WALMLEY
JUNIOR SCHOOL

Mobile Phone and Photography Policy

Policy agreed: September 2026
Policy review date: September 2027
Approved by: Headteacher
DPO : M Clinton

Mobile phones and photography policy

Policy Statement

The school recognises that mobile phones are an important means of communication for many families. However, to safeguard pupils, maintain a positive learning environment and promote professional standards, the use of mobile phones on the school site is subject to clear expectations for pupils, staff, parents, carers and visitors.

This policy aims to:

- Safeguard all pupils and staff.
- Minimise disruption to learning.
- Promote responsible use of technology.
- Protect the privacy and wellbeing of the school community.
- Ensure compliance with safeguarding requirements.

1 Purpose and scope

This policy brings together expectations for pupils, staff, parents, carers and visitors. It supports a calm learning environment, safe supervision and the protection of personal information. It applies on school premises and, where relevant, during educational visits, residentials and other school activities off site.

School devices are used for photography on school premises. Staff may use personal phones for agreed professional purposes off site, including taking and temporarily sharing trip photographs, subject to the safeguards below. Personal use and professional use are treated separately.

References to phones include other devices capable of recording, storing or sharing information. Read this policy alongside safeguarding, staff conduct, acceptable use, data protection, privacy notices, retention and educational visits procedures.

Pupils and medical exceptions

Pupils bringing a phone to school must switch it off on arrival and hand it to staff. Phones are placed in the designated collection basket and taken to the school office for secure storage throughout the day. They are returned at the end of the school day.

Pupils must not access or use phones during the school day unless a member of staff permits an exceptional use. Unauthorised use may lead to confiscation, contact with parents or carers and action under the behaviour policy.

Where a phone or connected device is needed for medical reasons or as a reasonable adjustment, individual arrangements will be agreed with parents or carers and relevant professionals. These arrangements will protect access to necessary support and set appropriate limits on other uses.

Visit information will explain pupil phone arrangements for trips and residentials. Parents needing to contact their child must use the school office or the agreed visit contact.

Staff

Use on school premises

Staff must model appropriate phone use. Personal calls, messages and browsing must take place during designated breaks away from pupils. Phones must be silent, out of sight and stored securely during teaching and supervision unless needed for an agreed professional purpose, an emergency or an authorised medical or accessibility adjustment.

Use school cameras, tablets or other approved school devices to photograph, film or record pupils on school premises. Personal phones must not be used for this purpose on site. Necessary work authentication or an urgent call is permitted, provided supervision is maintained.

Staff must not give pupils their personal contact details or communicate privately with pupils through personal accounts. Family communication must use school channels wherever possible. School devices must be secured, used through authorised accounts and returned to designated storage.

Use on visits and residentials

The Headteacher may agree the use of personal phones for legitimate school purposes off site. This can include contacting school or emergency services, navigation, coordinating staff, accessing approved school systems and photographing agreed activities and achievements. Staff may therefore need to use a phone in pupils' presence when carrying out these duties.

Before a visit, the visit leader must record the agreed purposes, staff involved, photography arrangements, transfer method and deletion deadline, and obtain Headteacher approval. School equipment must be available where a personal phone cannot meet the safeguards or a member of staff does not wish to use their own device.

- Use a strong passcode or equivalent protection, automatic locking and current security updates. Do not use shared or compromised devices. Keep devices under staff control and prevent access by pupils, family members or others.
- Before photography, prevent automatic upload to personal cloud accounts, shared albums and linked devices. If this cannot be assured, use school equipment. Check messaging downloads and backups as well as camera settings.
- Phone use must not distract from supervision. Personal use on residentials must be limited to agreed off-duty periods away from pupils. Do not use a phone while driving.
- Do not copy safeguarding, medical or other sensitive records into personal messaging, email or notes apps. Arrange secure access to essential visit information in advance. If an urgent family call from a personal phone is necessary, withhold the number where practicable and record significant communication through school procedures.

Photographs and recordings

The school must establish and record an appropriate lawful basis for each use of identifiable images. Check current photo permissions, objections and safeguarding restrictions before taking or sharing photographs. Where consent is relied on, it must be valid for the intended purpose. Permission for one use must not be assumed to cover another.

The visit leader must brief relevant staff discreetly about restrictions. Respect a child's wish not to be photographed wherever possible and refer uncertainty to the DSL or Headteacher. Take only images needed for the agreed school purpose.

Never record changing, toileting, washing, intimate care or circumstances compromising privacy or dignity. Do not photograph children asleep in bedrooms or children in distress for trip updates. Do not photograph injuries or disclosures on a personal phone; follow safeguarding procedures and seek DSL advice.

Images must not be used personally, posted on personal social media or uploaded to unapproved editing or AI services.

6 Temporary staff sharing and parent access

Use an approved school-controlled system, such as an authorised Microsoft 365 or SharePoint location, to collect and retain school images. Check access permissions, recipients and links. Do not use public links, personal email or personal cloud drives.

A temporary staff-only group, or messaging platform, may be considered for visit coordination and temporary collection of trip photographs. It is not automatically approved because staff are permitted to use personal phones. Before use for pupil images or information, the Headteacher must approve a documented assessment informed by DPO advice, including whether a data protection impact assessment is needed.

Any approved group must have a named administrator and verified membership limited to staff who need access. The arrangements must cover device security, automatic saving, backups, linked devices, onward sharing, school access to records and deletion. Parents and pupils must not be added. Staff must not forward images outside the agreed process; all recipients must follow the same storage and deletion requirements.

Photographs for families must be checked against permissions and restrictions and shared through approved school communication channels or a restricted school-controlled service. Consider the disclosure of other children's images in group photographs. Explain the intended audience and use. Public online publication requires a separate check of the relevant permissions and lawful basis.

Transfer retention and deletion

Transfer selected photographs to the agreed school-controlled location as soon as practicable. The normal visit arrangement is to complete transfer and delete personal-device copies before returning to school. Confirm successful transfer before deleting the required school copy. If secure transfer is unavailable, record the reason and obtain Headteacher agreement to a short extension, normally no later than the next working day after return.

Deletion covers the camera roll, files, downloads, recently deleted or trash folders, approved messaging applications and duplicates on linked devices. Check for accidental personal cloud uploads or backups. Each staff member must confirm completion to the visit leader. Report any copy that cannot be removed or located for DPO advice; do not confirm deletion where it is uncertain.

Retained school images must have restricted access, a documented purpose and a retention period set in the school's retention schedule with DPO advice. Delete unnecessary duplicates promptly. If images are relevant to a safeguarding concern, complaint or investigation, seek DSL or DPO instructions before deletion and preserve necessary material in an approved restricted school system.

Parents carers visitors and events

Phones should be kept out of sight on the school premises and must not be used in the building or grounds without staff permission. Parents, carers and visitors must not photograph, film or record pupils, staff or school activities without prior school authorisation. Visitors may be asked to store or refrain from using phones.

Families will not normally be permitted to record performances, assemblies or school events using personal devices. Where appropriate, the school may arrange a recording and share it through approved channels, subject to the relevant permissions, objections and safeguarding restrictions. The school may decide not to record or distribute an event where this would be inappropriate.

Responsibilities emergencies and concerns

The Headteacher approves arrangements and oversees implementation. The visit leader briefs staff and checks transfer and deletion confirmations. The DSL advises on safeguarding restrictions and concerns. The DPO advises on lawful processing, platforms, retention and data incidents. All staff are responsible for following the agreed safeguards and reporting problems promptly.

Protecting life and obtaining urgent help take priority. Use an available phone to contact emergency services or school when necessary, share only information needed and inform the visit leader or Headteacher as soon as practicable.

Immediately report lost devices, wrong recipients, unauthorised access, accidental uploads or failure to delete to the Headteacher and DPO through school procedures. Report safeguarding concerns to the DSL without delay. Record what happened and the containment attempted; do not recirculate images to demonstrate the problem. The school, with DPO advice, will assess any breach and meet applicable notification duties, including the 72-hour ICO deadline where notification is required.

Implementation and review

Provide this policy at induction and before relevant visits, record staff acknowledgement, publish an accessible copy and explain planned trip updates and photography arrangements to families. Align privacy notices and related procedures with actual practice.

Breaches will be addressed proportionately through behaviour, staff conduct, safeguarding or visitor procedures as appropriate. Visitors may be asked to stop recording or using their phone, cooperate with removal of unauthorised recordings, or leave where necessary. Complaints will be handled through the school's complaints procedure.

This combined policy takes effect on its actual approval date and will be reviewed annually and after significant changes or incidents. The supplied general mobile phone policy records approval on 22 September 2026; that date is not evidence that these additional off-site provisions were approved then.

Breaches of the Policy

Failure to comply with this policy may result in appropriate action being taken by the school.

For pupils, this may include:

- Confiscation of the device.
- Contact with parents/carers.
- Application of the school's behaviour procedures.

For staff, breaches may be managed through relevant staff conduct procedures.

For parents, carers and visitors, the school may ask individuals to cease using their device, delete unauthorised images or recordings, or leave the premises where necessary.

Monitoring and Review

This policy will be reviewed annually by the school leadership team and governing body to ensure it remains effective, compliant with safeguarding requirements and reflects current guidance and practice.

Approved by: ___Headteacher_____

Date: ____22.09.26_____

R

eview Date: ___September 2027_____

Appendix A Visit record

Visit and dates: _____

Visit leader and participating staff:

_____

Agreed phone and photography purposes:

_____

Lawful basis and pupil restrictions checked by and date:

_____

Approved storage and transfer method:

_____

Messaging assessment and DPO advice reference:

_____

Device cloud and backup controls checked:

_____

Transfer and deletion deadline:

_____

Headteacher approval and date:

_____

Transfer verified by and date:

_____

Staff deletion confirmations and date:

_____

Exceptions incidents or retained evidence:

_____

Reference guidance

Department for Education — Mobile phones in schools — The role of staff
https://www.gov.uk/government/publications/mobile-phones-in-schools/mobile-phones-in-schools

Department for Education — Data protection in schools — Taking and using photos and videos and using CCTV in schools
https://www.gov.uk/guidance/data-protection-in-schools/taking-and-using-photos-and-videos-and-using-cctv-in-schools

The operational safeguards in this policy are school requirements for approval, rather than quotations from DfE guidance.