University of Chichester Academy Trust

Mobile Phone and Smart Device Policy

2026-2027

Review Cycle: Annually

Approved by: Local governing body

Date: 5-10-26

Contents

1. Introduction 2
2. Purpose 2
3. Legislation 3
4. Pupil use of Mobile Phones and Smart Devices 4
5. Exceptions and Reasonable Adjustments 4
6. Staff use of Mobile Phones and Personal Devices 5
7. Parents/Carers, Visitors, Volunteers and Contractors 6
8. Images, Recordings and AI Misuses 6
9. Filtering, Monitoring and Mobile Data 6
10. Searching, Confiscation and Safeguarding Concerns 6
11. Loss, Theft or Damage 7
12. Monitoring and Review 7
13. Policy Approval 7
14. Links with other Policies 7
15. Appendices 8

Appendix 1: Stamshaw Infant School Mobile Phone Policy 8

1. Introduction

The Trust is committed to maintaining calm, safe, focused, and respectful learning environments where all pupils can achieve their full potential. The Trust and its family of schools recognise the impact that mobile phones, smart devices and social media have on learning, wellbeing and social interaction. To support our pupil's academic success and personal development, our academies are mobile phone-free by default.

This policy sets clear expectations for the use of mobile phones and smart devices in our academies and supports safeguarding, behaviour, data protection and online safety arrangements and applies to all pupils on an academy site and during the school day.

This policy applies to pupils, staff, volunteers, governors/trustees, contractors, visitors, parents/carers.

2. Purpose

For the purposes of this policy, "mobile phones" includes smartphones, smart watches, wearable technology, tablets, personal laptops, cameras, gaming devices and any device capable of communication, internet access, notifications, image capture, audio or video recording, or data storage.

- Ensure pupils do not use mobile phones during the school day except where a specific exception has been approved (see exception section 5);

- Support safe, responsible and lawful use of technology;
- Reduce risks linked to bullying, harassment, distraction, harmful content, image sharing, safeguarding and data protection;
- Make expectations clear to pupils, staff, parents/carers, visitors and volunteers;
- Ensure concerns are reported, recorded and escalated promptly.

3. Legislation

The Trust will comply with applicable UK legislation, statutory guidance and recognised good practice. This includes:

Reference	Official source
Department for Education – Mobile phones in schools: statutory guidance (statutory from 29 June 2026; schools should follow from 1 September 2026) (GOV.UK)	DfE – Mobile phones in schools
Department for Education – Keeping Children Safe in Education 2026 (comes into force 1 September 2026) (GOV.UK)	DfE – Keeping children safe in education
Department for Education – Behaviour in schools (GOV.UK)	DfE – Behaviour in schools
Department for Education – Searching, screening and confiscation in schools (GOV.UK)	DfE – Searching, screening and confiscation
Education and Inspections Act 2006 – sections 91 and 94	Section 91 · Section 94
Education Act 1996 – section 550ZA	Section 550ZA
Equality Act 2010	Equality Act 2010
Children and Families Act 2014 – section 100	Children and Families Act 2014, section 100
DfE – Supporting pupils at school with medical conditions: statutory guidance (GOV.UK)	DfE – Supporting pupils with medical conditions
Data Protection Act 2018	Data Protection Act 2018
UK GDPR	ICO – UK GDPR guidance and resources
Data (Use and Access) Act 2025	Data (Use and Access) Act 2025
UK Online Harms Early Warning Working Group – Protecting your setting's images from AI manipulation and abuse (UK Safer Internet Centre)	UK Safer Internet Centre – Image guidance for education settings

4. Pupil use of Mobile Phones and Smart Devices

The Trust's position is that pupils must not use personal mobile phones or smart devices on school site and during the school day unless a specific exception has been approved by the Headteacher or a delegated senior leader.

Pupils must not use personal mobile devices to:

- Access social media, messaging apps, games or other non-approved services during the school day;
- Bypass Trust filtering or monitoring using mobile data, VPNs, proxies, tethering or hotspots;
- Take, store or share images, video or audio of pupils, staff, visitors or school activities without permission;
- Bully, harass, intimidate, pressure or abuse others;
- Access, create, store or share harmful, sexual, violent, extremist, discriminatory or illegal content;
- Record lessons, conversations, incidents or meetings unless explicitly authorised for an approved educational, medical or accessibility purpose.

Each academy will manage how it stores any mobile phone or smart devices when pupils bring them on to the school site. By exception, where a minority of pupils are permitted to have access to their mobile phone to school, as noted in section 5, the academy will set local arrangements for how those phones are managed. Please refer to each primary academy for their system of managing mobile devices.

Appendix 1 sets out the Stamshaw Infant School mobile phone policy.

KCSIE 2026 recognises that many children have unlimited and unrestricted access to the internet through mobile networks such as 3G, 4G and 5G, and that this can enable bullying, sexual harassment, controlling behaviour, sharing indecent images, viewing pornography and accessing other harmful content while at school.

5. Exceptions and Reasonable Adjustments

The Trust recognises that there may be legitimate reasons why a pupil may need access to a mobile phone or smart device.

Exceptions may include:

- Medical needs, such as diabetes monitoring or other health-related apps
- SEND, disability or accessibility needs
- Young carer responsibilities
- Safeguarding or welfare arrangements agreed by the academy or Local Authority
- Travel safety arrangements
- Specific educational activities approved by a senior leader
- Residential visits or off-site activities where controlled access is appropriate.

Any exception must be considered case by case, documented and reviewed regularly. DfE guidance confirms that schools must comply with legal duties, including reasonable adjustments under the Equality Act 2010 and arrangements to support pupils with medical conditions under the Children and Families Act 2014.

Where an exception is agreed, access should be limited to the specific purpose, time and location required. An exception does not give a pupil unrestricted permission to use a mobile phone during the school day.

6. Staff use of Mobile Phones and Personal Devices

Staff may bring personal mobile phones and smart devices onto school premises. Personal use must normally be restricted to non-contact time and must not take place in front of pupils.

The Trust recognises that staff may occasionally need to use a personal mobile phone during the school day for legitimate professional purposes, including:

- Emergency communications or contacting emergency services
- Contacting senior leaders or the school office
- Responding to urgent safeguarding, health and safety or operational matters
- Accessing multi-factor or passwordless authentication
- Accessing approved school systems where no Trust device is reasonably available
- Supporting off-site visits, educational trips, PE activities or emergency procedures

Any such use must be professional, proportionate and limited to the purpose required. Personal devices should only be used in front of pupils where there is a clear operational, safeguarding, emergency or authorised work-related reason.

Central Team staff should not use their mobile phone in areas with pupils present. If they need to take a call, this must be done in a room with no access to pupils or outside the academy gates.

Staff must not use personal mobile phones, smart watches, cameras or other personal devices to take photographs or make video or audio recordings of pupils. Where images or recordings are required for an approved educational, safeguarding, communication or operational purpose, staff must use authorised school devices, systems and storage locations.

Staff must not use personal devices to:

- Store pupil images, recordings, personal data or safeguarding information
- Communicate privately with pupils
- Transfer information outside approved Trust systems
- Bypass Trust filtering, monitoring or security controls
- Use personal messaging applications for official communication with pupils or parents, unless formally authorised
- Record meetings, conversations or incidents without a lawful basis and appropriate authorisation

All photographs, recordings and personal data must be managed in accordance with UK GDPR, the Data Protection Act 2018 and the Trust's safeguarding, consent and records-retention requirements.

Any accidental capture, storage, disclosure or sharing of pupil information on a personal device must be reported immediately as a safeguarding and/or data protection concern. This will then be dealt with in accordance with the relevant policies.

Further requirements are set out in the Staff Code of Conduct, Acceptable Use Policy, Data Protection Policy and Records Retention Policy, where applicable.

7. Parents/Carers, Visitors, Volunteers and Contractors

Parents and carers have an important role in supporting the Trust's mobile-phone-free school day. They are encouraged to reinforce the policy at home, discuss the risks associated with mobile phone use, and support the benefits of a calm, safe and focused school environment.

Parents/carers should contact the school office if they need to get a message to their child during the school day. They should not contact pupils directly on personal mobile phones

Parents/carers, visitors, volunteers, governors/trustees and contractors must not use phones where pupils are present unless authorised or necessary in an emergency.

Staff, visitors and volunteers must not take photographs, video or audio recordings of pupils unless explicitly authorised by the academy for an approved purpose.

Parents/carers and volunteers supporting trips must refer any breach by a pupil to a member of staff and they must not search or confiscate devices themselves.

8. Images, Recordings and AI Misuses

Images and recordings of pupils must be treated as safeguarding and data protection material. Staff must use approved school devices, approved systems and approved storage locations for any authorised photographs, videos or audio recordings.

Personal devices must not be used to capture, store or share pupil images or recordings.

The Trust will consider image security risks, including AI manipulation, deepfakes, nudification apps, blackmail, metadata exposure and misuse of images published online.

Where image-based abuse, AI-generated sexual imagery, blackmail or threats involving imagery are suspected, staff must inform the DSL immediately and follow safeguarding procedures.

The **Safeguarding and Child Protection Policy** published on each academy websites and includes the use of images, recordings and AI misuse.

9. Filtering, Monitoring and Mobile Data

The Trust uses RM SafetyNet as its approved filtering system and Smoothwall Monitor as its approved safeguarding monitoring system. These controls apply to Trust-managed systems and networks where technically possible as noted in our Filtering & Monitoring Policy.

Personal mobile phones using mobile data are not normally protected by Trust filtering and monitoring. This is a key reason why pupil use of personal mobile phones is prohibited during the school day and why bypassing Trust controls is treated seriously and further information on the actions being taken are detailed in Safeguarding & Child Protection Policy.

10. Searching, Confiscation and Safeguarding Concerns

Breaches of this policy will be managed in line with the academy Behaviour Policy, Safeguarding and Child Protection Policy and DfE guidance. Sanctions must be reasonable, proportionate and take account of the pupil's age, SEND, disability, medical needs and any safeguarding concerns.

Where there is a reasonable concern that a mobile device may contain evidence of harm, abuse, bullying, sexual content, criminal activity, radicalisation, exploitation or another safeguarding concern, staff must follow the academy's safeguarding procedures and seek advice from the DSL or a senior leader.

DfE guidance confirms that headteachers, or authorised staff, have statutory powers to search a pupil or their possessions where they have reasonable grounds to suspect possession of a prohibited item, or an item identified in the school rules as searchable.

11. Loss, Theft or Damage

Pupils and staff who bring mobile devices to school do so at their own risk. The Trust and its academies accept no responsibility for mobile phones or smart devices that are lost, damaged or stolen on school premises, during school transport, school visits, trips or while travelling to and from school, unless caused by proven negligence on the part of the school. If a mobile device is approved for medical exemptions, the school is not liable if the device gets damaged.

Confiscated devices must be stored securely and returned in line with local academy procedures.

12. Monitoring and Review

This policy will be reviewed annually, or in response to changes to statutory guidance, safeguarding risks, technology or Trust systems.

The review will consider:

- Behaviour and safeguarding incidents linked to mobile phones or smart devices
- Approved exceptions and reasonable adjustments
- Feedback from pupils, parents/carers and staff
- Records of attempts to bypass filtering or monitoring
- Relevant DfE, KCSIE, data protection and online safety guidance
- Whether implementation remains clear, consistent and proportionate

13. Policy Approval

This policy will be approved at each Academy Local Governing Body meeting in line with localised mobile phone and smart device management processes.

14. Links with other Policies

Trust Policies

- Behaviour, Safeguarding and Child Protection:
  - Anti-bullying Policy
  - Child Protection and Safeguarding Policy
  - Exclusions Policy
- Data Protection, IT and Cyber
  - Acceptable Use Policy
  - Data Protection Policy
  - Filtering and Monitoring Policy
  - Record Management Policy (record retention periods)
- Staff professional standards
  - Allegations Against Staff
  - Staff Code of Conduct

Academy Policies

Each academy will have the following linked policies published on their website:

- Behaviour Policy
- Online Safety Policy

15. Appendices

Appendix 1: Stamshaw Infant School Mobile Phone Policy

Devices Covered by this Policy

This policy applies to:

- Mobile phones.
- Smartphones.
- Smart watches.
- Wireless earbuds and headphones.
- Tablets with communication capabilities.
- Any device capable of internet access, communication, photography, video recording or gaming.

Arrival at School

Students who bring a mobile phone to school must:

1. Hand their phone to the teacher at the start of the school day.
2. These are locked away and are inaccessible to children throughout the school day.
3. Children can collect phones from teachers at the end of the day.

Arriving Late to School

Upon signing in students will need to hand their phones to the office staff to be locked away.

Leaving School Early

If a student is leaving school early, they will collect their phone from the teacher or office when they leave.

Smart Watches

Smart watches are not permitted for use during the school day as they often provide access to communication, internet services, and notifications in the same way as mobile phones. Students who bring smart watches to school must hand them to their class teacher to be locked away.

Any smart watch found in use during the school day will be treated as a breach of this policy.

Medical Exemptions

The school recognises that some students may require access to a mobile-connected medical device.

Medical exemptions will only be granted where:

- There is a documented medical need.
- The device is required to support an approved medical condition.
- Appropriate medical evidence has been provided.

Examples may include continuous glucose monitoring systems that communicate with a mobile phone. Alternative arrangements will be agreed between the school, parents/carers, and relevant medical professionals.

If a mobile device is approved for medical exemptions, the school is not liable if the device gets damaged.

Communication Between Home and School

During the school day:

- Parents/carers should contact students through School Reception.
- Students who need to contact home must do so through a member of staff or the school office.
- Emergency messages will be communicated promptly through established school procedures.

Students must not use personal devices to communicate during the school day.

Breaches of the Policy

The following are considered breaches of this policy:

- Using a phone during the school day.
- Attempting to access a phone during the school day.
- Carrying a second phone or undeclared device.
- Using a smart watch during the school day.
- Using earbuds or headphones without permission.

Liability

Students bring mobile phones and electronic devices to school at their own risk.

Whilst the school provides a secure storage system by locking devices away; school cannot accept responsibility for loss, theft, or damage to personal electronic devices unless caused by proven negligence on the part of the school.