



Abbey Multi Academy Trust **Policies & Procedures**

Mobile and Smart Technology Policy

Approved on	1 st September 2026
Approved by	Abbey MAT Board of Trustees
Last reviewed on	1 st September 2025
Next review due	1 st September 2027

1. Policy aims and scope

- This policy has been written by Abbey Multi Academy Trust, involving staff, learners and parents/carers, building on The Education People's mobile and smart technology policy template with specialist advice and input as required, taking into account the DfE statutory guidance 'Keeping Children Safe in Education' 2026 which places increased emphasis on online safety, digital safeguarding, and the role of mobile and smart technologies in potential safeguarding concerns, Early Years and Foundation Stage 2021 'Working Together to Safeguard Children' 2023 and the relevant local authority procedures.
- This policy also reflects the Department for Education statutory guidance Mobile phones in schools (2026), which establishes the expectation that schools operate as mobile phone-free environments by default and that the use of mobile phones and other smart technology with comparable functionality is prohibited throughout the school day except in clearly defined exceptional circumstances.
- The purpose of this policy is to safeguard and promote the welfare of all members of Abbey Multi Academy Trust and its academies when using mobile devices and smart technology.
 - Abbey Multi Academy Trust and its academies recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm when using mobile and smart technology.
 - As outlined in our Child Protection Policy, the Designated Safeguarding Lead (DSL), Helen Owen Deputy Headteacher, is recognised as having overall responsibility for online safety. The DSL will ensure appropriate filtering and monitoring systems are in place, and that staff are trained in recognising and responding to online risks, including those involving mobile and smart technology.
- This policy applies to all access to and use of all mobile and smart technology on site; this includes mobile phones and personal devices such as tablets, e-readers, games consoles and wearable technology, such as 'smart watches and fitness trackers, which facilitate communication or have the capability to record sound or images.
- This policy applies to learners, parents/carers and all staff, including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy).
- This policy also recognises the increasing risk of online abuse, coercion, and harassment facilitated via mobile and smart technologies, and aims to mitigate such risks through education, monitoring, and clear boundaries

This policy sets out the Trust-wide expectations for the safe use of mobile and smart technology across all academies within Abbey Multi Academy Trust. Individual academy operational arrangements, including pupil mobile phone procedures, are set out within

academy-specific appendices and must comply with the principles established by this policy.

2. Links with other policies

- This policy links with several other policies, practices and action plans, including but not limited to:
 - Anti-bullying policy
 - Acceptable Use Policies (AUP)
 - Behaviour and discipline policy
 - Safeguarding and child protection policy
 - Code of conduct policy
 - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
 - Online safety policy

3. Roles and Responsibilities

The Trust Board is responsible for:

- approving this policy
- receiving assurance that academies are complying with statutory safeguarding requirements, Trust policy and relevant DfE guidance
- providing strategic oversight of mobile and smart technology risks across the Trust
- receiving assurance that appropriate filtering and monitoring arrangements are in place and operating effectively
- holding leaders to account for the implementation and effectiveness of this policy

The CEO is responsible for:

- ensuring that effective Trust-wide systems, processes and controls are in place to support compliance with this policy
- providing assurance to the Trust Board regarding implementation and effectiveness

Headteachers/Principals/Heads of School are responsible for:

- implementing this policy within their academy
- ensuring compliance with Trust requirements, statutory safeguarding guidance and academy-specific arrangements
- monitoring the effectiveness of local procedures and taking action where improvements are required
- ensuring staff and pupils understand expectations

The DSL is responsible for:

- managing safeguarding concerns arising from technology use
- overseeing online safety arrangements
- ensuring incidents are appropriately recorded and reviewed

4. Safe use of mobile and smart technology expectations

- Abbey Multi Academy Trust and its academies recognises that use of mobile and smart technologies is part of everyday life for many learners, staff and parents/carers.
- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of Abbey Multi Academy Trust and its academies are advised to:
 - take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
 - use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on their phones or devices.
- Mobile phones and personal devices are not permitted to be used in specific areas on site, such as changing rooms and toilets.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line our policies.
- All members of Abbey Multi Academy Trust and its academies are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our behaviour, child protection or code of conduct policies.

5. School/setting-provided mobile phones and devices

- Staff providing formal remote learning will do so using school provided equipment in accordance with our acceptable use policy/remote learning protocols.
- School mobile phones and devices will be suitably protected via a passcode/password/PIN and must only be accessed or used by members of staff *and/or* learners.
- School/setting mobile phones and devices will always be used in accordance with the acceptable use of technology policy and other relevant policies.
- Where staff and/or learners are using *school* provided mobile phones and/or devices, they will be informed prior to use via our Acceptable Use Policy (AUP) that activity may be monitored for safeguarding reasons and to ensure policy compliance.
- In line with KCSIE 2026, school uses appropriate filtering and monitoring systems on all school-provided mobile and smart technology to ensure safeguarding and detect potential risk. These systems are regularly reviewed to ensure effectiveness and age-appropriateness.

6. Staff use of mobile and smart technology

- Members of staff will ensure that use of any mobile and smart technology, including personal phones and mobile devices, will take place in accordance with the law, as well as relevant school policy and procedures, such as confidentiality, child protection, data security staff code of conduct and Acceptable Use Policies.
- Staff will be advised to:
 - Keep mobile phones and personal devices in a safe and secure place during lesson time.
 - Keep personal mobile phones and devices switched off or set to 'silent' mode during lesson times.
 - Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
 - Not use personal devices during teaching periods unless written permission has been given by the *headteacher/principal*, such as in emergency circumstances.
 - Ensure that any content bought onto site via personal mobile phones and devices is compatible with their professional role and our behaviour expectations.
- Staff are expected to model the responsible and proportionate use of mobile technology and should avoid unnecessary personal mobile phone use in the presence of pupils unless required as part of their role or in an emergency.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
 - Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the DSL and/ headteacher/principal.
- Staff will only use school provided equipment (not personal devices):
 - to take photos or videos of learners in line with our image use policy.
 - to work directly with learners during lessons/educational activities.
 - to communicate with parents/carers.
- Where remote learning activities take place, staff will use school provided equipment. If this is not available, staff will only use personal devices with prior approval from the headteacher/principal following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy and the remote learning protocols.
- If a member of staff breaches our policy, action will be taken in line with our staff *code of conduct* and allegations policy.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

- All staff will receive regular training on safe and appropriate use of mobile and smart technology, including recognising safeguarding risks arising from technology use. This will be part of annual safeguarding training and updated in line with KCSIE 2026.

7. Learners use of mobile and smart technology

Mobile phones and smart technology are managed as a safeguarding issue as well as a behaviour issue. The Trust recognises that mobile and smart technology may facilitate bullying, child-on-child abuse, image-based abuse, sexual harassment, coercion, exploitation, online grooming, misinformation, disinformation, deepfake content and AI-generated abuse. Academy procedures must therefore prioritise safeguarding and child welfare when determining local arrangements.

- Learners will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices, and will be made aware of behaviour expectations and consequences for policy breaches.
- Safe and appropriate use of mobile and smart technology will be taught to learners as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources.
- Abbey Multi Academy Trust adopts the principle that all academies should be mobile phone-free environments by default. Any departure from this principle should be by exception only and should be supported by a clear educational, medical, safeguarding, accessibility or legal rationale.
- Academy arrangements must ensure that pupils do not have routine access to mobile phones during lessons, registration or tutor periods, movement between lessons, breaktimes, lunchtimes or other activities taking place during the school day unless a documented exception applies. For local details see appendix 2.
- Pupils may only bring mobile phones and personal devices onto academy sites in accordance with local academy procedures.
- Academy-specific arrangements regarding:
 - possession of mobile phones
 - storage arrangements
 - smart watches
 - permitted use
 - sanctions for misuse
 - educational visits
 - examination procedures

are contained within appendix 2 and form part of this policy.

The Trust recognises that smart watches, fitness trackers and other wearable technologies may possess functionality equivalent to a mobile phone, including messaging, internet access, recording and notifications. Academy procedures must therefore address such devices alongside mobile phones.

- If a learner needs to contact their parents or carers whilst on site, they will be allowed to use a school phone e.g. the office telephone.
- Academies will communicate mobile phone expectations clearly to pupils, parents, carers, staff, visitors and governors. Parents and carers will be encouraged to support academy expectations and use established communication routes during the school day.
- If a learner requires access to a personal device in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the headteacher/principal prior to use being permitted.
 - Any arrangements regarding access to personal devices in exceptional circumstances will be documented and recorded by the school.
 - Any specific agreements and expectations (including sanctions for misuse) will be provided in writing and agreed by the learner and/or their parents carers before use is permitted.
- Where learners' mobile phones or personal devices are used when learning at home, this will be in accordance with our Acceptable Use Policy and Remote Learning protocols.
- Mobile phones and personal devices must not be taken into examinations. Learners found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- Any concerns regarding learner's use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including anti-bullying, child protection and behaviour.
 - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection, behaviour or anti-bullying policy.
 - Searches of learners' mobile phones or devices will be conducted in line with the Department for Education's guidance on Searching, Screening and Confiscation (DfE, 2024) and KCSIE 2026, ensuring any action is proportionate, necessary, and carried out by authorised staff with appropriate recording and oversight.
 - Academy-specific arrangements regarding confiscation, storage and return of devices are outlined within the relevant academy appendix and will be implemented in accordance with the Behaviour Policy and DfE guidance on searching, screening and confiscation.
 - Appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy.
 - Concerns regarding policy breaches by learners will be shared with parents/carers as appropriate.
 - Where there is a concern that a child is at risk of harm, we will respond in line with our child protection policy.

- If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.
- Learners will be made aware of the risks of image sharing, coercive control, livestreaming, and online exploitation through mobile and smart devices. They will be taught how to report concerns and seek help, in line with our wider safeguarding education curriculum

Exceptions

Exceptions to academy mobile phone arrangements will only be considered where required for:

- medical monitoring or treatment
- SEND-related reasonable adjustments
- safeguarding arrangements
- exceptional family circumstances
- legal requirements

Any exception must be approved by the Headteacher/Principal, documented and reviewed periodically.

8. Visitors' use of mobile and smart technology

- Visitors are expected to comply with academy-specific requirements regarding mobile phone and device use when on site.
- Local procedures are detailed within the appendix 2.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our acceptable use of technology policy and other associated policies, including child protection.
- If visitors require access to mobile and smart technology, for example when working with learners as part of multi-agency activity, this will be discussed with the headteacher/principal prior to use being permitted.
 - Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by the school. This may include undertaking appropriate risk assessments if necessary.
- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or headteacher/principal of any breaches of our policy.
- Visitors are not permitted to make recordings of meetings on their own devices; if necessary, the academy will provide a minute taker. If the academy wishes to record a virtual meeting that is taking place with parents / external parties, this should be made clear at the start of the meeting and permission sought from all those in attendance for the recording to take place. Meetings should only be recorded, by the academy, for the purpose of creating minutes / notes of the

meeting. Once the minutes/notes have been created, the recording should be erased.

- All visitors will be made aware of our safeguarding expectations regarding mobile device use on-site. This includes not taking photos or recordings unless authorised. The safeguarding team retains the right to restrict or supervise visitor mobile use if any safeguarding concern is raised.

9. Policy monitoring and review

- Technology evolves and changes rapidly. Abbey Multi Academy Trust and its academies will review this policy at least annually. The policy will be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied. Any issues identified will be incorporated into our action planning.
- Headteachers will periodically review the effectiveness of academy mobile phone arrangements and consider feedback from pupils, staff and parents. Trustees and governors will receive assurance that academy arrangements remain aligned with this policy and with current DfE guidance.

10. Responding to policy breaches

- All members of the community are informed of the need to report policy breaches or concerns in line with existing school policies and procedures.
- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- We require staff, parents/carers and learners to work in partnership with us to resolve issues.
- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
- Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- If we are unsure how to proceed with an incident or concern, the DSL (or a deputy) or headteacher/principal will seek advice in accordance with our child protection policy.

Appendix 1 – Glossary of Terms

Acceptable Use Policy (AUP):

A set of rules outlining the responsible and appropriate use of technology, digital services, and the internet by learners, staff, and visitors.

Child-on-child abuse:

Also referred to as peer-on-peer abuse, this includes bullying (including cyberbullying), physical abuse, sexual violence and harassment, and coercive control between children, including through technology.

Designated Safeguarding Lead (DSL):

A senior staff member with responsibility for safeguarding and child protection in school, including oversight of online safety and policy implementation.

Filtering and Monitoring Systems:

Technical tools used to block or log access to inappropriate or harmful online content and activity. Schools are required to ensure these are effective, age-appropriate, and actively monitored.

Image-based abuse:

The non-consensual taking, sharing or threat of sharing of intimate images, also known as sextortion or 'revenge porn'. Increasingly facilitated via mobile devices and apps.

KCSIE (Keeping Children Safe in Education):

Statutory guidance from the Department for Education (DfE) outlining schools' and colleges' duties to safeguard and promote the welfare of children.

Mobile and Smart Technology:

Any portable device that can connect to the internet or communicate electronically, including mobile phones, tablets, smartwatches, e-readers, and games consoles.

Online safety:

The process of protecting children and adults from harm on the internet and through digital technology, including exposure to harmful content, contact, and conduct.

Remote learning protocols:

Guidance and procedures that set out safe and effective practice when delivering education via online platforms, especially where school-issued or personal devices are used at home.

Sexting (also known as youth-produced sexual imagery):

The creating, sharing, or forwarding of explicit images or messages by young people via mobile devices. Considered a safeguarding and potentially criminal matter.

Smartwatch/Fitness Tracker:

Wearable technology capable of connecting to other devices, accessing the internet, tracking location, or capturing audio/video.

Social media:

Web-based platforms that enable users to create and share content or participate in social networking (e.g. Instagram, Snapchat, TikTok, WhatsApp).

Visitor:

Any non-regular adult present on school premises including parents, volunteers, contractors, and professionals from external agencies.

Appendix 2 – Academy Mobile Phone Arrangements

Item	Local Arrangement
Rationale for local approach	
Can pupils bring phones?	Only pupils in Y5 or Y6 who are walking to or from school independently.
Storage requirements	Phones are handed in on their classroom door and are stored in the office during the day before being returned at home time as they leave the room.
Smart watch requirements	Children are not permitted to wear / use smartphones during the school day.
Use during school day	No phone use allowed during the day by pupils.
Sanctions	Parents informed. Children then need to hand in direct to the school office. Repeat use would then mean that child is no longer able to bring a phone at all.
Exceptional medical use	Phones or devices may be required for medical use e.g. diabetes monitoring. Safeguarding checks on use and access with be individualised between the school, parents and medical team.
Educational visits	Children do not have access to mobile phones on trips or residential.
Exams	N/A
Staff use of mobile phones	Staff use of mobile phones is restricted to staffrooms and office spaces. At times their use may be needed to verify devices / log in however wherever possible this will be done when children are not present.
Visitor use of mobile phones	Visitors are informed phones are not permitted to be used within the school. This is in the visitor leaflet and there is a sign on the internal entrance door.