

THE MOUNT SCHOOL

USE OF MOBILE DEVICES IN EYFS

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 retains The Mount School's existing strict approach to personal phones, cameras and smart watches in the EYFS while correcting the legal basis and strengthening operational controls.

1. Purpose and safeguarding principle

Safeguarding and protecting children within The Mount School EYFS is paramount. Mobile phones, cameras, tablets, smart watches and other electronic devices with imaging or sharing capabilities can support legitimate work but can also create opportunities for distraction, breaches of privacy, inappropriate communication, covert recording or misuse.

The EYFS statutory framework requires safeguarding policies to include how mobile phones, cameras and other electronic devices with imaging and sharing capabilities are used in the setting.

The Mount therefore applies robust controls to personal devices while providing authorised School equipment for legitimate educational and operational purposes.

2. Scope

This policy applies throughout the nursery and all School-based EYFS provision to employees, agency/supply staff, students, apprentices, volunteers, visitors, contractors, parents/carers and other adults. It also applies to children where they bring or use a personal device.

It covers mobile phones, personal cameras, tablets, laptops, smart watches, wearable cameras, connected glasses, audio/video recorders and any other personal electronic device capable of imaging, recording, communication or sharing.

3. Statutory and policy framework

- EYFS statutory framework for group and school-based providers applying from 1 September 2026, particularly safeguarding policies and procedures;
- Keeping Children Safe in Education 2026;
- Working Together to Safeguard Children 2026;
- DfE statutory guidance on mobile phones in schools, to be followed from 1 September 2026;
- the Education (Independent School Standards) Regulations 2014;
- the Data Protection Act 2018 and UK GDPR;
- the School's Safeguarding & Child Protection Policy, Online Safety Policy, Mobile Phone Policy, Staff Code of Conduct and data-protection arrangements.

The School's prohibition on image-capable smart watches in EYFS is a Mount safeguarding rule. The previous policy incorrectly described this specific smart-watch prohibition as itself being required by statutory guidance. The statutory requirement is that the setting's safeguarding procedures address the use of mobile phones, cameras and other electronic devices with imaging and sharing capabilities.

4. Responsibilities

4.1 Headteacher / DSL

- ensure this policy is implemented consistently;
- ensure staff understand the rules during induction and safeguarding training;
- respond to safeguarding concerns or breaches involving devices;
- ensure concerns about adults are considered under the allegations/low-level concerns procedure;
- ensure authorised photography and recording arrangements are safeguarding- and data-protection compliant; and
- review this policy after significant incidents or changes in technology/guidance.

4.2 EYFS leaders

- model and enforce the policy in daily practice;
- ensure staff, students, volunteers and visitors understand where personal devices may be kept and used;
- challenge device use that does not comply with this policy;

- ensure School devices are stored securely and used only for authorised purposes; and
- report concerns promptly to the DSL.

4.3 All adults

Every adult is responsible for complying with this policy and for challenging or reporting unsafe practice. Staff must not assume that another person will report a breach.

5. Personal mobile phones – staff

The existing Mount rule is retained: staff may bring a personal mobile phone to work, but its use is tightly controlled.

- Personal phones must not be used for personal calls, messaging, social media or browsing while supervising or directly caring for children.
- Routine personal use is limited to recognised breaks and must take place away from children.
- Personal phones must never be used to photograph, film or audio-record a child.
- Personal phones must never be used to store, transmit or access safeguarding records or confidential pupil information unless an expressly authorised emergency procedure requires this and the Headteacher/DSL directs it.
- Phones must not be used in toilets, nappy-changing areas, intimate-care spaces or other designated camera/mobile-free areas.
- Staff must not lend a personal phone to a child or allow a child to access it.

Where an exceptional personal circumstance means a staff member needs to remain contactable, the Headteacher may agree an individual arrangement. This may permit the volume to remain on or the device to be accessible, but it does not permit photography/recording or unrestricted use around children.

The School recognises the wellbeing value of being contactable in genuinely stressful or exceptional circumstances; the arrangement must nevertheless preserve effective supervision and safeguarding.

6. Storage and access to personal devices

EYFS leaders will identify where personal phones and other prohibited devices are to be stored during working time. Storage arrangements must prevent children from accessing devices and reduce the risk of covert or casual use.

Where staff are permitted to keep a phone about their person under the School's existing approach, it must remain unused while working directly with children except under an agreed exceptional arrangement. The Headteacher/EYFS leader may require phones to be placed in designated secure storage if concerns arise.

7. Smart watches and wearable/connected devices

The Mount retains its rule that staff working in EYFS must not wear a smart watch or other personal wearable device that can take, generate, receive, display, store or share images, audio/video or messages while working with children.

This includes devices with camera, messaging, voice-recording, internet, AI-assistant or remote communication functionality where that functionality cannot be reliably disabled.

A simple watch or a device being used solely for an agreed medical/disability purpose may be permitted following an individual assessment. The School will consider reasonable adjustments and medical needs rather than applying the rule in a way that unlawfully disadvantages a member of staff.

Unauthorised use or wearing of a prohibited device may be considered under the Staff Code of Conduct/disciplinary procedure and, where relevant, the safeguarding adult-concern procedure.

8. School-owned iPads, cameras and devices

The Mount provides authorised School devices, including iPads, to record children's activities, achievements and learning where appropriate. The original policy's use of School iPads is retained.

- Only authorised School equipment may be used to photograph or record children for School purposes.
- Devices must be password/PIN protected and configured in accordance with School security arrangements.
- School devices must not be removed from the premises without permission from the Headteacher or an authorised senior leader.
- Devices must not be left where children can access them unsupervised.
- Images and recordings must be transferred/stored only on approved School systems.
- Staff must not send authorised pupil images to personal email accounts, personal cloud storage or personal messaging applications.
- Loss, theft, unauthorised access or suspected compromise must be reported immediately.

The School may use device-management, filtering or monitoring controls where appropriate. School-owned status does not itself make every use acceptable.

9. Taking photographs and recordings

Photographs and recordings may be taken only for a clear, legitimate School purpose and in accordance with safeguarding, privacy and data-protection requirements.

Upon admission, parents/carers are provided with the School's current information and choices concerning photography and use of images. The previous policy referred to the annual emergency form; the School will continue to record relevant permissions/preferences but will ensure that the lawful basis for processing is determined by the School rather than treating consent as the only possible lawful basis.

- images used to document learning and development;
- authorised displays or learning journals;
- School communications, website or marketing where the School's privacy/permission arrangements allow;
- training or qualification evidence where authorised and necessary; and
- other specifically approved educational or operational purposes.

The DSL/EYFS safeguarding lead will ensure that photographs used by staff for further training or qualifications are appropriate to the context and handled securely.

Staff will seek to ensure that photographs fairly represent the diversity of children at The Mount and that no child is repeatedly favoured or excluded without a legitimate reason.

10. Image identification, publication and sharing

Where images are published publicly, staff will minimise identifying information and will not routinely combine a child's full name with an identifiable photograph. Any exception must be authorised and have a clear lawful and safeguarding basis.

Before publishing or sharing an image, staff must consider whether the image is appropriate, dignified and consistent with the purpose for which it was taken.

Images of children during intimate care, toileting, changing, sleep or other situations where dignity may be compromised must not be taken except in a highly exceptional safeguarding/medical context expressly directed through an approved procedure.

11. Storage, retention and deletion of images

The previous policy stated that photographs would be deleted when no longer required 'as decided by each form teacher'. This is replaced by a School-wide approach. Images and recordings are School records and must be retained and deleted in accordance with the School's data-retention schedule, privacy information and the purpose for which they were created.

Individual staff must not retain images indefinitely or make personal decisions about retention outside School procedures. Images will be stored on password-protected approved systems and printed only through authorised School arrangements.

12. Toilets, nappy changing, intimate care and private areas

Toilets, changing spaces, nappy-changing areas, intimate-care spaces and other designated private areas are mobile phone/camera-free areas.

Staff must not take personal phones, personal cameras or prohibited image-capable wearables into these areas. A breach may constitute misconduct and may also require consideration under the safeguarding adult-concern procedure.

Where a device is genuinely required for a child's medical or disability need, an individual arrangement will specify how privacy and safeguarding are protected.

13. Sleep rooms and rest areas

Personal phones, cameras and image-capable personal wearables must not be used in sleep/rest areas while children are present. Staff must maintain active supervision and follow the School's separate safer-sleep procedures.

Authorised School technology used for an approved monitoring or operational purpose must not replace the physical checks and supervision required by the EYFS and the School's safer-sleep arrangements.

14. Parents and carers

Parents/carers must not use phones, cameras or recording devices in toilets, changing/intimate-care areas or other designated device-free spaces.

At events, the School may permit or restrict parental photography according to the nature of the activity, safeguarding risks and privacy arrangements. Any restrictions communicated by staff must be followed.

Parents/carers should not post photographs or recordings of other people's children online without appropriate permission. Where a concern affects a child's safeguarding or privacy, staff should inform the DSL.

15. Visitors, contractors, volunteers and students

Visitors, contractors, volunteers and students must be informed of the EYFS device rules as appropriate to their access.

- Personal devices must not be used to photograph or record children.
- Device use must be limited to legitimate purposes and, wherever practicable, away from children.
- No personal device may be used in intimate-care/private areas.
- A professional who needs a device for an authorised professional function must explain this to the relevant leader and follow agreed controls.
- Staff should challenge unexplained or inappropriate device use rather than assuming it has been authorised.

Where a visitor's or professional's use of a device is integral to an authorised statutory/professional function, the School will apply proportionate controls rather than imposing a rule that obstructs necessary safeguarding, health or professional work.

16. Children's personal devices

Children in the EYFS must not have access to personal mobile phones or communication-enabled smart devices during the session/day. This is consistent with the School's Mobile Phone Policy and the statutory mobile-phone guidance.

Any device brought in accidentally will be secured out of the child's access and returned in accordance with School procedures. A necessary medical/SEND device will be managed through an individual arrangement.

17. Screen use and digital technology in EYFS

From 1 September 2026 the EYFS framework requires providers to have regard to DfE guidance on children's screen use in early years settings. The Mount will use screens purposefully and proportionately, taking account of children's age, development, individual needs, the quality of the activity and the importance of interaction, movement, play and real-world experiences.

Digital devices will not be used as a routine substitute for responsive adult interaction, supervision, comfort, play or behaviour support. Where screens are used, staff will consider the educational purpose, duration, content, posture/environment and opportunities for adult-child interaction.

Screen use required for an individual child's SEND, communication, medical or accessibility need will be considered separately and supported appropriately.

18. Online safety, AI and connected functions

Where an authorised EYFS device has internet, communication or generative-AI functions, the School's Online Safety Policy applies. Staff must not upload identifiable pupil information, images, safeguarding information or confidential material to unauthorised AI systems or online services.

AI image generation, image alteration, facial manipulation or other generative functions must not be used with children's images unless expressly approved following safeguarding and data-protection assessment.

19. Responding to a breach or concern

Any concern that a device has been used to photograph, record, communicate with or otherwise involve a child inappropriately must be treated seriously.

Situation	Immediate response
Staff member uses personal phone routinely in front of children	Challenge where safe; report to EYFS leader/Headteacher. Consider Code of Conduct/low-level concern.
Adult photographs or records a child on a personal device	Stop the activity if safe; do not investigate the device yourself; report immediately to Headteacher/DSL.
Device used in toilet/changing/intimate-care area	Report immediately; preserve safeguarding information; Headteacher/DSL considers adult-concern/LADO route.
School device lost or compromised	Report immediately to Headteacher/DSL and IT/data-protection lead; take security/data-breach action.
Child accesses inappropriate content	Make safe, reassure, report safeguarding concern and follow Online Safety Policy.
Suspected intimate/sexual image involving a child	Do not view/copy/forward unnecessarily; report immediately to DSL and follow safeguarding procedure.

20. Concerns about adults, low-level concerns and allegations

A breach of this policy may be a conduct matter, a low-level safeguarding concern or an allegation that meets the harm threshold. Staff must report concerns promptly through the Safeguarding & Child Protection Policy rather than attempting to determine the threshold themselves.

Where the concern may meet the harm threshold, the Headteacher will consider LADO consultation/referral in accordance with the School's safeguarding procedure. If the concern relates to the Headteacher, it must be reported to the Director/Proprietor.

The device must not be searched by colleagues unless there is a clear lawful and authorised basis. Police, LADO or other professional advice may be required.

21. Training and implementation

- All EYFS staff will receive this policy during induction and relevant updates thereafter.
- Agency staff, students and volunteers will be briefed before they work with children.
- Staff will understand which devices are prohibited, where personal phones may be stored/used, how School devices are used, and how to report a concern.
- Leaders will use supervision, observation and safeguarding culture to check that the policy is implemented in practice.
- Repeated minor breaches will be considered for patterns rather than treated in isolation.

22. Monitoring and review

The Headteacher/DSL and EYFS leadership will monitor implementation. The Director/Proprietor will receive assurance through the School's safeguarding oversight arrangements.

This policy will be reviewed at least annually and earlier following a safeguarding incident, a significant change in technology, a change to the EYFS framework or KCSIE, or learning from inspection/audit.

The policy must remain consistent with the Safeguarding & Child Protection, Mobile Phone and Online Safety policies.

Appendix A – EYFS device rules: staff quick guide

- **PERSONAL PHONE:** may be brought to work, but routine use only on breaks away from children; never photograph/record children.
- **SMART WATCH / IMAGE-CAPABLE WEARABLE:** not worn while working with EYFS children under Mount policy unless an agreed medical/disability arrangement applies.
- **SCHOOL iPad/CAMERA:** authorised School purposes only; secure it and store images on approved systems.
- **TOILET / NAPPY / INTIMATE-CARE / PRIVATE AREA:** no personal phone, camera or prohibited wearable.
- **SLEEP/REST AREA:** no personal imaging/communication device use while children are present.
- **PARENT/VISITOR:** challenge unexplained photography/device use and report concerns.
- **BREACH INVOLVING A CHILD:** make safe and report to DSL/Headteacher; do not search the adult's device yourself.
- **AI/CLOUD SERVICE:** never upload pupil images or confidential information to an unauthorised service.