The Gateway Primary Academy

Mobile Phones and Smart Devices/ Technology Policy

September 2026

Key Contact Personnel

Nominated Member of Leadership Staff Responsible for the policy: Mr J Cassem

Designated Safeguarding Lead (s): Mr J Cassem

Named Governor with lead responsibility: Mr F Westmorland

Date written: September 2026

Date agreed and ratified by Governing Body: To be shared at Term 1 Governing Body meeting

Date of next review: September 2027

This policy will be reviewed at least annually, and following any concerns and/or updates to national/local guidance or procedure

Contents

1. Policy aims and scope....3
2. Links with other policies....4

3. Mobile phone and smart device expectations in The Gateway 4
3.1 Adaptations and reasonable adjustments 5
4. School provided mobile phones and smart devices 6
5. Staff use of personal mobile phones and smart devices 6
6. Pupils use of mobile and smart devices 7
7. Visitors' use of mobile phones and smart devices 9
8. Communicating the policy and working with parents/carers 10
9. Responding to policy breaches 11
9.1 Searching, screening and confiscation of mobile phones and smart devices 12
10. Policy monitoring and review 13

1. Policy aims and scope

- This policy has been written by The Gateway involving staff, pupils and parents/carers, building on the Kent County Council LADO Education Safeguarding Advisory Service mobile and smart technology policy template, with specialist advice and input as required.
- It takes into account the Department for Education (DfE) statutory guidance 'Keeping Children Safe in Education' (KCSIE), 'Early Years and Foundation Stage' (EYFS) and 'Working Together to Safeguard Children' (WTSC), the DfE non-statutory guidance 'Behaviour in Schools Advice for headteachers and school staff', 'Searching, screening and confiscation at school', 'Mobile Phones in Schools' and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.
- The purpose of this policy is to safeguard and promote the welfare of all members of our community when using mobile phones and smart devices.
    - The Gateway recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils 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), Jamiel Cassem (Headteacher), is recognised as having overall responsibility for online safety.
- This policy applies to all access to and use of all mobile phones, smart technology or smart devices on site. For the purposes of this policy, 'mobile phone' includes any device with similar functionality, such as the ability to send or receive messages or notifications, connect to mobile networks, or record images, audio and/or video. This may include, but is not limited to, devices with built-in mobile connectivity, smart phones, smart watches, smart glasses, fitness trackers and other wearable technology.
- This policy applies to pupils, 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 school/setting (collectively referred to as "staff" in this policy).
- The Gateway recognises that the use of mobile and smart devices/technology is part of everyday life for many pupils, staff and parents/carers. Pupils will be supported to develop an understanding of safe, responsible and appropriate use of technology through an embedded safeguarding approach, including through our curriculum delivery as applicable.

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
  - Cameras and image use policy
  - Child protection policy
  - Staff code of conduct
  - Confidentiality policy
  - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
  - Data security
  - Online Safety (**included in our child protection policy)**
  - Social media

5.

6.

3. Mobile phone and smart device expectations in The Gateway

- The Gateway recognises that expectations regarding the use of mobile phones and smart devices must be appropriate to the age, stage, needs and context of the pupils attending the setting. Safeguarding and the creation of calm, safe and purposeful learning environments underpin our expectations regarding all mobile and smart technology use.
- Personal devices of any kind that are brought onto site are the responsibility of the user. All members of our community are advised to:
  - take steps to protect their personal mobile phones or other smart 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 personal phones or devices.
- Mobile devices and other forms of smart technology must be stored in the office from arrival on school site through the gate until leaving at 3.20pm. The Gateway would only expect pupils walking to or from school independently to bring phones or smart technology onto site and to have a signed phone contract outlining how they will use it.

- The sending of abusive or inappropriate messages or content, including via personal devices is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying, behaviour and child protection policies.
- All members of The Gateway community are advised to ensure that personal mobile and smart technology devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our behaviour or child protection policies.
- The school will ensure that appropriate filtering and monitoring systems are in place on all -provided devices, networks and online platforms, in line with statutory safeguarding guidance, including the Prevent Duty and Keeping Children Safe in Education. For further details, please access our Child Protection Policy – available on our school website.

3.1 Adaptations and reasonable adjustments

- Where appropriate, reasonable adjustments and adaptations may be made to this policy to support individual needs. This may include, for example, circumstances relating to disability, special educational needs, medical requirements or other specific individual needs.
  - The Gateway recognises its duties under the Equality Act 2010 and is committed to ensuring that policies relating to mobile and smart technology do not disadvantage pupils with protected characteristics.
  - Maintained schools and academies have a duty under the Children and Families Act 2014 to make arrangements to support pupils with medical conditions, so that they can access education and participate fully in school/setting life. Where access to mobile or smart technology is required to meet a child's medical needs, this will be considered as part of those arrangements.
  - The school recognises that, in addition to disabilities or medical needs, there may be other exceptional circumstances where a pupil requires limited access to a mobile phone or smart devices. Any such circumstances will be considered on an individual basis, taking into account safeguarding, wellbeing and the best interests of the child.
- Any adaptations or reasonable adjustments will:
  - be considered on an individual basis.
  - be proportionate and necessary to meet the identified need.
  - be agreed in advance by the headteacher.
  - be risk assessed and clearly documented.
  - include clear expectations regarding use, supervision and storage of devices.

    - be discussed and agreed with parents/carers and, where appropriate, the pupil before access is permitted.
    - be regularly reviewed.
- The provision of adaptations or reasonable adjustments does not alter the school's default expectations regarding mobile and smart technology use for the wider community. Adjustments are not exemptions from behaviour expectations and will be reviewed regularly to ensure they remain appropriate.

4. School provided mobile phones and smart devices

- The Gateway does not provide any mobile phones or smart devices to be used which are enabled to send or receive messages and filtering/monitoring removes access to social media. Only administrators can download APPs and this is restricted from pupil use.

5. Staff use of personal mobile phones and smart devices

- Staff are expected to model safe, responsible and appropriate use of technology and to ensure that the use of mobile phones and other devices does not compromise supervision, safeguarding or the care of children.
- Members of staff will ensure that the use of any mobile and smart technology, including personal phones, wearable technology and other smart devices, will take place in accordance with the law, and relevant school policy and procedures. This includes but is not limited to confidentiality, child protection, data security, staff code of conduct and Acceptable Use Policies.
- In line with our expectations regarding mobile phone free or restricted environments, staff must not use personal mobile phones or smart devices in a way that undermines behavioural expectations or the learning environment.
- Staff are expected to:
    - be responsible for ensuring that personal devices are configured appropriately so that their use complies with this policy. This includes disabling notifications, messaging, image display, recording and sharing functions where these could compromise safeguarding, professional boundaries or the learning environment. Where devices cannot be configured to meet these expectations, they must not be worn or used while on duty.
    - keep personal mobile and smart devices in a safe and secure place during teaching, learning or supervision time, for example in a cupboard or bag.

- ensure personal mobile and smart devices are switched off or set to 'silent' or 'do not disturb' modes during teaching sessions and other times when supervising pupils.
- disable or hide Bluetooth, 'AirDrop' or similar sharing and communication functions during teaching and learning sessions or when supervising pupils.
- not use personal mobile phones or smart devices during teaching, learning or supervision periods, unless written permission has been given in advance by the headteacher, for example, in emergency circumstances.
- ensure that any content brought onto site via personal mobile or smart devices is appropriate to their professional role and consistent with our behaviour and safeguarding expectations.

- Members of staff are not permitted to use their own personal mobile or smart devices for contacting pupils or their parents/carers.
  - Any preexisting relationships or circumstances that may compromise this requirement will be discussed with the DSL (Headteacher) and be formally recorded.
- Staff will only use school provided equipment:
  - to take photos or videos of pupils in line with our image use policy.
  - to work directly with pupils during learning/educational activities.
  - to communicate with parents/carers.
- Where remote or online learning takes place, staff will use school provided equipment wherever possible, in accordance with our Acceptable Use Policies. Where use of a personal device is unavoidable, this will be agreed in advance by the headteacher and supported by a risk assessment and clear safeguards.
- Any breach of this policy by a member of staff will be managed in line with the staff code of conduct policy, child protection policy and allegations management procedures.
- Where there is concern that a member of staff may have accessed, created or stored illegal content on a personal or school provided device, or may have committed a criminal offence using a device, the matter will be reported to the police and the Local Authority Designated Officer (LADO) in line with our staff code of conduct and allegations management procedures.

6. Pupils use of mobile and smart devices

- Pupils will be educated about the safe, responsible, and appropriate use of mobile and smart devices. This includes understanding expected standards of behaviour,

safeguarding risks and consequences of policy breaches at a level appropriate to their age and/or understanding.

- Safe and appropriate use of mobile and smart devices is taught as part of an embedded and progressive safeguarding education approach, using age-appropriate resources. Further information is set out in the school's child protection and relevant specific curriculum policies; RSHE policy and computing policy.
- The Gateway will ensure that online safety considerations are reflected across all relevant policies and procedures, including behaviour, safeguarding, acceptable use, anti-bullying and educational visits policies.
- Where concerns arise in relation to online activity, including incidents that occur outside the school/setting environment or during residential visits, pupils will be encouraged and supported to raise these concerns with staff.
- The school will ensure that pupils are able to access their mobile phone or other devices, where necessary and appropriate, to report concerns to staff about issues that have occurred online. This may include enabling limited or supervised access to a device for the purpose of seeking support or reporting a safeguarding concern.

Schools

- The Gateway operates as mobile phone free environment by default. Pupils are not permitted to use personal mobile phones or smart devices with similar functionality during the school day. This applies throughout the school day, including lessons, the time between lessons, breaktimes and lunchtime.
- This is achieved by:
    - **requiring personal mobile phones or smart devices to be handed in at the start of the school day and returned at the end of the day.**
- Any adaptations or reasonable adjustments necessary to support pupils' individual needs will be implemented in line with section 3.1.
- If a pupil needs to contact their parents or carers whilst on site, the office will contact them on their behalf e.g. a forgotten lunch box.
    - Parents are advised to contact their child via the school office; exceptions may be permitted on a case-by-case basis, as approved by the Headteacher.
- Where pupils' personal mobile or smart devices are used when learning at home, this will be in accordance with our Acceptable Use Policy and Remote Learning AUP.
- Personal mobile or smart devices must not be taken into examinations. Pupils 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.

Early Years

- Within our early years setting, children are unlikely to require access to personal mobile phones or smart devices whilst in our care.
- Any use of mobile phones or smart technology in relation to children within the setting is managed in line with safeguarding requirements, supervision expectations and the need to maintain safe, secure and developmentally appropriate environments for young children.
- This is achieved by:
  - **children not bringing personal mobile phones or smart devices into the setting.**
  - **ensuring that children do not have access to personal mobile phones or smart devices during their time in the setting.**
  - **supporting children's early understanding of safe and appropriate use of technology through age-appropriate safeguarding education and adult modelling, where relevant.**
- The Gateway recognises that some children may require access to mobile phones or smart devices as a reasonable adjustment or to support medical or individual needs. Any such arrangements will be considered on an individual basis, agreed in advance, and supported by clear safeguards and expectations as set out in section 3.1.

Residential Trips

- The school recognises that the risks associated with mobile phone use and online activity may differ during residential visits, trips and other activities taking place away from the school site.
- When planning and delivering residential visits, the school will remain vigilant to online safety risks and will ensure that appropriate safeguards are in place.
- Expectations regarding mobile phone and/or other smart devices use on residential trips will be clearly communicated to pupils, staff and parents/carers in advance and reflected in relevant risk assessments and visit planning documentation. Mobile phones and smart technology will not be permitted for pupils.

7. Visitors' use of mobile phones and smart devices

- Parents/carers and visitors, including volunteers and contractors, are expected to use mobile phones and smart devices in a way that safeguards our pupils and respects our policies and expectations.

- In The Gateway, this is achieved by:
    - **restricting the use of personal mobile phones and smart devices by visitors in areas where pupils are present.**
    - **permitting the use of mobile phones or smart devices only in designated areas or for specific purposes.**
    - **allowing access to mobile phones or smart devices where required for professional purposes, for example as part of agreed multi-agency working arrangements.**
- Appropriate signage and information are in place and information is in place to inform visitors of our expectations for safe and appropriate use of mobile or smart devices.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to comply with the setting's acceptable use of technology policy and other relevant safeguarding policies, including child protection.
- Where a visitor requires access to mobile phones or smart devices as part of their role when working directly with pupils, this will be discussed and agreed in advance with the headteacher or delegated senior leader.
- Any agreed arrangements for visitor access to mobile or smart technology will be documented and recorded by the school and with appropriate leadership approval. Where appropriate, this may include undertaking a risk assessment.
- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart devices and will report any breaches of this policy to the DSL or headteacher.

8. Communicating the policy and working with parents/carers

- The Gateway recognises that clear communication and effective partnership with parents/carers are essential to the successful implementation of this policy.
- The policy will be communicated to parents/carers, pupils and staff in a clear and accessible way. This will include publication on the school website, inclusion in induction materials, direct communication to parents/carers and ongoing reminders and communications throughout the year as appropriate.
- Communication with parents/carers will include the rationale for the policy, including its role in supporting learning, wellbeing and safeguarding.
- Where changes are made to expectations regarding mobile phones or smart devices, the school will provide parents/carers with appropriate notice and clear information about the rationale for the policy and how it will be implemented.

- Parents/carers are expected to support the school's approach and to work in partnership with staff to reinforce expectations, particularly where policies are breached or concerns arise.
- Where concerns or policy breaches occur, the school will seek to engage constructively with parents/carers to support positive outcomes for children.
- Where individual adaptations or reasonable adjustments are required, for example to support medical needs or disabilities, these will be discussed and agreed directly with parents/carers and recorded appropriately.
- Where parents/carers have questions or concerns, the school will address these in a timely manner and clearly communicate any reasons for prohibiting/restricting the use of mobile phones.
- The school will seek to work constructively with parents/carers to promote children's wellbeing, including supporting safe and responsible use of mobile phones and smart technology beyond the school environment.

9. Responding to policy breaches

- All members of the community are expected to report concerns or breaches of this policy in line with existing school policies and procedures. This includes **our child protection and behaviour policy.**
- Where pupils breach this policy, the school/setting will respond proportionately and appropriately.
    - Appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy.
    - Parents/carers will be informed of concerns or breaches as appropriate.
    - Where there is a concern that a child is at risk of harm, the school/setting will respond in line with the child protection policy.
- Where incidents are investigated, leadership staff will review the circumstances, identify any lessons learned and implement changes to policy, procedures or curriculum provision where required.
- The school/setting expects staff, parents/carers and pupils to work in partnership to resolve concerns and support positive outcomes.
- All members of the school community are expected to respect confidentiality and to follow official procedures when reporting concerns.
- Pupils and parent/carers will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

- Where the school/setting is unsure how to proceed with an incident or concern, the Designated Safeguarding Lead (DSL), a deputy DSL will seek advice from the local authority or other relevant agencies, in line with the child protection policy.

9.1 Searching, screening and confiscation of mobile phones and smart devices

- Electronic devices, including mobile phones and smart devices, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children (including images generated by artificial intelligence), pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.
- Where there are any concerns regarding pupils' use of mobile phones, smart devices, they will be dealt with in accordance with our existing policies, including anti-bullying, child protection and behaviour.
- Staff may confiscate a pupils' personal mobile or smart device where they reasonably believe it is being used to contravene our school policies, for example our child protection or behaviour policy, or where confiscation is necessary to safeguard others or maintain a safe environment.
- Confiscated devices will be stored securely and released to parents/carers in line with the school's behaviour policy. They will returned at the end of the school day alongside discussion with the Headteacher or deputy Headteacher linked to the issue.
- Where a concern involves potentially indecent images or videos of children, including AI generated content, staff will respond in line with the child protection policy. Devices will be confiscated, staff will not view the content, and the matter will be referred to the Designated Safeguarding Lead (DSL) or deputy without delay.
- Where there is reasonable suspicion that data or files on a device may be illegal or may constitute evidence of a criminal offence, the device will be confiscated and handed over to the police for further investigation.
- Mobile phones and similar smart devices are identified as items that may be searched for, in line with statutory powers and the DfE **Searching, Screening and Confiscation'** guidance.
- Searches of children and their possessions will only be carried out in accordance with the DfE **Searching, Screening and Confiscation'** guidance.
- Staff will respond in line with our child protection policy and follow the most appropriate safeguarding response if they find images, data or files on a child's electronic device that they reasonably suspect are likely to put a person at risk.

- The DSL (or deputy) will always be informed of any searching incidents where authorised members of staff have reasonable grounds to suspect a child was in possession of prohibited items, as identified in our behaviour policy.
- The DSL (or deputy) will be involved without delay if staff believe a search of a child's personal mobile or smart device has revealed a safeguarding risk.
- In exceptional circumstances and in accordance with our behaviour policy and the DfE 'Searching, Screening and Confiscation' guidance, the headteacher or authorised members of staff may examine or erase data or files if there is a good reason to do so.
    - In determining whether there is a 'good reason' to examine images, data or files, the headteacher or an authorised member of staff will need to reasonably suspect that the images, data or files on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.
    - In determining whether there is a 'good reason' to erase any images, data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable.
    - If the data or files are not suspected to be evidence in relation to an offence, the headteacher or an authorised member of staff may delete the images, data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the child and/or the parent refuses to delete the data or files themselves.
- If the headteacher or a member of staff finds any data or files that they suspect might constitute a specified offence, they will be delivered to the police as soon as is reasonably practicable.

10. Policy monitoring and review

- The Gateway will review this policy at least annually to ensure it remains appropriate, relevant and up to date. The policy will also be reviewed following any changes to national or local guidance, identified safeguarding concerns, or significant changes to the setting's use of technology or technical infrastructure.
- The school monitors the use of internet and technology on school/setting provided devices and systems as part of its safeguarding responsibilities. Monitoring and filtering arrangements are designed to be lawful, proportionate and appropriate to the

setting's context. Further information about the appropriate filtering and monitoring systems in place are detailed in our Child Protection Policy. Any issues identified through monitoring will be addressed through appropriate safeguarding responses and incorporated into action planning.

- Members of the school community will be informed of expectations relating to the use of mobile and smart technology and how compliance with this policy is monitored. This may include, for example, Acceptable Use Policies, staff training, induction processes, and communication with parents/carers.