Mobile Phone and Personal Device Policy

Rotherfield Primary School

This policy was adopted on 3rd November 2026

This policy is due for review on [insert date].

Contents

1. Purpose and scope 4

2. Statutory status and setting applicability..... 4

3. Devices covered by this policy 5

4. Core principles 5

5. Pupil and learner use during the day..... 6

6. Exceptions, adaptations and reasonable adjustments 8

7. Smart watches, smart glasses and AI-enabled wearables..... 9

8. Staff use of personal devices 9

9. Visitors, volunteers, contractors and parents/carers 10

10. Setting-owned mobile and portable devices 11

11. Educational visits, travel, boarding and residential provision 11

12. Contact between pupils and parents during the day..... 12

13. Breaches, sanctions and confiscation 13

14. Searching for devices..... 14

15. Safeguarding concerns involving a device 14

16. Loss, theft, damage and security..... 15

17. Communication, training and review 16

Appendix A. Local device arrangements 17

Appendix B. Exceptions and reasonable-adjustment record 18

Appendix C. Staff quick guide: What happens if a phone or device is seen or used? 19

1. Purpose and scope

This policy sets out how the setting manages mobile phones, personal devices and other communications or smart technology in order to support safeguarding, behaviour, learning, privacy, professional boundaries and the safe use of technology.

The policy applies to pupils and learners, staff, governors or trustees, volunteers, contractors, visitors and parents/carers where their use of a personal or portable device takes place on setting premises, during setting activities, or otherwise affects safeguarding, behaviour or professional conduct.

The policy distinguishes between personal devices and setting-owned or setting-managed devices. It should be read alongside the Core Online Safety Policy, AI and Emerging Technology Procedure and Communications, Social Media and Image Use Procedure.

2. Statutory status and setting applicability

The Department for Education's Mobile Phones in Schools guidance became statutory on 29 June 2026. Schools should begin following it from 1 September 2026. It requires schools to implement a policy that prohibits pupil use of mobile phones throughout the school day, including lessons, movement between lessons, breaktimes and lunchtime.

For schools, this policy is therefore drafted on a mobile-phone-free-by-default basis. The statutory guidance also states that references to mobile phones should be read as including other communications and smart technology that the school has decided to bring within scope.

The statutory guidance is directed to schools and trusts. Colleges, early years settings and other education providers should not assume that the same statutory

school powers or pupil-behaviour provisions apply to them. They should adapt the policy to their legal framework and learner population. Keeping Children Safe in Education 2026 comes into force on 1 September 2026.

3. Devices covered by this policy

For the purposes of this policy, 'mobile phone and personal device' may include:

- mobile and smart phones;
- smart watches and other wearable communications devices;
- smart glasses and wearable cameras;
- tablets, personal laptops, games consoles and media devices;
- wireless earbuds or headphones where they include communications, recording or assistant functions;
- AI-enabled smart devices, voice assistants and connected technology;
- health or fitness wearables;
- personal cameras, audio recorders or other devices capable of capturing or transmitting information; and
- future devices with equivalent communication, recording, internet-access or smart functionality.

4. Core principles

- Pupils should not have access to or use a mobile phone throughout the school day except where an approved individual exception applies.
- The setting may allow a pupil to bring a phone to and from the site while still prohibiting access to or use of the phone during the school day.
- Rules will be simple, clearly communicated and enforced consistently.
- Safeguarding, medical needs, disability, SEND and individual circumstances will be considered before sanctions or restrictions are applied.
- Personal devices must not be used to bypass filtering, monitoring, security

or other technical controls.

- Personal devices must not be used to photograph, film, record or livestream people or setting activity except where this policy or another setting procedure expressly permits it.
- Staff use of personal devices must support professional boundaries and model the expectations placed on pupils.
- AI-enabled devices and wearables will be assessed according to their actual functionality and risk, not simply by their product name.
- Assistive and medical technology will not be subject to a blanket restriction where its use is necessary and reasonable.

5. Pupil and learner use during the day

5.1 Schools

Pupils must not use or have access to mobile phones during the school day, including during lessons, movement between lessons, breaktimes and lunchtime, except where an approved individual adaptation or reasonable adjustment applies.

Any phone that is required for use after school must be switched off and handed in to the school office at the start of the day. It will be handed back to the child with parent consent once the children have been dismissed from the classroom.

Pupils must not use mobile data, hotspot functions, personal VPNs, tethering or another personal connection to avoid setting filtering, monitoring or security controls.

6. Exceptions, adaptations and reasonable adjustments

A mobile-phone-free school day does not remove the setting's other legal duties. Schools must make reasonable adjustments where necessary and should consider exceptional individual circumstances on their merits.

Examples may include:

- a disabled pupil who needs access to a phone or smart device because of the nature of their disability;
- a pupil using continuous glucose monitoring or another medical device linked to a phone;
- a pupil with an agreed communication or assistive-technology need;
- a young carer or another pupil whose home circumstances create an evidenced need for limited access;
- a safeguarding plan requiring controlled access to a device; or
- another exceptional circumstance agreed by the school following individual assessment.

An exception should normally be no wider than necessary. The school may restrict use to a particular purpose, time, location or supervised arrangement rather than exempting the pupil from all rules.

Where an exception relates to disability, medical need or assistive technology, the relevant safeguarding, SEND, medical, pastoral and data-protection staff should contribute as appropriate.

Approved exceptions should be recorded on Arbor so that staff can apply the arrangement consistently without requiring the pupil to repeatedly explain private circumstances.

7. Smart watches, smart glasses and AI-enabled wearables

Smart technology can perform functions similar to a mobile phone even where it looks different. Schools may include devices with the ability to send or receive messages, connect to mobile or wireless networks, record audio or video, access AI assistants, capture images, share location or transmit data within the scope of this policy.

- Smart watches and smart glasses used primarily for communications or recording may be treated in the same way as mobile phones during the school day.
- Wearable cameras and smart glasses must not be used to record pupils, staff or setting activity unless expressly authorised.
- Personal AI-enabled devices must not be used to capture, transcribe, summarise or transmit confidential conversations or safeguarding information.
- Health and medical wearables should be considered under the exceptions and reasonable-adjustment section where their use is necessary.
- AI-enabled assistive technology should be assessed proportionately and should not be prohibited merely because it contains AI functionality.
- Where a device connects to setting networks or systems, the Cyber Security and Account Management Standard and Filtering and Monitoring Standard also apply.

8. Staff use of personal devices

Staff must model professional and proportionate device use. DfE statutory guidance states that staff should not use their own mobile phone for personal reasons in front of pupils throughout the school day. Responsible bodies and leaders should make local expectations clear.

- Personal use should take place only in authorised circumstances and locations and should not interfere with duties.
- Staff must not use personal phones, personal messaging accounts or personal social-media accounts to communicate with pupils or parents/carers for setting business.
- Staff must not use personal phones, smart glasses, wearable cameras or other personal devices to photograph, film or record children, except under an explicitly authorised exceptional arrangement.
- Staff should use setting-owned devices where mobile communication,

photography or recording is required for work.

- Personal devices must not be used to store setting confidential information or safeguarding records outside approved arrangements.
- Staff must not use mobile data, hotspots or personal devices to circumvent filtering, monitoring or cyber-security controls.

The only time mobile phones may be used during the school day is for authorised multi-factor authentication for work email systems. This is required very occasionally and where possible done out of sight of the children,

9. Visitors, volunteers, contractors and parents/carers

- Visitors, volunteers and contractors will be informed of local restrictions on personal-device use when relevant to their role or access.
- Personal devices must not be used to photograph, film or record children or confidential setting activity unless expressly authorised.
- Visitors with privileged access to systems or data must follow the setting's cyber-security and confidentiality arrangements.
- Parents and carers attending events are not permitted to photograph, film, audio-record or livestream setting events unless the setting has explicitly authorised an event-specific exception. This includes recording meetings with staff.
- Parents and carers should not use mobile phones in ways that compromise safeguarding, privacy or the safe operation of the setting while on site.

The parent/carer event-photography restriction is a local safeguarding control and is not presented as a general requirement of data-protection law.

10. Setting-owned mobile and portable

devices

Setting-owned or managed devices may be used where they support a legitimate educational, safeguarding, communication or operational purpose.

- Staff should use setting-owned devices for work-related calls, messaging, photography or recording where such functions are required.
- Devices must be configured, secured and managed in accordance with the Cyber Security and Account Management Standard.
- Where devices are issued to pupils, access, filtering and monitoring arrangements should follow the Filtering and Monitoring Standard.
- Setting-owned devices used off site remain subject to the setting's safeguarding, acceptable-use, data-protection and security arrangements.
- Lost, stolen or compromised devices must be reported promptly.

11. Educational visits, travel, boarding and residential provision

Children do not need to bring mobile phones on school trips or residentials. Staff members will have setting-issued phones to call parents and take photos. For the residential an emergency contact number will be shared with parents as part of the visit information pack.

12. Contact between pupils and parents during the day

Parents who need to contact their child during the school day should go via the school office. Messages will be relayed to staff and pupils via the internal phone system, or where urgent, face to face.

- Pupils should not use personal phone or communication device during the

school day to contact parents unless an approved exception applies.

- Where a pupil needs to contact home urgently, staff should facilitate this through the school office.
- Parents should be informed of the setting's arrangements so that pupils are not placed under pressure to keep a phone or personal device accessible during the day.
- Exceptions for disability, medical need, safeguarding or exceptional family circumstances should be managed under section 6.

13. Breaches, sanctions and confiscation

For schools, sanctions for breaching this policy must be consistent with the Behaviour Policy and applied lawfully and proportionately. The statutory guidance confirms that schools may use confiscation and detention where appropriate.

- Consequences should be clear, consistent and known to pupils and parents.
- Confiscation may be used where a phone or similar device is used, accessed, heard or otherwise dealt with contrary to the school's rules.
- The length and conditions of confiscation should be proportionate to the disciplinary purpose.
- Age, SEND, disability, safeguarding circumstances and any agreed exception should be considered before a sanction is imposed.
- Repeated breaches may justify escalated sanctions or a different storage arrangement under the Behaviour Policy.
- A refusal to hand over a device should be managed through the Behaviour Policy and should prompt consideration of whether there is an underlying safeguarding or pastoral issue.

Where a confiscated device may contain evidence of a safeguarding concern or suspected criminal activity, staff should follow section 15 and the Incident Response Procedure rather than conducting an informal investigation.

The statutory school guidance notes that staff are protected from liability for loss

or damage to items confiscated as a disciplinary penalty where they have acted lawfully. Settings should nevertheless handle and store confiscated devices carefully and keep proportionate records where appropriate.

14. Searching for devices

This section applies only where the relevant statutory search powers apply. Headteachers, and staff they authorise, have statutory powers to search a pupil or their possessions where the legal conditions are met. Schools can identify mobile phones and similar devices in their behaviour rules as items that may be searched for.

- Any search must follow the current DfE Searching, Screening and Confiscation guidance and the setting's Behaviour Policy.
- Only authorised staff should exercise statutory search powers.
- The legal basis, grounds and safeguards for a search should be considered before it takes place.
- This policy does not extend school search powers to colleges or other settings to which those statutory powers do not apply.

Searching for a device is different from examining its contents. Staff should not assume that possession or confiscation automatically gives authority to browse messages, images, apps or files. Where content may be relevant to safeguarding or criminal conduct, the DSL and, where appropriate, police or other specialist advice should guide the response.

15. Safeguarding concerns involving a device

A breach of the device rules may also be a safeguarding concern. Staff must consider the underlying behaviour and risk rather than treating every incident as a routine behaviour matter.

- Concerns may include bullying, harassment, sexual harm, exploitation, sharing nudes or semi-nudes, sexual extortion, harmful or illegal content, deepfakes, AI-generated sexual imagery, grooming, radicalisation, fraud, involvement in criminal activity (e.g. county lines), impersonation or cybercrime.
- Where there is a safeguarding concern, staff should speak to the DSL or safeguarding team promptly and follow the Incident Response Procedure.
- Staff should not ask a child to forward sexual imagery to prove what has happened.
- Staff should not unnecessarily view, copy, print, save or distribute sexual or illegal material.
- Relevant evidence should be preserved where this can be done safely and lawfully.
- If a pupil needs access to their device to show or explain an online concern, staff should facilitate this safely; the statutory guidance specifically recognises the importance of pupils being able to access a phone where necessary to raise online-safety concerns.

Cyber-security, personal-data-breach and AI-related concerns should also be referred through the relevant supporting standards and procedures.

16. Loss, theft, damage and security

Users remain responsible for taking reasonable care of personal devices they choose or are permitted to bring onto the site. The setting should avoid making absolute statements that attempt to exclude liability in all circumstances.

- Personal devices should be protected by appropriate authentication and kept secure.
- Pupils should follow the school's chosen storage arrangements.
- The setting should state how confiscated or handed-in devices will be stored and returned.

- Lost, stolen or damaged setting-owned devices must be reported immediately.
- A lost or stolen personal device that contains setting information or has access to organisational systems must be reported promptly to the relevant IT or data-protection contact.
- Where a device is compromised, remote access, account-reset or other containment action should follow the Cyber Security and Account Management Standard.

Pupils' phones will be stored securely in the school office and handed back once the class has been dismissed at the end of the day. If a device has been confiscated a parent or guardian will need to collect it from the office. Arrangements will be made with the parent for this to happen.

17. Communication, training and review

The policy and its rationale will be communicated clearly to pupils, staff and parents/carers.

Schools should publish details of the policy on prohibiting mobile-phone use.

Pupils should be reminded of the rules and consequences at the start of each academic year and at other appropriate times.

Parents should be told how to contact pupils during the day and how the school manages urgent messages.

Staff should receive clear guidance on consistent enforcement, exceptions, confiscation, searching, safeguarding and professional use of personal devices.

The setting should use online-safety education to help pupils understand the risks associated with mobile-phone use as well as the purpose of a mobile-phone-free environment.

The policy should be reviewed at least annually and following significant incidents,

changes in statutory guidance or material changes in device technology.

Appendix A. Local device arrangements

Local control	Setting position
Setting type / statutory position	Rotherfield Primary School, Local Authority maintained.
Pupil possession of phones on arrival	Not permitted.
Storage during the school day	If needed for walking home they must be handed in at the school office with prior agreement.
Approved individual exceptions route	Please see Miss Bishop to agreed exceptions.
Medical / disability / assistive-technology arrangements	Any arrangements will be detailed in the children's IPP or IHCP and shared with staff
Smart watches	Watches that send messages or take photos are not allowed in school.
Smart glasses / wearable cameras	Not allowed
Personal tablets / laptops / BYOD	Not allowed
Staff personal-device locations / times	Not to be used when children are present.
Visitor / contractor device restrictions	Not to be used when children are present.
Parent/carer event photography	Not permitted by default unless an event-specific exception is authorised
Educational-visit arrangements	Children do not need phones on visits. Staff will have school issues devices
Confiscation and return arrangements	Confiscated items will be stored in the office and return to parents by arrangement
Items identified in Behaviour Policy as searchable	Not applicable
Contact route for parents during the day	The school office 01892 852574
DSL / safeguarding route	safeguarding@rotherfield-cps.e-sussex.sch.uk

Appendix B. Exceptions and reasonable-adjustment record

Use this record, where a pupil needs an individual adaptation. Avoid recording unnecessary medical or safeguarding detail in a widely accessible document.

Field	Local record
Pupil / learner identifier	[Insert]
Reason category	[Disability / medical / SEND / safeguarding / young carer / exceptional circumstance / other]
Purpose for which device access is needed	[Insert]
Device / function required	[Insert]
Permitted times	[Insert]
Permitted locations	[Insert]
Supervision / storage arrangements	[Insert]
Any restrictions on recording, messaging, internet or AI functions	[Insert]
Staff who need to know	[Insert]
Approved by	[Insert role / date]
Review date	[Insert]
Linked plan / evidence location	[Insert - do not duplicate sensitive information unnecessarily]

Appendix C. Staff quick guide: What happens if a phone or device is seen or used?

If...	Staff should...
A pupil's phone is visible, rings or is used contrary to policy.	Apply the Behaviour Policy consistently. Confiscate where authorised and proportionate. Check whether an approved exception applies.
A pupil says they need the phone for a medical or disability-related reason.	Do not assume misuse. Check the recorded adjustment or seek advice Miss Robins, SENCO
A pupil refuses to hand over a device.	Follow the Behaviour Policy and involve the appropriate Senior Leadership Team member. Consider whether there is an underlying safeguarding issue.
A device may contain a safeguarding concern.	Do not browse it informally. Speak to the DSL and follow the Incident Response Procedure.
A child wants to show staff something worrying on their phone.	Facilitate this safely and involve the DSL where appropriate. Do not ask the child to forward sexual imagery.
A phone may contain illegal or sexual content.	Avoid unnecessary viewing, copying or forwarding. Follow safeguarding procedures and seek specialist/police advice where required.
A member of staff needs to use a phone for MFA or an authorised work task.	Use it discreetly and in accordance with local staff expectations.
A staff member wants to photograph a pupil.	Use an authorised setting device. Do not use a personal phone, smart glasses or wearable camera except under an explicitly authorised

If...	Staff should...
	exception.
A smart watch or smart glasses are being used to message or record.	Treat them according to their functionality and the local rules for equivalent mobile/smart technology.
A parent needs to contact their child urgently.	Direct them to the setting's approved contact route, normally the office.
A pupil exhibits extreme anxiety about not being able to access their phone.	Refer the pupil for assessment under section 6; do not make an informal exception.