

THE MOUNT SCHOOL

ONLINE SAFETY POLICY

2026–2027

Version	2.0
Policy writer	Euan Burton-Smith
Last updated	August 2026
Effective from	1 September 2026
Review date	August 2027
Approved by	Chris Sellers - Director / Proprietor

This policy retains and develops the School's existing online-safety arrangements, including Pearce IT support, NetSupport DNA monitoring and the Ubiquiti UDM Pro firewall. It is aligned with the Safeguarding & Child Protection Policy 2026–2027 and incorporates the substantive online-safety changes in KCSIE 2026.

Contents

- 1. Aims and safeguarding principles
- 2. Statutory and guidance framework
- 3. The four areas of online risk
- 4. Roles and responsibilities
- 5. The Mount technical safeguarding arrangements
- 6. Filtering and monitoring governance
- 7. Annual filtering and monitoring effectiveness review
- 8. Routine filtering and monitoring checks
- 9. Staff responsibilities for monitoring
- 10. Educating pupils about online safety
- 11. Generative AI, deepfakes and AI-generated content
- 12. Nude, semi-nude and intimate imagery
- 13. Pornography, extreme content and harmful influencers
- 14. Online child-on-child abuse and cyber-bullying
- 15. Grooming, exploitation and harmful contact
- 16. Cybercrime
- 17. Commerce, scams and financial exploitation
- 18. Online radicalisation and Prevent
- 19. SEND, age and vulnerability
- 20. Educating and supporting parents
- 21. Acceptable use of School technology
- 22. Pupils' mobile and connected devices
- 23. Staff use of School devices outside School
- 24. Personal devices, BYOD and wearable technology
- 25. Social media, messaging and communication
- 26. Searching, confiscation and electronic evidence
- 27. Responding to an online-safety incident
- 28. Illegal content and reporting
- 29. Data protection, monitoring data and privacy
- 30. Cyber security and information security
- 31. Remote learning and off-site access
- 32. Visitors, contractors and external providers
- 33. Staff training
- 34. Pupil voice and review of emerging risk
- 35. Monitoring, audit and inspection readiness
- 36. Related policies and external support
- Appendix A – Staff online-safety response guide
- Appendix B – Annual filtering and monitoring review record
- Appendix C – Routine filtering and monitoring check record
- Appendix D – Online-safety incident decision guide

1. Aims and safeguarding principles

The Mount School recognises that technology is integral to children's education, communication and everyday life. Online safety is therefore an integral part of safeguarding and child protection rather than a separate technical issue.

- protect and educate pupils, staff and the wider School community in their use of technology;
- provide appropriate filtering and monitoring without unreasonably restricting teaching and learning;
- identify, intervene in and escalate online-safety concerns promptly;
- teach children how to recognise risk, seek help and behave safely and respectfully online;
- ensure that safeguarding arrangements keep pace with changing technology, including generative artificial intelligence;
- ensure staff understand that technical systems support, but do not replace, professional vigilance and supervision; and
- maintain clear governance, accountability, records and review arrangements.

The School maintains an attitude that online harm can happen here. Harm may occur wholly online, wholly offline or through a combination of the two.

2. Statutory and guidance framework

- Keeping Children Safe in Education 2026 (KCSIE), particularly the online-safety, filtering and monitoring provisions;
- the Education (Independent School Standards) Regulations 2014, including the safeguarding and welfare standard;
- DfE Independent School Standards guidance, April 2026;
- the EYFS statutory framework where applicable;
- DfE Teaching online safety in schools guidance;
- DfE Meeting digital and technology standards in schools and colleges, including the filtering and monitoring and cyber-security core standards;
- DfE statutory guidance on mobile phones in schools, effective from September 2026;
- current DfE guidance on generative AI and product safety;
- Searching, screening and confiscation guidance;
- the Prevent duty guidance;
- the Data Protection Act 2018 and UK GDPR;
- the Equality Act 2010; and
- relevant UK Council for Internet Safety and Internet Watch Foundation guidance.

Where technology or guidance changes during the life of this policy, the School will follow the current statutory requirement and update operational arrangements without waiting for the annual policy review.

3. The four areas of online risk

The School uses the four Cs framework: content, contact, conduct and commerce.

3.1 Content

Content risks include illegal, inappropriate or harmful material such as pornography, extreme sexual or physical violence, racism, misogyny, self-harm and suicide content, antisemitism, radicalisation and extremism, disinformation, harmful challenges, material that normalises abuse, and harmful or inappropriate AI-generated content.

3.2 Contact

Contact risks arise from harmful interaction with other users, including peer pressure, grooming, adults posing as children or young adults, sexual or criminal exploitation, financial exploitation, coercive contact, harmful interactions through games or social media, and potentially harmful interactions with AI systems.

3.3 Conduct

Conduct risks concern behaviour that increases the likelihood of harm, including cyber-bullying, harassment, abusive communication, unsafe disclosure of personal information, making or sharing nude/semi-nude or intimate imagery, livestreaming, cybercrime, and misuse of generative AI.

3.4 Commerce

Commerce risks include online gambling or gambling-style features, inappropriate advertising, phishing, scams, fraud, in-app purchasing pressure, financial exploitation and pressure to transfer money or provide access to accounts.

4. Roles and responsibilities

4.1 Director / Proprietor – Chris Sellers

- hold strategic responsibility for ensuring appropriate filtering and monitoring systems are in place;
- ensure the effectiveness of filtering and monitoring provision is reviewed at least annually;
- participate in or receive the recorded outcome of the annual review and ensure actions are completed;
- hold the Headteacher and DSL to account for effective implementation of this policy;
- ensure staff understand their filtering and monitoring responsibilities;
- consider online-safety risks in strategic decisions, procurement and safeguarding assurance; and
- ensure the School's online-safety arrangements meet the Independent School Standards and have regard to KCSIE.

4.2 Headteacher / DSL – Euan Burton-Smith

- take lead responsibility for online safety as part of safeguarding;
- understand the filtering and monitoring systems and processes in place;
- work with the Director, DDSL, responsible senior leader and Pearce IT to review effectiveness;
- ensure safeguarding alerts and online incidents are triaged, recorded and acted upon;
- ensure staff receive appropriate online-safety training and updates;
- consider whether online incidents require child-protection, behaviour, police, Prevent or other external action;
- ensure curriculum provision reflects current and emerging risks; and
- report significant themes, risks and assurance information to the Director.

4.3 Deputy DSL – Natalie Sandford

The DDSL supports the DSL, receives and responds to safeguarding alerts, acts when the DSL is unavailable, contributes to filtering and monitoring review and ensures urgent alerts do not remain unattended.

4.4 Pearce IT

- maintain and support appropriate filtering and monitoring systems;
- maintain the security of the School's ICT infrastructure and protection against malware and cyber threats;
- support the configuration and maintenance of the Ubiquiti UDM Pro firewall and relevant filtering controls;
- support NetSupport DNA and other monitoring arrangements used by the School;
- ensure systems are updated and technical changes do not inadvertently disable filtering, monitoring or security;
- provide technical information and assurance for the annual review and routine checks;
- support investigation of technical incidents while respecting safeguarding confidentiality and data-protection requirements; and
- escalate technical or safeguarding concerns promptly to authorised School staff.

4.5 All staff, contractors and volunteers

- understand and implement this policy and applicable Acceptable Use arrangements;
- actively supervise children's use of technology where this forms part of their role;
- recognise that filtering may fail and monitoring may not detect every risk;

- report online-safety and safeguarding concerns immediately through the School's safeguarding procedure;
- not assume that a technical alert has already informed the DSL;
- not deliberately bypass or disable filtering, monitoring or security controls;
- use School systems and devices in accordance with professional standards; and
- challenge unsafe or abusive online behaviour in accordance with safeguarding and behaviour procedures.

5. The Mount technical safeguarding arrangements

The School's existing technical arrangements are retained and form part of its safeguarding system.

5.1 NetSupport DNA

Devices accessed by pupils are monitored through NetSupport DNA. The system is used to identify words, searches or activity that may indicate safeguarding or online-safety risk. Alerts are assessed according to risk. High-risk alerts are escalated to authorised safeguarding staff and monitoring reports are reviewed by the School.

The School will not rely on automated categorisation alone. An alert must be considered in context, including the pupil's age, SEND, curriculum activity, search terms, surrounding activity and any existing safeguarding information.

5.2 Ubiquiti UDM Pro firewall

Devices accessing the School network are filtered through the Ubiquiti UDM Pro firewall and associated filtering/security configuration. The system is intended to prevent access to illegal, inappropriate and potentially harmful material while permitting legitimate educational use.

5.3 Pearce IT support

Pearce IT provides technical support and assurance. Safeguarding accountability remains with The Mount School and its proprietor; it is not outsourced to the IT provider.

5.4 Email / communication monitoring

Where School communication systems identify suspicious or potentially harmful pupil messages or activity, alerts will be referred to the DSL/DDSL for safeguarding assessment. The School will keep the exact technical route under review as systems change.

6. Filtering and monitoring governance

Filtering is preventative: it seeks to prevent users accessing illegal, inappropriate or potentially harmful online content. Monitoring is reactive: it identifies or records user activity so that concerning behaviour can be reviewed and acted upon.

The School will ensure that filtering and monitoring arrangements are appropriate for its pupils, including their ages, SEND, EAL and other vulnerabilities, the technology used, locations in which technology is used, remote access arrangements and the balance between safeguarding and legitimate learning.

Filtering and monitoring must address, so far as reasonably possible, text, images, video and other formats, including risks arising from dynamic, personalised and AI-generated content.

Access to monitoring information will be restricted to authorised staff. Staff with access will receive appropriate safeguarding and system training.

7. Annual filtering and monitoring effectiveness review

The effectiveness of filtering and monitoring provision will be reviewed at least once every academic year. The review will be led by relevant members of the senior leadership team with the DSL and Pearce IT/IT support and will involve the Director as the responsible proprietor.

- current filtering and monitoring provision and whether it meets the School's needs;
- the pupil risk profile, including age, SEND, EAL and known safeguarding vulnerabilities;

- whether systems operate across all relevant School-managed devices and locations;
- whether remote, cloud-based and off-site use creates gaps;
- whether filtering can address dynamic, personalised and AI-generated content;
- the effectiveness, timeliness and accuracy of monitoring alerts and escalation;
- over-blocking or under-blocking and the impact on teaching and learning;
- staff understanding of responsibilities;
- recent incidents, attempted bypasses and emerging risks;
- changes to devices, software, network configuration, BYOD or generative-AI tools;
- privacy, proportionality and data-protection arrangements; and
- actions, owners and timescales arising from the review.

The outcome and actions will be recorded and retained as safeguarding assurance evidence. The review will also be repeated or revisited when a significant safeguarding risk is identified, working practice changes, new technology is introduced, major software updates occur or network/device configuration changes.

8. Routine filtering and monitoring checks

In addition to the annual effectiveness review, the responsible senior leader, DSL and Pearce IT will ensure that checks are conducted and recorded to confirm that filtering and monitoring systems are working as intended.

- test representative pupil devices and user profiles;
- test different relevant physical locations and network connections;
- confirm filtering operates on new or reconfigured School-managed devices;
- confirm NetSupport DNA or equivalent monitoring agents are active where expected;
- confirm alerts reach the correct authorised recipients;
- sample whether categorisation and escalation are functioning appropriately;
- check that legitimate safeguarding or curriculum sites are not unreasonably blocked;
- check for known methods of bypass, including proxy/VPN or browser-based workarounds where relevant;
- confirm changes made by IT support have not created gaps; and
- record date, tester, scope, outcome, defect and remedial action.

A defect that creates an immediate safeguarding gap will be escalated to the DSL and Headteacher without delay and temporary controls will be put in place while the defect is remedied.

9. Staff responsibilities for monitoring

Technical monitoring is only one part of the School's monitoring strategy. Staff are expected to use professional observation and classroom supervision, including viewing screens where appropriate, noticing changes in behaviour and responding when pupils seek help.

Staff must not ignore concerning activity because a site was accessible through the School's filter. Accessibility does not mean that content is safe or authorised.

10. Educating pupils about online safety

Online safety is taught through computing, relationships/health education, PSHE, assemblies and wider curriculum opportunities. Teaching will be age- and developmentally appropriate and revisited as technology and risks change.

- safe and respectful use of technology and personal information;
- how online identity may differ from offline identity and how people may pretend to be someone else;
- healthy and respectful online relationships and boundaries;
- how information and data are shared, copied and used;
- how to identify harmful content and contact and where to seek help;
- image sharing, consent and the permanence and replicability of digital material;
- deepfakes, manipulated media and AI-generated imagery;
- the risks of pornography and extreme sexual or physical content in an age-appropriate way;

- misogynistic and other harmful influencers and how algorithms may reinforce harmful material;
- grooming, exploitation, coercion and scams;
- cyber-bullying and discriminatory abuse;
- cybercrime and lawful/ethical use of technical skills;
- how generative AI works at an age-appropriate level, including limitations, hallucination, bias, privacy and safe prompting; and
- the importance of telling a trusted adult when something online worries, frightens or pressures them.

Pupils will be taught that reporting an online concern is the right thing to do and that they will be listened to rather than automatically blamed for having encountered harmful content.

11. Generative AI, deepfakes and AI-generated content

Generative AI can create or alter text, images, audio, video and simulated interactions. It creates educational opportunities but also safeguarding, privacy, accuracy and security risks.

- AI-generated intimate or sexual images of children;
- deepfakes or altered images used to humiliate, bully, coerce or sexualise;
- harmful simulated conversations, including sexual, violent, self-harm or manipulative interactions;
- AI-generated misinformation, impersonation or fraudulent content;
- uploading personal, confidential or safeguarding information to public AI systems;
- bias, inaccurate information and fabricated sources;
- circumvention of filtering or age restrictions; and
- use of AI to facilitate bullying, exploitation, cheating, cybercrime or other harmful behaviour.

The School will risk assess any generative-AI product it introduces, including safeguarding, filtering/monitoring, privacy, age suitability, terms of service and data processing. Staff must use only School-approved systems for School business where approval is required.

AI-generated content will be judged by its impact and safeguarding context, not dismissed because it is artificial.

12. Nude, semi-nude and intimate imagery

Every incident involving the making, requesting, receiving, possession or sharing of nude, semi-nude or other intimate imagery by pupils requires a safeguarding response. This includes photographs, videos, livestreams, digitally altered material, deepfakes and wholly AI-generated intimate images.

Staff must not routinely view, copy, print, save, forward or ask a child to send intimate imagery. The DSL will follow current safeguarding guidance and determine what evidence should be preserved and whether police or other agencies are required.

A pupil who reports an incident will be supported and must not be made to feel that they caused the problem by reporting it.

13. Pornography, extreme content and harmful influencers

The School recognises the potential impact of pornography, extreme sexual or physical violence and online personalities who promote misogyny, hatred, coercion, violence or other harmful attitudes.

Teaching will be age-appropriate and focused on safety, respect, healthy relationships, critical thinking and help-seeking. Staff who become aware that a child is accessing or being exposed to such content will consider the child's age, frequency, context, coercion, emotional impact and wider safeguarding picture and report concerns to the DSL.

14. Online child-on-child abuse and cyber-bullying

Online abuse can occur independently or alongside face-to-face harm. It can include cyber-bullying, harassment, sexual harassment, threats, hate speech, impersonation, coercion, exclusion, image-based abuse, doxxing, abusive group chats and coordinated attacks.

Cyber-bullying is not limited to repetitive behaviour where the impact or nature of a single online act is sufficiently harmful. The School will respond under safeguarding and behaviour procedures according to context.

Where illegal, inappropriate or harmful material has spread among pupils, the School will seek to contain further distribution, support affected children and consider external reporting.

15. Grooming, exploitation and harmful contact

Staff will be alert to adults or peers using games, social media, messaging, livestreaming, AI or other platforms to build trust, manipulate, coerce or exploit children for sexual, criminal, financial or other purposes.

- secretive or rapidly intensifying online relationships;
- requests to move to encrypted/private channels;
- gifts, money, game currency or other inducements;
- requests for images, livestreaming or sexual activity;
- threats to share material;
- pressure to move money, use bank accounts or commit fraud;
- older or controlling contacts; and
- changes in behaviour, attendance, sleep or emotional wellbeing associated with online contact.

16. Cybercrime

Cyber-dependent crime includes unauthorised access to computers or accounts, creation or use of malware, denial-of-service activity and other offences that can only be committed using technology.

The School will distinguish healthy technical curiosity from deliberate harmful or unlawful conduct and will provide positive pathways for pupils with advanced technical interests. Safeguarding or police advice will be sought where necessary.

17. Commerce, scams and financial exploitation

Pupils will be taught about phishing, fraudulent messages, fake shops, in-app pressure, gambling-style features, account theft and financial scams. Concerns about children being coerced to move money, surrender account access or participate in fraud will be treated as potential financial/criminal exploitation and reported to the DSL.

18. Online radicalisation and Prevent

Filtering arrangements will seek to restrict access to terrorist and extremist material while staff remain alert to radicalisation through social media, gaming, messaging and other online communities.

Concerns about possible radicalisation must be reported to the DSL/Prevent Lead and managed under the Safeguarding & Child Protection Policy and local Prevent/Channel arrangements.

19. SEND, age and vulnerability

Online-safety provision will consider children's age, developmental stage, SEND, communication needs, EAL and known vulnerabilities. Children with SEND may face additional risks through social isolation, difficulty recognising manipulation, literal interpretation, a strong desire for friendship or difficulty reporting harm.

Filtering and monitoring will not be configured in a way that unnecessarily prevents access to legitimate accessibility tools. Reasonable adjustments and individual online-safety plans may be used where appropriate.

20. Educating and supporting parents

The School will raise parent/carer awareness through communications, meetings, curriculum information and signposting. Information may cover parental controls, age ratings, social media, gaming, image sharing, scams, AI, harmful content and how to report concerns.

Parents should raise online-safety concerns with the School promptly. A safeguarding concern should be reported to the DSL rather than waiting for a routine meeting.

21. Acceptable use of School technology

Pupils, staff, volunteers and other users will follow the School's Acceptable Use arrangements. School internet and systems are provided principally for educational and legitimate professional purposes.

The School may monitor use of its systems for safeguarding, security, operational and lawful purposes. Monitoring will be proportionate and transparent and will be described in relevant privacy information.

- attempting to bypass filtering or monitoring;
- using proxy, VPN or anonymising services without authorisation;
- accessing or sharing illegal, abusive or inappropriate material;
- bullying, harassment or discriminatory communication;
- sharing passwords or attempting to access another user's account;
- installing unauthorised software;
- uploading confidential School information to unauthorised AI or cloud services; and
- using School technology for unlawful or seriously inappropriate purposes.

22. Pupils' mobile and connected devices

The School's current rule is that pupils should not bring or use personal internet-capable mobile devices in School unless specifically authorised for an identified SEND, medical or educational reason. This is implemented alongside the separate Mobile Phone Policy and the statutory mobile-phone guidance effective from September 2026.

Where an authorised device is required, a risk assessment or agreed arrangement will specify permitted use, storage and any safeguarding controls. Unauthorised devices may be confiscated in accordance with School policy and current legal guidance.

23. Staff use of School devices outside School

- keep devices password/PIN protected and secure;
- not share passwords or accounts;
- use approved software and services;
- not install unauthorised software;
- protect confidential and safeguarding information from family members or other third parties;
- use secure connections and follow School guidance on public Wi-Fi/VPN use;
- report loss, theft, malware, suspicious access or data breach immediately; and
- return devices for updates or technical checks when requested.

School devices may be used for legitimate School work. Any previous blanket statement that work devices may be used 'solely for work activities' will be interpreted through the current Acceptable Use rules rather than used to obstruct reasonable authorised practice.

24. Personal devices, BYOD and wearable technology

Personal devices used on School premises or for School business are subject to the Mobile Phone, EYFS Mobile Devices, Staff Code of Conduct and BYOD arrangements.

Personal devices must not be used to photograph or record pupils unless expressly authorised under a specific School procedure. In the EYFS, image-capable personal devices and connected/wearable technology are subject to particularly strict controls.

Any BYOD arrangement must consider filtering, monitoring, data protection, network security and safeguarding before access is granted.

25. Social media, messaging and communication

Staff must use authorised professional channels to communicate with pupils and parents and maintain appropriate boundaries. Personal social-media accounts and private messaging must not be used to establish inappropriate direct relationships with pupils.

Pupil use of messaging, group chats and social media that creates a safeguarding concern may be addressed even where activity occurred outside School, particularly where it affects pupils' safety or welfare in School.

26. Searching, confiscation and electronic evidence

Any search of a pupil or device will be carried out in accordance with current DfE searching, screening and confiscation guidance and the School's Behaviour Policy.

The previous policy wording suggesting that staff can simply decide to delete or retain any inappropriate file is replaced by a safeguarding-led approach. Staff must consider whether material may be evidence of a safeguarding concern or criminal offence and must involve the DSL before viewing, deleting, copying or forwarding sensitive content wherever practicable.

Intimate imagery must be handled under the specific safeguarding rules in section 12.

27. Responding to an online-safety incident

Incident	Immediate route	Record	Possible additional action
Safeguarding concern about a child	DSL/DDSL immediately	Safeguarding system	Social care/police/other agency as appropriate
Immediate danger / serious threat	999 plus DSL	Safeguarding and incident record	Emergency response
Intimate image / deepfake / AI sexual image	DSL/DDSL immediately	Safeguarding system	UKCIS/police/IWF route as appropriate
Cyber-bullying / child-on-child abuse	DSL where safeguarding; behaviour route also	Safeguarding/behaviour records	Risk assessment/support/sanction
Filtering/monitoring alert	Authorised DSL/DDSL review	Monitoring/safeguarding record as appropriate	Escalation, welfare check, technical action
Cyber-security incident / suspected breach	Pearce IT + Head/DSL/DPO as relevant	Security/data-breach record	ICO/police/NCSC as appropriate
Staff misuse / adult safeguarding concern	Headteacher / adult-concern route	Safeguarding/HR record	LADO where harm threshold may be met

Urgent safeguarding concerns must not be left solely in an email inbox or technical alert queue. Staff must make a direct report.

28. Illegal content and reporting

The DSL will consider police involvement where an online incident may involve a crime, but the School will not use a blanket rule that every potentially criminal matter must automatically be reported to police without considering current safeguarding guidance.

Suspected criminal online child sexual abuse content may be reported to the Internet Watch Foundation through the appropriate route. Staff must not search for, download or redistribute illegal material in order to make a report.

29. Data protection, monitoring data and privacy

Filtering and monitoring involves processing personal data. The School will ensure this is lawful, proportionate and transparent.

- access to monitoring alerts and reports is restricted to authorised persons;
- staff with access receive appropriate training;
- monitoring records are retained in accordance with safeguarding/data-retention procedures;
- privacy notices explain, as appropriate, what is monitored, why, who can access information and how long it is kept;
- third-party provider privacy and processing arrangements are reviewed;
- a Data Protection Impact Assessment is completed before introducing a new monitoring system or making a significant change where required; and
- automated or AI-supported monitoring is used proportionately and does not replace human decision-making.

30. Cyber security and information security

Cyber security is linked to safeguarding because compromised systems can expose sensitive pupil information, disrupt safeguarding systems and create opportunities for harm.

- appropriately configured firewall controls;
- centrally managed and updated anti-malware protection;
- secure user accounts and passwords;
- multi-factor authentication where required/appropriate;
- timely software and firmware updates;
- controlled administrator privileges;
- secure backup and recovery arrangements;
- monitoring for suspicious network activity;
- appropriate security for cloud systems and remote access; and
- prompt reporting of phishing, malware, lost devices or suspicious access.

Pearce IT will support the School in meeting current DfE cyber-security standards. The Headteacher/SLT digital lead will ensure technical recommendations and identified risks are tracked.

31. Remote learning and off-site access

Where pupils or staff access School systems remotely, safeguarding, filtering/monitoring, privacy and security arrangements will be considered. The School will not assume that controls applying on the School network automatically apply to a device used at home or on another network.

Any material change to remote access or working practice will trigger consideration of whether the filtering and monitoring review needs to be revisited.

32. Visitors, contractors and external providers

Visitors who use School ICT systems must follow relevant Acceptable Use and safeguarding requirements. Contractors and external technology providers with access to monitoring information, pupil data or systems must be appropriately authorised, bound by confidentiality/data-processing arrangements and aware of safeguarding escalation routes.

The School will assess the online-safety arrangements of external educational providers where Mount pupils use their technology or networks and safeguarding responsibility remains with the School.

33. Staff training

All new staff receive online-safety training as part of safeguarding induction. All staff receive at least annual safeguarding updates that include relevant online-safety developments.

- the four Cs and emerging risks;
- generative AI, deepfakes and intimate imagery;
- online child-on-child abuse and exploitation;
- filtering and monitoring responsibilities and limitations;
- how to respond to an alert or pupil disclosure;
- safe handling of electronic evidence;
- cyber security, phishing and data breaches;
- Prevent and online radicalisation; and
- the School's reporting and escalation mechanisms.

The DSL's safeguarding training includes online safety and filtering/monitoring. Directors receive sufficient training to exercise effective strategic oversight. Pearce IT and other persons with access to safeguarding monitoring data will receive safeguarding awareness appropriate to their role.

34. Pupil voice and review of emerging risk

The School will seek pupil views about online safety, including whether pupils know how to report, whether they encounter harmful material, whether controls create unintended barriers and whether particular platforms, trends or locations create concern.

Pupil voice, monitoring alerts, behaviour incidents, safeguarding records, complaints, parent feedback and staff observations will inform curriculum and filtering/monitoring review.

35. Monitoring, audit and inspection readiness

- annual recorded filtering and monitoring effectiveness review;
- recorded routine checks across devices and locations;
- evidence that alerts are received, triaged and acted upon;
- staff training and understanding;
- online-safety curriculum mapping and pupil voice;
- records of significant incidents and safeguarding response;
- evidence of Pearce IT assurance and remediation of defects;
- review of new technology and generative-AI products;
- alignment between this policy, Safeguarding, Mobile Phone, EYFS Mobile Devices, Behaviour and Acceptable Use policies; and
- Director oversight and challenge.

The School will be able to explain to inspectors how its filtering and monitoring works in practice, how leaders know it is effective, how staff respond to concerns and how pupils are educated and supported.

36. Related policies and external support

36.1 Related School policies

- Safeguarding & Child Protection Policy
- Behaviour and Anti-Bullying Policies
- Staff Disciplinary and Conduct Policy / Code of Conduct
- Data Protection Policy and privacy notices
- Complaints Procedure
- Acceptable Use Policy
- Bring Your Own Device Policy
- Mobile Phone Policy
- EYFS Mobile Devices Policy
- Prevent / safeguarding arrangements
- Safer Recruitment Policy

- Missing Child and Attendance Policies

36.2 External support

- UK Safer Internet Centre and Professionals Online Safety Helpline;
- Childnet International;
- NSPCC;
- Internet Watch Foundation;
- UK Council for Internet Safety;
- National Cyber Security Centre; and
- Department for Education online-safety, digital-standards and generative-AI guidance.

Appendix A – Staff online-safety response guide

If this happens...	Do this...
A pupil tells you something worrying happened online	Listen, do not investigate, report to DSL/DDSL immediately and record.
You see harmful content on a pupil screen	Make the situation safe; do not assume the filter/monitor has reported it; tell DSL if safeguarding-related.
NetSupport/monitoring alert identifies concerning activity	Authorised safeguarding staff review promptly in context and record/escalate as appropriate.
A pupil reports an AI-generated nude/deepfake	Treat as an intimate-image safeguarding incident; do not ask to see/copy/forward it; report immediately.
You suspect grooming or exploitation	Report to DSL/DDSL immediately; preserve relevant information without conducting your own investigation.
You discover illegal sexual-abuse content	Do not download/copy/share; make safe; report immediately to DSL for IWF/police route.
Filtering appears not to work	Tell Pearce IT and DSL/Head immediately; put temporary supervision/control in place if safeguarding gap exists.
A School device is lost, hacked or compromised	Report immediately to Pearce IT and the appropriate School lead; follow data-breach/security procedure.
Concern relates to staff online conduct	Use adult safeguarding/low-level concern procedure, not merely the IT misuse process.

Appendix B – Annual filtering and monitoring review record

Academic year / review date:

Review participants: Headteacher/SLT lead; DSL; DDSL as appropriate; Pearce IT; Director/Proprietor:

Current filtering product/configuration:

Current monitoring product/configuration:

Devices and operating systems reviewed:

Locations/network routes reviewed:

Remote/cloud access considered:

Pupil risk profile considered (age/SEND/EAL/known vulnerabilities):

AI-generated/dynamic content risk considered:

Monitoring alert effectiveness and response times:

Over-blocking / under-blocking identified:

Recent incidents/bypass attempts/themes:

Staff training/understanding:

Privacy/DPIA/retention arrangements:

Changes to technology or working practice:

Actions required, owner and deadline:

Director assurance / challenge:

Date actions completed:

Appendix C – Routine filtering and monitoring check record

Date	Tester	Device/user	Location/network	Test / alert	Result	Action

Appendix D – Online-safety incident decision guide

- 1. Is anyone in immediate danger? If yes, use emergency procedures / 999 and inform DSL.
- 2. Is this a safeguarding concern about a child? Report immediately to DSL/DDSL and record on safeguarding system.
- 3. Does it involve intimate imagery, including deepfake or AI-generated material? Do not view/copy/forward unnecessarily; DSL leads response.
- 4. Does it involve child-on-child abuse, harassment or bullying? Safeguarding and behaviour procedures may both apply.
- 5. Does it suggest grooming, exploitation, radicalisation, self-harm/suicide risk or serious violence? Escalate immediately to DSL.
- 6. Is content potentially illegal? Preserve safety and relevant information without redistributing illegal material; DSL considers police/IWF/other route.
- 7. Is it primarily a technical/cyber-security incident? Notify Pearce IT and relevant School lead, while considering safeguarding/data implications.
- 8. Does it involve an adult's conduct? Use the allegations/low-level concerns procedure.
- 9. Record action, rationale, outcome and any technical remediation.
- 10. Consider whether the incident indicates a wider curriculum, supervision, filtering/monitoring or policy issue.