the DfE Generative AI Product Safety Standards when assessing products intended for use in educational settings. Particular attention will be given to age appropriateness, SEND accessibility, filtering, monitoring, reporting, security and emerging harmful content.

AI-generated and manipulated content

The school recognises risks from synthetic or manipulated media, including deepfakes and misleading AI-generated content. Education will be age appropriate and will focus on children knowing that images, voices and information can be changed or created and that they should seek adult help when unsure.

AI review

The school's approach to AI will be reviewed regularly in response to emerging risks, changes in technology and updated DfE guidance. New or significantly changed AI use cases will be subject to appropriate safeguarding and data-protection consideration before implementation.

10. Responding to Online Safety Incidents

All members of the school community are expected to report online safety concerns promptly. Online incidents may be safeguarding, behavioural, technical, data-protection or disciplinary matters, and may involve more than one of these areas.

Immediate response

- Act promptly and prioritise the safety and wellbeing of the child or adult involved.
- Report safeguarding concerns to the DSL or deputy without delay.
- Where a child is in immediate danger, emergency services will be contacted as appropriate.
- Record the concern, actions taken, decisions, rationale and outcomes in accordance with school safeguarding procedures.

Suspected illegal or seriously harmful material

- Staff must not download, save, forward, print or otherwise reproduce suspected child sexual abuse material or other illegal material.
- Staff must not attempt to investigate suspected criminal material themselves.
- Where illegal or seriously harmful material is encountered, staff should stop accessing it where safe to do so and report the concern immediately to the DSL/Headteacher.
- The school will contact the police or other relevant agency where required.
- Any technical evidence or system information required for investigation will be preserved through appropriate IT and safeguarding procedures.

Other online safety incidents

- Incidents may include cyberbullying, inappropriate content, harmful communications, misuse of devices, unauthorised access, data breaches or inappropriate AI use.
- Incidents will be assessed and dealt with proportionately through safeguarding, behaviour, disciplinary, data-protection or technical procedures as appropriate.
- More than one senior member of staff will be involved in significant investigations where appropriate, both to support effective decision-making and to protect those involved.

11. Vulnerable Pupils, SEND and EAL

Pinewood recognises that online risks and the ability to understand or report those risks may differ according to age, developmental stage, SEND, communication needs, EAL and individual circumstances.

- Online safety teaching will be adapted where required.
- Children who have difficulty communicating concerns will be provided with appropriate alternative ways to report that something is wrong.
- Staff will consider whether additional supervision, accessibility support or individualised teaching is needed.
- Filtering and monitoring arrangements will be reviewed with the needs of pupils with SEND and EAL in mind.
- Safeguarding concerns involving vulnerable pupils will be considered within the child's wider safeguarding context.

12. School Actions and Sanctions

The school expects members of the school community to use digital technology responsibly. Most incidents are expected to involve inappropriate rather than illegal use. Incidents will be dealt with as soon as reasonably possible and in a proportionate manner.

- Pupil incidents may be managed under the Behaviour Policy, Acceptable Use Agreement and safeguarding procedures.
- Staff incidents may be managed under relevant employment, acceptable-use, safeguarding and disciplinary procedures.
- Serious incidents may be referred to the Local Authority, police, ICO, Report Fraud, NCSC or other relevant body where appropriate.
- Safeguarding concerns will be referred to the DSL and managed in accordance with the Child Protection and Safeguarding Policy.

13. Training, Awareness and Governance

Staff training

- All staff will receive appropriate online-safety and safeguarding training as part of induction and ongoing professional development.
- Training will cover current online risks, reporting routes, filtering and monitoring, cyber security, data protection and appropriate use of AI.
- The training needs of staff will be reviewed regularly.
- The Online Safety Lead will keep up to date through relevant external guidance, training and professional networks.

Governors

- Governors will receive appropriate online-safety awareness and information.
- The Online Safety Governor will support oversight of online safety incident logs and filtering/monitoring arrangements.
- Governors will receive the outcome of the annual filtering and monitoring review and any significant actions.

Parents and carers

- Parents/carers will be given appropriate information about online safety risks and practical ways to support children at home.
- The school will signpost reliable sources of advice and age-appropriate resources.
- Where appropriate, the school will share information about specific apps, platforms, emerging risks and parental controls.

14. Acceptable Use, Devices and Access

The following principles apply to use of digital devices within school. Detailed arrangements are set out in the relevant Acceptable Use Agreements and Mobile Phone Policy.

Device/user	Allowed in school	Full network access	Internet only
School-owned device – single user	Yes	Where authorised	Yes
School-owned device – multiple users	Yes	Where authorised	Yes
Authorised school device	Yes	Where authorised	Yes
Pupil-owned personal device	Only where specifically permitted	No	No
Staff personal device	Only in accordance with policy	No	Where authorised
Visitor personal device	Yes, subject to visitor arrangements	No	Where authorised

General access principles

- Users will have only the access required for their role.
- Passwords and authentication details must be kept confidential.
- Users must not attempt to bypass filtering, monitoring or security controls.
- Unauthorised software, executable files or removable media must not be introduced onto school systems.
- Personal data must not be removed from school systems unless this is authorised and appropriately secured.
- Visitors will follow the school's visitor acceptable-use arrangements.

15. Annual Online Safety Compliance Checklist

Area	Reviewed	Evidence / action
KCSIE and relevant statutory guidance reviewed	✓	Document reviewed by DSL and feedback to all staff on INSET Sept 2026. Part 1 read by all staff. All new updates now included in this policy
Filtering reviewed	✓	These have been reviewed and tested. Jeff Lee keeps DSL informed of any relevant changes.
Monitoring reviewed	✓	
Filtering tested on relevant devices	✓	
Monitoring alerts and incident records reviewed	✓	
SEND/EAL considerations reviewed	✓	Reviewed with SENDCO and SLT and updated within this policy
Cyber-security risk assessment completed	✓	Cyber training completed by all staff
Staff online-safety training completed	✓	All completed and signed off
Governor oversight completed	✓	TBC
Acceptable Use Agreements reviewed	✓	Reviewed in Sept 2026. No changes were necessary
Mobile phone arrangements reviewed	✓	Reviewed in light of the latest KCSIE and staff have been updated on safe use in school
Data protection/privacy arrangements reviewed	✓	All GDPR policies and training has been completed and updated

Key guidance used in preparing this 2026 update

- Keeping Children Safe in Education 2026 – Department for Education.
- Meeting digital and technology standards in schools and colleges: Filtering and monitoring – core standard.
- Meeting digital and technology standards in schools and colleges: Cyber security – core standard.
- Generative AI: product safety standards – Department for Education.
- Generative artificial intelligence (AI) in education – Department for Education.
- Mobile phones in schools – statutory guidance, applicable from September 2026.
- Data protection in schools – Department for Education guidance.

Policy review statement

This policy will be reviewed annually, normally during the Autumn term, and sooner where there are significant safeguarding incidents, technological developments, changes to legislation or statutory guidance, or emerging online safety risks.