

The Darent Federation of Schools

Mobile Phones, Smart Devices and Acceptable Use Policy



Approved by: Governing Body

Date: September 2026

Last reviewed on: New Policy

Next review due by: September 2027

Mobile Phones, Smart Devices and Acceptable Use Policy

Contents

1. Purpose and scope	2
2. Core expectations.....	3
3. Responsibilities.....	3
4. Pupil mobile phones and smart devices	4
5. Exceptions and reasonable adjustments	4
6. Staff, volunteers and contractors	4
7. Visitors and parents/carers	4
8. Acceptable use of Federation technology	5
9. Pupil use of Federation devices	5
10. Images, recording and communication	5
11. Filtering, monitoring and privacy	6
12. Reporting concerns	6
13. Breaches, confiscation and searching.....	6
14. Trips, clubs, remote use and personal devices	6
15. Communication, education and review.....	6
Appendix A – Pupil and parent/carers agreement.....	7
Appendix B – Staff acceptable-use acknowledgement.....	7
Reference framework.....	7

1. Purpose and scope

This policy combines the Federation’s mobile phone and smart-device requirements with its acceptable-use rules. It applies to pupils, staff, governors, volunteers, visitors, contractors and parents/carers when using Federation devices, accounts, systems or internet access, or when personal technology is used on Federation premises or for Federation business.

It covers phones, tablets, laptops, Chromebooks, cameras, eReaders, smart watches, smart glasses, fitness trackers, wearable or connected technology, removable media, apps, cloud services, social media and generative artificial intelligence (AI). It should be read with the Child Protection, Behaviour, Staff Code of Conduct, Data Protection, Generative Artificial Intelligence (AI) policies and Searching, Screening and Confiscation guidance.

Mobile Phones, Smart Devices and Acceptable Use Policy

2. Core expectations

- Safeguarding and the best interests of children come first.
- Pupils will not have access to mobile phones or smart technology with equivalent communications or recording functions during the school day, except under a formally agreed exception.
- Federation technology, accounts and internet access are provided primarily for authorised educational and professional purposes.
- Users must protect personal information, passwords, images, records and the reputation of the Federation and its community.
- Filtering and monitoring support safeguarding but do not remove each user's responsibility to behave safely and report concerns.
- No user may deliberately bypass security, filtering, monitoring or access controls.

3. Responsibilities

Role	Responsibilities
Governing Body	Approve the policy and seek assurance that safeguarding, filtering, monitoring, data protection and behaviour arrangements are effective.
Executive Headteacher and Senior Leadership Team	Implement the policy consistently; approve exceptions and authorised services; ensure staff, pupils and families understand expectations.
Designated Safeguarding and Lead (DSL) and Deputies	Respond to safeguarding concerns arising from devices or online activity and understand the Federation's filtering and monitoring arrangements.
IT Provider/Support	Maintain agreed security controls; report technical risks; support testing, monitoring and incident response.
Subject and phase leaders	Check that intended uses preserve curriculum progression, subject integrity, accessibility and appropriate assessment
All users	Follow this policy, use technology responsibly and report concerns, accidental access, loss, damage or suspected compromise promptly.

Mobile Phones, Smart Devices and Acceptable Use Policy

4. Pupil mobile phones and smart devices

The Federation is mobile phone-free throughout the school day, including lessons, transitions, breaktimes, lunchtimes, clubs taking place within the normal day and while pupils are under school supervision on site.

- Pupils should not bring a phone or communication-enabled smart device to school unless it is needed for the journey to or from school or an agreed individual need.
- Any phone brought to school must be switched off—not merely silenced—and handed to the school office on arrival. It will be stored securely and collected at the end of the day. The device remains the family's responsibility.
- Smart watches or wearables able to message, notify, connect, record, photograph, film or share location are treated as mobile phones. A basic watch without these functions may be worn.
- Parents/carers must contact pupils through the school office during the day. Pupils needing to contact home must ask a member of staff.
- Pupils must never photograph, film or record another person, access social media, message others, livestream, use an unapproved AI tool or share harmful or inappropriate content using any device under school supervision.

5. Exceptions and reasonable adjustments

Exceptions are individual, necessary and proportionate. They will be agreed by the Executive Headteacher or delegated senior leader for a medical condition, disability, SEND, safeguarding plan or another exceptional need. The agreement will specify the purpose, device, times, location, supervision and review date. An exception does not permit unrestricted use.

6. Staff, volunteers and contractors

- Personal phones must be silent, out of sight and securely stored whenever children are present. Staff must not use them for personal calls, texts, email, internet access or social media in front of pupils.
- Personal calls must be made away from children during authorised breaks. A medical or urgent professional exception must be notified to SLT and used in a separate area.
- Staff may use a device briefly for an authorised professional purpose, such as multi-factor authentication or emergency communication, where this is necessary and does not expose information to pupils.
- Personal devices must never be used to photograph, film or record pupils or to store, transmit or access pupil information.
- Staff must use Federation-approved accounts, devices and services for professional communication and must maintain appropriate boundaries with pupils and families, including on social media.
- Repeated or serious breaches may be addressed under the Staff Code of Conduct and Federation Disciplinary Policy.

7. Visitors and parents/carers

Visitors, contractors and parents/carers must keep devices silent and must not photograph, film, record, livestream or use a device in a way that compromises safety, privacy or the orderly running of the school. Essential calls must be taken in an agreed area away from pupils. School events may have specific photography instructions which must be followed.

Mobile Phones, Smart Devices and Acceptable Use Policy

8. Acceptable use of Federation technology

Federation devices, accounts, systems and internet access must be used responsibly. Limited incidental personal use by staff may be permitted where authorised, lawful, reasonable, outside contact time and without cost, risk or disruption.

- Use only an account issued to or approved for you. Keep passwords and authentication codes private; lock or sign out of unattended devices.
- Access, create, store and share only lawful, appropriate and authorised content. Do not bully, harass, discriminate, impersonate, threaten, deceive or create or distribute sexual, violent, extremist or otherwise harmful material.
- Do not search for illegal or inappropriate content, except within a specifically authorised safeguarding or curriculum process. Accidental access must be closed or covered and reported immediately without copying or forwarding it.
- Do not install software, connect unapproved devices or media, change settings, use personal cloud storage, or attempt to bypass filtering, monitoring, antivirus, network separation, Safe Search or other security controls.
- Use respectful language and verify recipients before sending. Do not use Federation systems for unauthorised commercial activity, political campaigning, gambling, copyright infringement or excessive personal use.
- Protect confidential and personal data. Use approved storage and secure transfer methods; collect only what is needed; do not upload pupil or staff information, images or work to unapproved services.
- Copyright, licensing and intellectual-property requirements must be followed. Sources and permitted AI assistance must be acknowledged where appropriate.
- Lost, stolen, damaged or compromised equipment, suspicious messages and suspected data or cyber incidents must be reported immediately.

9. Pupil use of Federation devices

- Pupils use technology only as directed by staff, with age-appropriate supervision and approved accounts, apps and websites.
- Pupils keep login details private, respect other people's work and privacy, and tell a trusted adult if something worries, upsets or confuses them.
- Pupils do not change settings, install items, access another person's account, communicate with unknown people, share personal information or images, or attempt to avoid school controls.
- Pupils may use generative AI only within a specifically authorised and supervised activity and must follow the Federation's Generative AI Policy.

10. Images, recording and communication

Images, audio and video may be captured only on Federation approved equipment, for an authorised purpose and in accordance with consent, safeguarding and data-protection arrangements. Content must be transferred promptly to approved storage and deleted from the capture device where required. Secret recording, covert photography, impersonation, deepfakes and the alteration or sharing of another person's image or voice without authority are prohibited.

Mobile Phones, Smart Devices and Acceptable Use Policy

11. Filtering, monitoring and privacy

Federation devices, systems, accounts and internet use are subject to proportionate filtering, monitoring, logging and technical administration. Users will be informed of this. Monitoring is undertaken for safeguarding, security, operational and legal purposes and is managed in accordance with data-protection, human-rights and retention requirements. Independent mobile-data connections do not pass through Federation filtering and monitoring and must not be used to evade controls.

12. Reporting concerns

- A safeguarding concern must be reported immediately to the DSL or a deputy and recorded on CPOMS in accordance with the Child Protection Policy.
- An immediate danger or suspected crime must be escalated without delay through the safeguarding procedure, including 999 where necessary.
- A concern about an adult must be reported under the allegations and low-level concerns procedures—not investigated informally.
- A technical, data-protection or cybersecurity concern must be reported promptly to the relevant senior leader and IT support; evidence must not be unnecessarily viewed, copied or circulated.

13. Breaches, confiscation and searching

Pupil breaches will be addressed consistently and proportionately under the Behaviour Policy. A phone or similar device may be confiscated where lawful and proportionate, stored securely and returned to the pupil or parent/carer as determined by a senior leader. Age, SEND, disability, medical needs, safeguarding context and other individual circumstances will be considered.

Searching a pupil or device will only be undertaken by authorised staff and in accordance with current DfE Searching, Screening and Confiscation guidance. Staff must not routinely search through device content. Where there may be illegal imagery, criminal activity or risk of harm, the device should be secured without unnecessary examination and the DSL consulted immediately.

14. Trips, clubs, remote use and personal devices

The trip or activity leader will state whether pupil devices are prohibited or exceptionally permitted, and the applicable storage, contact and supervision arrangements. Federation expectations continue when devices or accounts are used remotely. Personal devices must not connect to internal pupil or staff networks; authorised access must use the designated guest or managed network and remains subject to applicable controls.

15. Communication, education and review

The policy will be published and explained to pupils, staff and parents/carers. Expectations will be reinforced at induction, at the start of each academic year and through age appropriate online safety education. The Governing Body will review the policy at least annually and earlier following a serious incident, change in law or guidance, new technology or evidence that arrangements are ineffective.

Mobile Phones, Smart Devices and Acceptable Use Policy

Appendix A – Pupil and parent/carers agreement

Pupils and parents/carers are expected to understand and support the following:

- School is mobile phone-free throughout the day. Any permitted journey phone is switched off and handed to the office.
- Federation technology is used only as directed, safely, kindly and lawfully.
- Passwords and personal information are protected; other people are not photographed or recorded without authority.
- Filtering or monitoring controls are not bypassed, and worries or accidental access are reported to a trusted adult.
- Parents/carers contact their child through the school office and support proportionate consequences for misuse.

Appendix B – Staff acceptable-use acknowledgement

By using Federation technology or personal technology for Federation business, staff confirm that they will:

- Follow safeguarding, professional-boundary, confidentiality, security and data-protection requirements
- Use approved accounts, devices, storage, communication and AI services
- Keep personal phones silent, out of sight and unused for personal reasons when children are present
- Never photograph, record or store pupil information on a personal device
- Not evade filtering, monitoring or security controls
- Report safeguarding, technical, cyber or data concerns immediately through the correct route.

Reference framework

This policy reflects:

- Keeping Children Safe in Education 2026
- the DfE statutory guidance Mobile phones in schools (statutory from 29 June 2026 and to be followed from 1 September 2026)
- Behaviour in schools
- Searching, Screening and Confiscation
- DfE Filtering and Monitoring Core Standard
- DfE guidance on generative AI in education
- Kent County Council LADO Education Safeguarding Advisory Service 2026–27 child protection, mobile phone and acceptable use templates.