

AINSLIE WOOD PRIMARY SCHOOL

Online Safety Policy

2026–2027

This policy applies to all members of the school community who access or use school digital systems, on or off site, and to personal digital technology used on the school site where permitted.

School	Ainslie Wood Primary School
Headteacher	Julie Crouch
Designated Safeguarding Lead / day-to-day online safety lead	Philippa Ioannou
Governing Body safeguarding oversight	Chair of Governors / Safeguarding Governor
Policy version	1.0 – September 2026
Approval	To be confirmed by the Governing Body
Next review	September 2027, or sooner if required

140 Ainslie Wood Road, Waltham Forest, London E4 9DD
020 8523 7913 | school@awp.waltham.sch.uk | www.ainsliewood.co.uk



1. Purpose and scope

Ainslie Wood Primary School recognises online safety as an integral part of safeguarding, not a separate technical issue. This policy sets out how the school will safeguard children and adults when using digital technology, while enabling pupils to benefit from technology safely, responsibly and positively.

The policy is based on the August 2026 SWGfL School Online Safety Policy template and reflects Keeping Children Safe in Education (KCSIE) 2026 and current Department for Education digital and technology standards. It should be read alongside the school's Child Protection and Safeguarding, Behaviour, Anti-Bullying, Staff Code of Conduct, Data Protection, Acceptable Use and related technology policies.

It applies to staff, pupils, governors, volunteers, parents/carers, visitors and community users who access school digital systems. It applies to school systems used on or off site and to personal devices used on site where permitted. Where an online incident outside school affects a child's safety, wellbeing, behaviour or the school community, the school may respond under this and related policies.

2. Our approach to online safety

Online safety is a running and interrelated theme through Ainslie Wood's safeguarding practice. Our approach reflects the school values of Safe, Kind and Responsible and combines education, appropriate technology, clear reporting routes, effective supervision and proportionate responses to incidents.

We recognise the four broad areas of online risk identified in KCSIE:

- Content – exposure to illegal, inappropriate or harmful material, including pornography, racism, misogyny, self-harm and suicide content, antisemitism, radicalisation, extremism, extreme violence, misinformation, disinformation and conspiracy theories.
- Contact – harmful interaction with other users or generative AI applications, including peer pressure, grooming, exploitation, commercial targeting and adults posing as children or young adults.
- Conduct – behaviour that increases the likelihood of harm, including online bullying and making, sending or receiving explicit images, including AI-generated or manipulated images.
- Commerce – risks including gambling, inappropriate advertising, phishing, scams and other financial harms.

3. Policy development, monitoring and review

The Governing Body has strategic oversight. The Headteacher, DSL, senior leaders and technical support work together to implement and review the policy. Pupil, staff and parent/carer voice will be used where appropriate to understand emerging risks and the effectiveness of the school's approach.

The policy will be reviewed at least annually and sooner where there is:

- a significant safeguarding or online safety incident
- a material change to technology, systems or working practices
- new or substantially changed statutory guidance
- introduction of new technologies, including generative AI tools
- evidence from filtering, monitoring, audits or pupil voice that current arrangements need adjustment

The impact of the policy will be evaluated through incident records, safeguarding records, filtering and monitoring information, annual reviews, technical checks, curriculum review, staff training and stakeholder feedback.

4. Roles and responsibilities

Governing Body

- has overall strategic responsibility for ensuring appropriate filtering and monitoring systems are in place and effective
- approves and reviews this policy and seeks assurance that statutory safeguarding expectations are met
- ensures online safety is considered within safeguarding, curriculum, risk management and digital strategy
- receives assurance from leaders about the annual filtering and monitoring review and actions arising
- ensures governors receive appropriate safeguarding and online safety information and training

Headteacher and senior leaders

- set a culture in which online safety is understood as everybody's safeguarding responsibility
- ensure staff understand their roles and receive appropriate training, including filtering and monitoring expectations
- ensure children are taught how to keep themselves and others safe online, with teaching adapted to age, need and vulnerability
- ensure the DSL, IT support and relevant staff have sufficient authority, knowledge and access to carry out their roles
- ensure serious incidents are escalated appropriately and that lessons learned inform future practice

Designated Safeguarding Lead (DSL)

The DSL has lead responsibility for safeguarding and child protection, including online safety and understanding the school's filtering and monitoring arrangements. The DSL will:

- coordinate the safeguarding response to online safety concerns and ensure concerns are recorded and acted upon
- work closely with the Headteacher, senior leaders and IT support on filtering, monitoring and emerging online risks
- ensure online safety is reflected in staff safeguarding training and updates
- consider the needs of vulnerable pupils, including SEND, EAL and pupils with known safeguarding vulnerabilities
- refer to external agencies where thresholds are met and ensure immediate risks are managed promptly

IT support / technical provider

- maintains secure, appropriately configured systems and supports the school to meet DfE technical standards
- supports effective filtering and monitoring across relevant users, devices and networks
- provides leaders with information needed to understand system coverage, limitations, alerts and risks
- implements authorised changes promptly and records significant configuration changes
- works with the DSL and senior leaders when technical activity indicates a safeguarding concern

All staff and volunteers

- model safe, professional and responsible use of technology
- follow the Staff Acceptable Use Agreement, Staff Code of Conduct and safeguarding procedures
- maintain active supervision when pupils use technology and remain alert to online harm
- report safeguarding concerns immediately to the DSL or a deputy DSL; technical concerns are reported through the school's agreed route
- never investigate a safeguarding concern themselves or view, copy or forward illegal or indecent imagery unless specifically required by an authorised safeguarding process

- protect passwords, accounts, devices and personal information and report suspected breaches promptly

Pupils

Pupils are taught to use technology in ways that are Safe, Kind and Responsible. Expectations are age-appropriate and are reinforced through the curriculum, assemblies, class practice and responses to incidents.

5. Acceptable use of technology

Access to school technology is provided for educational and legitimate professional purposes. Users must follow the relevant Acceptable Use Agreement (AUA). The school may apply proportionate restrictions where use creates a safeguarding, security, legal or operational risk.

- Users must keep passwords and authentication details secure and must not use another person's account.
- Personal data and confidential information must only be stored, shared or processed through approved systems.
- School systems must not be used to access, create, store or distribute illegal, abusive, discriminatory, sexually explicit or otherwise harmful material.
- Attempts to bypass filtering, security or monitoring controls are prohibited unless specifically authorised for legitimate technical testing.
- Personal devices may only be used in accordance with school rules and professional expectations.
- Images, video or audio of pupils may only be created, stored and shared for authorised purposes and in accordance with consent, safeguarding and data-protection requirements.
- Copyright, licensing and intellectual-property requirements must be respected.

6. Reporting and responding to online safety concerns

Safeguarding concerns must be reported promptly. Staff should not wait for proof before raising a concern.

Concern	Immediate route
A child may be at risk of harm, exploitation, abuse, self-harm, radicalisation or other safeguarding harm	DSL / deputy DSL immediately; follow safeguarding procedures
Immediate danger or suspected serious crime	DSL / Headteacher and emergency services or police as appropriate
Illegal or suspected child sexual abuse material	Do not copy, forward or unnecessarily view; secure the situation and contact the DSL immediately
Cyber-security or data breach	Report immediately through the school's technical/data-breach route and inform senior leadership/DSL where safeguarding may be involved
Low-level inappropriate pupil use	Manage proportionately under behaviour/online safety procedures and record/escalate if safeguarding concerns emerge
Concern about a member of staff	Follow allegations/low-level concerns procedures; do not investigate independently

Responses will be child-centred and proportionate. The school will consider the child's age, developmental stage, SEND, vulnerability, intent, impact, recurrence, coercion or exploitation, and whether the behaviour indicates wider safeguarding concerns.

Where appropriate, parents/carers will be informed and involved. Information may be shared without consent where necessary to safeguard a child or meet a legal obligation.

7. Child-on-child online abuse and harmful sexual behaviour

Online abuse between children is taken seriously and is never dismissed as banter or an inevitable part of growing up. This includes online bullying, harassment, sexual harassment, coercion, threatening behaviour, sharing nudes or semi-nudes, upskirting, sexualised comments, exploitation and AI-generated or manipulated sexual imagery.

The school will respond under its safeguarding and behaviour procedures, support affected children, consider risk to others, preserve appropriate evidence without unnecessary viewing or duplication, and make referrals where required.

8. Artificial intelligence (AI)

Ainslie Wood recognises the educational and administrative potential of AI alongside risks relating to safeguarding, privacy, misinformation, bias, academic integrity, intellectual property, security and over-reliance.

- Only school-approved AI tools may be used for professional purposes where approval is required.
- Personal, special-category, safeguarding or otherwise confidential information must not be entered into unapproved AI systems.
- AI output must be critically checked by a human; AI must not be treated as an authoritative source or substitute for professional judgement.
- Pupils will receive age-appropriate teaching about AI-generated content, misinformation, manipulation, privacy, bias and safe interaction with conversational or generative systems.
- The school will assess safeguarding and data-protection risks before introducing AI products, including whether filtering and monitoring can address dynamic or personalised AI-generated content.
- AI must not be used to create harmful, humiliating, deceptive or sexualised content about another person.

9. Online safety education

Online safety education is progressive, age-appropriate and embedded across computing, RSHE/PSHE and wider curriculum opportunities. Teaching will help pupils understand both risk and resilience rather than relying on restriction alone.

- privacy, passwords, personal information and digital footprints
- recognising unreliable information, misinformation, disinformation and scams
- healthy online relationships, consent, respectful communication and reporting
- online bullying, discrimination, hate and harmful sexual behaviour
- grooming, exploitation, coercion and unsafe contact
- the risks and opportunities of AI and manipulated content
- copyright, ownership and responsible creation of digital content
- where and how to seek help, including trusted adults and reporting tools

10. Staff training and professional practice

All staff receive safeguarding training that includes online safety and the school's expectations for filtering and monitoring. New staff receive relevant information at induction. Updates are provided in response to emerging risks, incidents and changes in guidance.

Staff must maintain professional boundaries online. Personal accounts must not be used to communicate privately with current pupils. Staff should consider privacy, reputation and safeguarding implications when identifying themselves publicly as associated with the school.

11. Working with parents and carers

The school will support parents and carers with accessible, proportionate information about online safety, emerging risks and school expectations. Parents/carers are encouraged to report concerns and to work with the school when online behaviour outside school affects a child's safety or wellbeing.

12. Filtering and monitoring

Filtering and monitoring are safeguarding measures. Filtering is preventative and restricts access to illegal, inappropriate or harmful content. Monitoring is reactive and helps identify concerning activity so that it can be reviewed and acted upon.

Ainslie Wood's filtering and monitoring provision is supported through its technical services, including LGfL provision where applicable. The existence of a filtering service alone is not treated as assurance of compliance: the school will review its own configuration, coverage, monitoring arrangements, alert handling and risk profile.

- The Governing Body retains overall strategic responsibility and seeks assurance that appropriate systems are in place.
- A nominated senior leader, the DSL, IT support and the responsible governor will participate in the review of provision.
- Filtering and monitoring provision will be formally reviewed at least once each academic year and additionally following significant risks, incidents, system changes or introduction of new technology.
- The review will consider pupil risk profiles, including age, SEND, EAL and known safeguarding vulnerabilities; school use of technology; AI; off-site use; BYOD where relevant; curriculum needs; incidents; and technical limitations.
- Filtering should apply appropriately across school-managed devices, users and networks and should not unreasonably restrict teaching and learning.
- Monitoring will include appropriate in-person supervision. Where technical monitoring is used, high-risk concerns should be capable of prompt escalation and routine reports should be reviewed at an agreed frequency.
- Actions, exceptions and significant changes will be authorised and recorded.
- Safeguarding matters identified through monitoring are the responsibility of the DSL.

13. Technical security and cyber security

- Systems, accounts and devices will be configured and maintained to reduce the risk of unauthorised access, malware, phishing, ransomware and data loss.
- Access rights will be proportionate to role and reviewed when staff or pupils change roles or leave.
- Security updates and supported software will be managed in line with current technical standards.
- Backups, recovery arrangements and incident-response procedures will be maintained and tested appropriately.
- Staff and pupils will receive age/role-appropriate education about phishing, scams, credential theft and other cyber risks.
- Significant cyber incidents will be escalated to relevant technical, safeguarding, data-protection and external agencies as appropriate.

14. Data protection and privacy

Personal data will be processed lawfully, fairly, transparently and securely in accordance with UK data-protection law and school procedures. New technologies or high-risk processing will be assessed before use, including through a Data Protection Impact Assessment where required.

Monitoring must be proportionate and transparent. Users will be informed that school systems and devices may be filtered and monitored. Safeguarding information will only be shared with those who need it for a legitimate purpose.

15. Devices, mobile phones and searching

Use of personal devices and mobile phones is governed by school rules and the Behaviour Policy. Any searching, confiscation, examination or deletion of data from an electronic device will only take place where lawful, necessary and proportionate, by appropriately authorised staff and in line with DfE guidance and safeguarding procedures.

Where a device may contain evidence of a criminal offence or illegal imagery, staff will preserve the situation and seek safeguarding/police advice rather than unnecessarily accessing, copying or deleting material.

16. Public online communications and social media

- Official school accounts and websites will be managed by authorised staff with appropriate security and oversight.
- Published images and information will be selected carefully to reduce safeguarding, privacy, location and image-manipulation risks.
- Staff must not communicate with current pupils through personal social-media accounts.
- Complaints raised online will be directed to the school's formal complaints procedure; abusive or threatening content may be recorded, reported, blocked or referred as appropriate.

17. Responding to misuse

The school's response to misuse will be proportionate, restorative where appropriate and consistent with safeguarding and behaviour procedures. Sanctions will not replace safeguarding action where a child may be at risk. Incidents will be reviewed for patterns, vulnerabilities, training needs and any required changes to technical controls or curriculum provision.

18. Related policies and documents

- Child Protection and Safeguarding Policy
- Relationship and Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Data Protection and Privacy Notices
- Acceptable Use Agreements
- Filtering and Monitoring procedures/audit
- Technical Security and Cyber Security procedures
- Mobile phone / personal device expectations
- Whistleblowing Policy
- Complaints Policy

19. Key external framework

This policy has been customised from the SWGfL School Online Safety Policy Template updated August 2026. It reflects, in particular, Keeping Children Safe in Education 2026 and the Department for Education's current digital and technology standards, including filtering and monitoring, cyber security and digital leadership/governance. The school will use current statutory and government guidance when interpreting this policy.

Appendix 1 – Quick staff reporting guide

If you see / hear / discover...	Do...	Do not...
A pupil discloses online harm	Listen, reassure appropriately, record and report to a DSL immediately.	Promise secrecy, investigate, or contact alleged perpetrator.
Concerning search / monitoring alert	Preserve relevant factual information and pass to DSL through agreed route.	Assume the filter/monitor has dealt with it.
Nude/semi-nude or suspected illegal image	Stop unnecessary viewing; contact DSL immediately.	Copy, forward, print, screenshot or ask others to view.
Cyber/data incident	Report immediately through technical/data route; flag safeguarding implications.	Try to conceal or privately fix a serious breach.
AI-generated harmful content	Treat the impact as real; preserve only necessary evidence and report appropriately.	Dismiss it because it is 'fake' or AI-generated.

Appendix 2 – Pupil expectations: Safe, Kind, Responsible

SAFE

- I keep passwords and personal information private.
- I tell a trusted adult if something online worries, frightens or pressures me.
- I do not try to bypass school safety or security systems.
- I check before sharing images, information or content about other people.

KIND

- I communicate respectfully online as well as face to face.
- I do not create, share or encourage content intended to embarrass, threaten, bully or sexualise someone.
- I remember that edited or AI-generated content can still cause real harm.

RESPONSIBLE

- I use school technology for the purpose I have been given.
- I think critically about whether online information is true, reliable and appropriate.
- I respect copyright and acknowledge sources where appropriate.
- I report mistakes or problems rather than hiding them.

Appendix 3 – Annual filtering and monitoring assurance prompts

The annual review should record evidence and actions against, at minimum, the following prompts:

- Are named SLT, DSL, governor and IT responsibilities clear?
- What filtering and monitoring systems are in place, on which networks/devices/users, and what are their limitations?
- Are IWF/CTIRU protections and other required provider controls in place and not locally disableable?
- Are pupil and staff filtering profiles appropriately differentiated?
- How are unmanaged/BYOD and guest devices handled where applicable?
- How are real-time, dynamic, personalised and AI-generated content risks addressed?

- How are routine monitoring reports reviewed and how are high-risk alerts escalated?
- Are incidents, actions, exceptions and configuration changes recorded?
- Does the provision reflect the school's current pupil risk profile, including SEND, EAL and safeguarding vulnerabilities?
- Have recent incidents, curriculum needs, new technology, software/network changes or off-site use changed the risk profile?
- Do staff understand classroom supervision and reporting expectations?
- Have findings and actions been reported to the Governing Body and tracked to completion?

Approval and review record

Approved by	Governing Body – date to be confirmed
Policy owner	Headteacher
Operational safeguarding lead	Designated Safeguarding Lead
Next planned review	September 2027, or sooner if required