

THE MOUNT SCHOOL

ACCEPTABLE USE OF TECHNOLOGY POLICY AND STAFF ACCEPTABLE USE AGREEMENT

2026-2027

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

This policy applies to staff, supply/visiting staff, contractors, volunteers and other authorised adult users of The Mount's technology, systems or information, insofar as relevant to their role.

It should be read with the Online Safety Policy, Staff Code of Conduct, Safeguarding and Child Protection Policy, Mobile Phone Policy, EYFS Mobile Devices Policy, Data Protection arrangements, Whistleblowing Policy and Disciplinary and Conduct Policy.

1. Purpose

The Mount provides technology to support teaching, learning, safeguarding, administration and communication. All users are expected to use technology professionally, lawfully, securely and in a way that protects children, colleagues, families and the School.

2. Legal, safeguarding and guidance framework

The policy reflects Keeping Children Safe in Education 2026; the DfE's digital and technology standards, including the filtering and monitoring and cyber-security core standards; current DfE guidance on data protection and generative AI; UK GDPR and the Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025; the Computer Misuse Act 1990; copyright and intellectual-property law; and the School's duties under the Prevent framework.

Technology use is a safeguarding matter as well as an IT matter. Filtering is preventative; monitoring is reactive. Neither removes the responsibility of staff to supervise pupils, report concerns and use professional judgement.

3. Core acceptable-use commitments

Every authorised adult user must:

- use School technology primarily for legitimate professional purposes;
- follow safeguarding, confidentiality, data-protection and information-security requirements;
- use only accounts, systems, software and services they are authorised to use;
- protect passwords, devices and information from unauthorised access;
- maintain professional standards in electronic communication and online activity;
- respect copyright, licensing and intellectual-property rights;
- not deliberately access, create, store or share illegal, extremist, pornographic, discriminatory or otherwise inappropriate content;
- not attempt to bypass filtering, monitoring, security controls or access restrictions unless specifically authorised for technical duties;
- report safeguarding, cyber-security, data-protection and accidental-access incidents promptly; and
- cooperate with lawful and proportionate monitoring of School systems.

4. School accounts, passwords and authentication

- Each user must use their own authorised account and must not routinely share credentials.
- Passwords must be strong, unique and kept confidential. School passwords must not be reused for personal services.
- Multi-factor authentication must be used where the School requires or provides it.
- Users must lock or sign out of devices when leaving them unattended where another person could gain access.
- Suspected account compromise, phishing or unauthorised access must be reported immediately.
- Staff must not access another person's account, mailbox or files without lawful authority.

5. Email, messaging and professional communication

School email addresses and School telephone numbers must be used when contacting parents.

- Use School-approved communication channels for professional contact.
- Communications must be professional in tone, content and timing.
- Do not use personal social-media accounts or private/disappearing-message services to communicate with pupils.

- Do not use personal email or personal telephone numbers for pupil/parent communication unless an exceptional arrangement has been authorised.
- Check recipients and attachments carefully before sending personal or confidential information.
- Use BCC or other appropriate methods where multiple recipients should not see one another's contact details.
- Do not forward School information to a personal email account merely for convenience.
- Suspicious links, attachments or requests for credentials/payment must be treated as potential phishing and reported.

6. Personal mobile phones, smart watches and personal devices

All staff must adhere to the School's Mobile Phone Policy and, in EYFS, EYFS Mobile Devices Policy.

Personal devices must not be used casually while supervising or teaching pupils. Personal use should normally take place only during authorised breaks and in appropriate areas, except in an emergency or other expressly authorised circumstance.

Staff must not use a personal phone, smart watch, camera or other personal device to photograph, video or audio-record pupils for School purposes, except for an exceptional authorised safeguarding/emergency reason which is reported immediately.

Personal devices used for any authorised School activity must be appropriately secured. School data should not be stored locally on a personal device unless specifically authorised and protected.

7. School devices taken off site

- Keep devices physically secure and do not leave them unnecessarily visible in vehicles or public places.
- Use approved accounts, storage and security controls.
- Do not allow family members or other unauthorised people to use School accounts or access School data.
- Take particular care when viewing confidential information in public.
- Report loss, theft or suspected compromise immediately.
- Return equipment promptly when requested and do not deliberately erase School records that should be retained.

8. Personal data and confidential information

All staff have a responsibility to protect personal data. Personal information must only be accessed where there is a legitimate professional need and must not be browsed out of curiosity.

- Use approved School storage rather than personal cloud storage, USB devices or personal messaging services unless specifically authorised.
- Do not copy safeguarding, SEND, medical, HR or other sensitive information into unapproved systems.
- Check that information is being shared with the correct person and that the recipient has a legitimate need to know.
- Use secure disposal/deletion methods in accordance with the retention schedule.
- Report any actual or suspected loss, misdirection, disclosure or unauthorised access immediately so the School can assess whether a personal-data breach has occurred.

9. Generative artificial intelligence (AI)

Generative AI may support legitimate professional tasks, but its use must be safe, transparent, proportionate and subject to professional judgement. AI output is not inherently accurate and does not replace the responsibility of the member of staff using it.

Only AI tools approved for the intended School use may be used where School or personal data is involved. Staff should seek advice from the senior leadership team where uncertain.

Unless an approved tool and data-protection arrangement expressly permits it, staff must not enter identifiable or readily identifiable pupil, parent or staff personal data into public or consumer generative-AI tools.

- Do not enter safeguarding disclosures, child-protection records, medical information, SEND case information, staff HR information, photographs of identifiable pupils or confidential correspondence into an unapproved AI service.
- Anonymise or remove personal data before using AI where the task does not require it.
- Fact-check and critically review AI-generated content for accuracy, bias, safeguarding risk, age appropriateness and misinformation.
- Do not rely on AI alone to make safeguarding, disciplinary, admissions, SEND, assessment or other significant decisions about individuals.
- Check copyright and intellectual-property implications before publishing or distributing AI-generated material.
- Acknowledge/reference AI use where required by School procedure or professional/assessment rules.
- Do not use AI to impersonate pupils, parents, colleagues or leaders, or to create deceptive images, audio or communications.
- Do not use pupil-facing AI tools unless the School has approved the product, purpose, age suitability, safeguarding controls and data-processing arrangements.

10. Filtering and monitoring

The School uses filtering and monitoring as part of its safeguarding arrangements. Staff must understand that School networks, devices and accounts may be filtered and monitored in accordance with law, School policy and privacy information.

Users must not attempt to disable, evade or circumvent filtering or monitoring. A legitimate teaching or operational need to access blocked material should be raised through the authorised route rather than bypassing controls.

Staff must continue active supervision and safeguarding practice even where filtering is in place. No filtering system is completely effective.

Monitoring alerts and reports are safeguarding information. Access must be restricted to authorised, appropriately trained personnel. Alerts must be acted on promptly and outcomes recorded where required.

The School will review filtering and monitoring provision at least annually, involving senior leadership, the DSL, IT support and the responsible proprietor/governance role, and will record the review and actions.

The review will consider changes in technology, remote/BYOD use, the pupil risk profile including age and SEND, and whether provision can address real-time, dynamic, personalised and AI-generated content.

11. Accidental access to inappropriate material

The original requirement to report accidental access is retained. If a user accidentally encounters illegal, harmful, inappropriate or disturbing content, they should:

- avoid further viewing, sharing or downloading unless specifically necessary to preserve evidence and safe to do so;
- close/minimise the content where appropriate without taking steps that destroy evidence needed for safeguarding or technical investigation;
- report the incident promptly to the DSL/appropriate online-safety or IT lead according to its nature;
- ensure a safeguarding/online-safety record is made where required; and
- seek support if the material is distressing.

Suspected child sexual abuse imagery must never be copied, printed, forwarded or independently investigated by staff. The DSL must be informed immediately and the safeguarding procedure followed.

12. Software, apps, extensions and online services

Staff must not install or procure software, browser extensions, apps, AI tools or cloud services for School use where doing so would create unmanaged safeguarding, data-protection, licensing or cyber-security risk.

Users must apply security updates when prompted or allow managed updates to run and must not deliberately disable antivirus, endpoint management or security controls.

13. Removable media and external storage

USB drives and other removable media create loss and malware risks. School-approved secure storage should be used wherever practicable.

Where removable media is necessary, it must be authorised, appropriately protected and scanned/managed in accordance with IT arrangements. Sensitive information must not be placed on an unencrypted personal USB device.

14. Photography, video, audio and CCTV

Images and recordings of pupils are personal data and may also be safeguarding information. They must only be created for a legitimate authorised purpose and using approved equipment/systems.

School images must not be copied to personal photo libraries, personal cloud backups or personal messaging services. Staff must follow the School's consent, privacy, retention and safeguarding arrangements.

CCTV or monitoring footage must only be accessed by authorised persons for legitimate purposes and must not be copied or shared informally.

15. Social media and public online activity

The original requirement that online content remain professional and protect the School's reputation is retained, but staff private life is not subject to unlimited School control. The relevant test is whether online conduct breaches professional duties, confidentiality, safeguarding boundaries or materially affects suitability/trust.

- Do not post confidential information or identifiable pupil information without authority.
- Do not make or accept social-media connections with current pupils through personal accounts.
- Do not use anonymous accounts to harass, intimidate, discriminate or circumvent professional boundaries.
- Do not comment publicly on confidential School safeguarding, disciplinary or complaint matters.
- Report impersonation, threats, doxxing or online harassment rather than retaliating.

16. Cyber security and prohibited activity

Users must not knowingly:

- gain or attempt to gain unauthorised access to systems, accounts, data or networks;
- introduce malware or malicious code;
- probe, scan, exploit or test School security without explicit authorisation;
- use School systems for fraud, harassment, illegal activity or deliberate copyright infringement;
- disable security controls or conceal prohibited activity;
- connect unauthorised network equipment or create insecure access points;
- share credentials or authentication codes in response to unsolicited requests; or
- use School systems to mine cryptocurrency or undertake other unauthorised high-resource activity.

17. Remote working and public networks

The same safeguarding, confidentiality and data-protection duties apply when working away from School.

- Avoid discussing or displaying confidential information where it can be overheard or seen.
- Use School-approved secure access methods.
- Avoid insecure public Wi-Fi for sensitive work unless protected by approved security arrangements.
- Do not leave devices or paper records unattended in public.
- Ensure online meetings involving pupils use approved platforms and professional backgrounds/settings.
- Report incidents occurring off site in the same way as on-site incidents.

18. Copyright, licensing and intellectual property

Staff must respect copyright, software licences and other intellectual-property rights. The fact that material is accessible online does not mean it can be freely copied or republished.

School software licences must not be shared or installed outside their permitted terms. AI-generated or AI-assisted content must also be checked for copyright or attribution concerns before external publication.

19. Monitoring, privacy and transparency

All monitoring must be lawful, proportionate, transparent and for legitimate purposes such as safeguarding, cyber security, compliance, system management and investigation of suspected misuse.

The School's privacy information should explain relevant filtering/monitoring arrangements, including what is monitored, why, who can access alerts/reports and applicable retention arrangements.

Users should not assume that activity on School systems or School-owned devices is private. This does not authorise arbitrary or excessive surveillance.

20. Reporting incidents

Staff must report promptly:

- a safeguarding concern arising from technology use;
- loss or theft of a School device;
- loss, disclosure or misdirection of personal/confidential information;
- suspected phishing, malware or account compromise;
- accidental access to harmful or inappropriate material;
- a filtering/monitoring failure or concerning alert;
- suspected unauthorised access or cyber attack;
- inappropriate online contact involving a pupil; and
- a mistake involving AI, cloud services or digital systems that may expose personal data or create safeguarding risk.

Urgent safeguarding concerns go to the DSL/DDSL. Technical reporting does not replace safeguarding reporting.

21. Breaches and disciplinary action

Failure to follow acceptable-use rules may result in disciplinary action.

A breach may result in access restriction, management guidance, safeguarding action, investigation or disciplinary proceedings depending on seriousness and context. Serious deliberate misuse may amount to gross misconduct.

Illegal activity may also be referred to the police or other relevant authority. Safeguarding concerns about adult conduct will be considered under KCSIE harm-threshold/low-level-concern procedures.

22. Roles and review

The Director/Proprietor has strategic oversight of the School's safeguarding and technology arrangements. The Headteacher is responsible for implementation. The DSL has lead safeguarding responsibility for online safety and works with IT support and other relevant leaders.

Technical support providers must understand their safeguarding responsibilities where they have access to filtering/monitoring information or School data.

This policy and the associated agreement will be reviewed annually and sooner after significant technology change, a cyber/data incident, safeguarding concern, introduction of new AI capability, or change to statutory guidance.

Appendix A - Staff Acceptable Use Agreement

I confirm that I have read and will follow The Mount School Acceptable Use of Technology Policy, Online Safety Policy, Staff Code of Conduct and associated safeguarding/data-protection requirements.

- I will use School technology, accounts and information professionally, lawfully and securely.
- I will use my own account and protect my password and authentication credentials.
- I will use School-approved communication channels for pupils and parents unless an exceptional arrangement is authorised.
- I will not use a personal device to photograph, film or record pupils except for an exceptional authorised safeguarding/emergency reason.
- I will follow the Mobile Phone Policy and the EYFS device rules where applicable.
- I will protect School equipment and information when working off site.
- I will not upload identifiable pupil, parent or staff data, safeguarding information or other confidential information into an unapproved AI tool or online service.
- I will critically check AI-generated material and remain responsible for anything I use or publish.
- I will not attempt to bypass filtering, monitoring or cyber-security controls.
- I understand that School systems and devices may be monitored lawfully and proportionately for safeguarding, security and compliance purposes.
- I will immediately report safeguarding concerns, data loss/breach, phishing, malware, device loss, inappropriate material or suspected unauthorised access.
- I will not independently copy, share or investigate suspected child sexual abuse imagery.
- I understand that serious or deliberate breach of these requirements may lead to safeguarding and/or disciplinary action.

Name: _____

Role: _____

Signature: _____

Date: _____

Appendix B - AI quick check for staff

- **NEED** - Is AI actually necessary for this task?
- **DATA** - Does my prompt contain any personal, safeguarding, medical, SEND, HR or confidential information?
- **APPROVAL** - Is this tool approved for this use?
- **PRIVACY** - Do I understand what the service does with prompts/uploads and whether data may be retained or used for training?
- **ACCURACY** - Have I checked the output against reliable sources?
- **BIAS/SAFETY** - Is the content appropriate, fair, age-suitable and safe?
- **COPYRIGHT** - Am I entitled to use/reproduce the output and source material?
- **ACCOUNTABILITY** - Would I be comfortable explaining and taking professional responsibility for the final output?

Appendix C - Incident reporting prompt

What happened and when?

Which device/account/system was involved?

Was personal or safeguarding information exposed?

Was a pupil involved or at risk?

Has access been secured/password changed/device isolated where appropriate?

Who has been informed - DSL, Headteacher, IT support?

Has evidence been preserved without unnecessarily copying harmful material?

Does the incident require a safeguarding, data-breach, cyber-security or disciplinary record?

What immediate action and follow-up are required?