Special Partnership Trust

# MOBILE DEVICE AND PERSONAL CALL POLICY

Date Last Reviewed: September 2026
Mid Review March 2027
Review Date: September 2028

Special Partnership Trust

## AIM

This policy should be read in conjunction with the SPT on-line safety policy, acceptable use policy, safeguarding and whistleblowing policy, IT policy, and anti-bullying policy. All staff who work within our Trust must sign the acceptable use policy and abide by the guidance contained in it.

This policy applies to all pupils, staff and visitors and explains the rules and procedures regarding the use of mobile phones, and other personal devices within the Trust schools and ARB's.

This policy should be rad in conjunction with ;

- Keeping Children Safe in Education 2026
- SPT filtering and Monitoring standards
- Staff Code of Conduct
- Data Protection and Information security policies
- Online Safety Policy

For the purpose of this policy, a personal device refers to any mobile or tablet device with photographic capabilities, except for:

- Local Authority, Health Authority, or Approved Contractor-issued devices, which are governed by their respective policies;
- School Governors/Trustees, who may use personal devices during meetings but not during class visits or monitoring visits where children are present.

Even in the cases above, the use of such devices remains subject to safeguarding rules outlined in the school's Safeguarding Policy. Some key personnel (e.g., Parent Liaison Officers) have been issued personal devices for professional use and must keep them accessible for work-related contact.

Staff seeking guidance on this policy should consult their school's Senior Leadership Team (SLT). Any observed misuse of personal devices that contravenes this policy must be reported immediately to the Designated or Deputy Safeguarding Lead Officer. Failure to report may result in disciplinary action.

Any misuse of mobile technology which creates a safeguarding concern must be reported immediately to the DSL an recorded in line with safeguarding procedures.

## RATIONALE

- To safeguard pupils from potential grooming or inappropriate relationships with staff and visitors;

• To protect staff and visitors from allegations related to inappropriate communication with or misuse of pupil images;

To ensure appropriate communication within the school environment while upholding the acceptable use and safeguarding policies.

## USE OF PERSONAL DEVICES

**This includes mobile phones, smart watches, wearable technology. AI enabled glasses and any internet connected device capable of recording images, audio or communications.**

• It is the policy of the SPT that employees/visitors do not use their personal devices during reception working hours (08.30-15.30) other than under the exceptions below*. In exceptional circumstances personal devices may be used with permission from the Senior Leadership Team; personal devices must not be used until permission has been granted. Personal devices must be switched off and kept in a secure place during working hours. *They may be used in the staffroom and SLT offices. They may not be used in any other room. It is permissible for staff to use personal devices in their own vehicles if parked in the staff car park or away from the school building (e.g. – lunch-break).

• Anyone needing to contact employees/visitors for urgent reasons should do so using the school landline. Employees/visitors should give this number to family members etc. so that they can be contacted in an emergency. The receptionist will ask how urgent the call is and ascertain whether it can wait until a suitable time – e.g., the person's lunch break/after school. Urgent calls will always be passed on to employees/visitors immediately.

• In exceptional cases it may be necessary for a personal device to be used to make an emergency medical call from the classroom if all external lines are in use. In this situation the call would be fully recorded as part of the incident.

• If off-site, the visit lead/deputy may have their personal device switched on; the details/purpose of this must be recorded within the risk assessment/additional control measures. This will also allow the school to be able to contact the visit lead/deputy in cases of an emergency. The telephone number of the personal devices (visit lead and deputy) must be entered on the educational visits out of school record sheet so that the group can be contacted by school if necessary. When staff are out supporting educational visits, non-urgent calls received by the school will be noted and a message passed on

either through email or placed in the staff member's pigeonhole using the telephone message pad held at reception.

• It will be the responsibility of the visit lead/deputy to ensure personal devices are not used to take images of pupils; school cameras have been provided for this purpose. It will be the responsibility of the visit lead/deputy to remind all staff and parents who are helping to support such visits to remind them of this policy and the terms within it.

• If personal devices are required to support individuals or when classes are split etc, this needs to be bought to the attention of the SLT for immediate discussion.

• It is important to protect the pupils in our care from the possibility of their images being taken and used without permission (please refer to pupil permission slips at all times to ascertain if permission has been granted by parents/carers). Personal devices must never be used to take photos of pupils. A list will be kept by the school office for permissions to use pupil's images in various contexts – this should be adhered to at all times whenever using a pupils' image.

• Text messages or calls should not be made to pupils or parents using personal devices or personal landlines as this could open up the possibility of allegations against members of staff in relation to inappropriate relationships or communication. Calls made on the school telephones can be monitored but those on personal phones cannot. To do this, you must ask the permission of the SLT.

• All staff MUST make a record of any call made to parents/carers using the agreed telephone log which is stored in the school office.

• No personal calls should be made using school phones unless it is considered absolutely necessary; permission should be requested from a member of SLT to do so.

• Any staff member who abuses this policy and does not adhere to it may be subject to information gathering which may lead to the disciplinary policy being invoked.

**USE OF WORK MOBILES**

Some schools within the Trust have issued work mobiles to staff for professional use. The following rules apply:

Work mobiles must only be used for work-related purposes. They should not be used for personal calls, except in emergencies. Staff must ensure work mobiles are kept secure and not left unattended.

They may be used to contact parents and external agencies where necessary. Calls and messages related to pupils must be logged appropriately. Staff must never use work mobiles to contact pupils directly, except in pre-approved exceptional circumstances.

They must not be used to take images of pupils unless explicitly authorised. Any images taken for work purposes must be stored securely and deleted once no longer needed. Work mobiles must not be used to store personal data outside of authorised school systems.

Any loss, theft, or suspected misuse of a work mobile must be reported immediately to the SLT. Staff are responsible for ensuring work mobiles are used appropriately and returned in good condition. If the device is lost or stolen contact IT immediately. Where personal data may have been compromised, the Data Protection Officer must be informed immediately.

All SPT supplied mobile devices and their contents remain the property of SPT and are subject to security features, regular audit, and monitoring. These devices should only be connected to networks, laptops or desktop computers that meet with the requirements in this policy. Any misuse may lead to disciplinary action.

Information processing equipment, internet, intranet, and e-mail access provided by SPT are for SPT business use ONLY. Under no circumstances should these devices be used by anyone other than a SPT staff member. It is not permitted to let children, family members or any unauthorised person to have access to these devices.

**USER OBLIGATIONS**

- Ensure that any mobile device is kept safe and secure at all times;
- Ensure that a PIN, complex password, or bio-metric access is always in use, and you do not allow any other person (including children) to have that password or access your device;
- Staff must use Multi-Factor Authentication (MFA) where provided by the Trust.
- Minimise the download of apps to smartphones and only download applications sourced from a known app store, such as Apple, or Google;
- Not store data on local drives or outside our secure firewalls; this means you must not email data to your private email address or save data outside of your workspaces;
- Not store personal data, such as music or photographs, on SPT devices;
- Personal data must only be accessed, processed , shared and stored using Trust approved systems and applications.

• Not change or attempt to make changes to the security settings or configuration of any approved device without prior authorisation from the Trust or IT Department;
• Promptly comply with requests from the Trust or IT Department for the return of devices for security or other upgrades and servicing;
• Staff must not use personal messaging applications, social media platforms or private communication channels for communication with pupils. Communication with parents or professionals must only take place using Trust approved systems except where expressly authorised by the Headteacher
• Sign a copy of this Policy to confirm your understanding of the importance of complying with these requirements.

**REMOTE WORKING**

In exceptional circumstances where teachers need to communicate with parents **from** home and do not have access to a school mobile. In these circumstances they must ensure that their phone number is withheld or blocked and not shared with parents – and that all calls made on their device are logged on the school system.

Staff must not use personal messaging apps or social media for work communication.

Use of AI and Generative Technology
Staff must not upload personal data, pupil information, safeguarding records, health information, behaviour records or confidential Trust information into public AI systems unless explicitly approved by the Trust.

Any use of AI for professional purposes must comply with Trust data protection, safeguarding and information security requirements.

AI content used within the Trust remains the responsibility of the member of staff who generated it.

**PUPILS**

Pupils are discouraged from bringing their personal devices to school unless its an absolute necessity; we recognise that many of our pupils wish to learn to use a personal device. We will recognise this aspiration and plan/deliver structured teaching session to support the development of their skills within this area; this will be taught via the functional curriculum offer within the school. In such instances a school personal device will be used.

If pupils bring personal devices to school, the phones must remain in their bags and switched off while pupils are in class, the school building and the school grounds. Parents will be advised that the [name] Trust accepts no liability for the loss or damage to personal devices which are bought into the school.

The misuse of personal devices by pupils , including cyber bullying, inappropriate photography , online harassment or accessing harmful content will be manged through the Behaviour policy, Online safety policy and Safeguarding procedures.

## MONITORING AND REVIEW

This policy will be monitored and reviewed by the Head Teacher and Trustees /Local Governing body.