St James' CE Primary School

Mobile and Smart Technology Policy

Key Details

Designated Safeguarding Lead (s): Sarah Greenfield, Assistant Headteacher

Named Governor with lead responsibility: Nina Skomorowski-Brown

Date written/updated: Updated September 2026

Date agreed and ratified by Governing Body: 23rd September 2026

Date of next review: September 2027

This policy will be reviewed **at least** annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

1. Policy aims and scope

- This policy has been written by St James' CE Primary School , involving staff, pupils and parents/carers, building on Kent County Councils 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) '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 devices and smart technology.
    - St James' CE Primary School 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), Sarah Greenfield, is recognised as having overall responsibility for online safety.
- This policy applies to all access to and use of all mobile and smart technology on site; this includes but is not limited to mobile/smart 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 and/or images.
- 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 setting (collectively referred to as "staff" in 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 policy, including searching, screening and confiscation
    - 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
    - Social media

3. Safe use of mobile and smart technology expectations

- St James' CE Primary School recognises that use of mobile and smart technologies is part of everyday life for many pupils, staff and parents/carers.
- Electronic 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 are not permitted to be used in specific areas on site such as pupil toilets and off site such as changing rooms or swimming pools.
- The sending of abusive or inappropriate messages or content, including via personal mobile devices and/or smart technology is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying, staff code of conduct, behaviour and child protection policies.
- All members of the St James' CE Primary School community are advised to ensure that their personal mobile and smart technology devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our staff code of conduct, behaviour or child protection policies.

4. School provided mobile phones and devices

- Members of staff will be issued with a work phone number in addition to their work email address, where contact with pupils or parents/carers is required or to enable site staff to be contactable whilst on site.
- Staff providing formal remote/online learning will do so using school provided equipment in accordance with our Acceptable Use Policy (AUP) and remote learning AUP.
- School mobile phones and devices (laptops, iPads) will be suitably protected via a password/PIN and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with our staff code of conduct, acceptable use of technology and child protection policies.
- Where staff are using school provided mobile phones and 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.

5. Staff use of mobile and smart technology

- Members of staff will ensure that use of any mobile and smart technology, including personal phones, wearable technology and other mobile/smart devices, will take place in accordance with the law, as well as relevant school policy and procedures, including

confidentiality, child protection, data security, staff code of conduct and Acceptable Use Policies.

- Staff will be advised to:
  - Keep personal mobile and smart technology devices in a safe and secure place during lesson time.
  - Keep personal mobile phones and devices switched off or set to 'silent' or 'do not disturb' modes during lesson times.
  - Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
  - Not use personal mobile or smart technology devices during teaching periods, unless written permission has been given by the headteacher, such as in emergency circumstances. In the event of a serious behaviour incident, members of staff may use a personal device to contact the headteacher/deputy headteacher if they cannot do so by any other means.
  - Ensure that any content bought onto site via personal mobile and smart technology devices is compatible with their professional role and our behaviour expectations.
- Members of staff are not permitted to use their own personal mobile and smart technology devices for contacting pupils 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 (or deputy DSL) and/or headteacher.
- Staff will only use school provided equipment (not personal devices):
  - to take photos or videos of pupils in line with our image use policy.
  - to work directly with pupils 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, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy and remote learning AUP.
- If a member of staff breaches our policy, action will be taken in line with our staff code of conduct, child protection policy, discipline and conduct policy, and allegations policy.
- If a member of staff is thought to have illegal content saved or stored on a personal mobile or other 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.

6. Pupils use of mobile and smart technology

- Pupils 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 pupils as part of an embedded and progressive safeguarding education approach using age-appropriate

sites and resources. Further information is contained within our child protection and relevant specific curriculum policies e.g. PSHE, RSE and Computing.

- Personal mobile or smart technology devices **<u>are not</u>** permitted on site for pupils (except in certain circumstances outlined below).
- St James' CE Primary School does not allow pupils to bring personal devices (including internet enabled smart watches) and mobile phones to school except with written permission from the headteacher or deputy headteacher, given in exceptional circumstances following a risk assessment. For those pupils who are given permission, St James' CE Primary School expects pupils' personal devices and mobile phones to be handed in to the class teacher who will store them out of reach of other children, other than when being used for the permitted purpose. 'Smart' phones/devices will only be allowed in some very occasional circumstances e.g. for medical needs.
- If a pupil needs to contact their parents or carers whilst on site, they will be allowed to use a school phone in the office.
  - 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.
- If a child/pupil/student requires access to personal mobile or smart technology devices in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the headteacher/deputy headteacher and risk assessed prior to use being permitted.
  - Any arrangements regarding access to personal mobile or smart technology 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 pupil and their parents/carers before use is permitted.
- Where pupils' personal mobile or smart technology 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 technology devices must not be taken into examinations. Pupils 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.

6.1 Searching, screening and confiscation of electronic devices

- Electronic devices, including mobile phones, 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, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.
- Where there are any concerns regarding pupils' use of mobile or smart technology or policy breaches, 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 technology device if they believe it is being used to contravene our school policies, for example our child protection or behaviour policy or if written permission has not been given by the headteacher/deputy headteacher.
- Personal mobile or smart technology devices that have been confiscated will be held by a member of SLT in a secure place and released to parents/carers at the end of the day or after a longer period for a repeat offence.
- Where a concern involves a potentially indecent image or video of a child, staff will respond in line with our child protection policy and will confiscate devices, avoid looking at any content, and refer the incident to the Designated Safeguarding Lead (or deputy) urgently as they will be most appropriate person to respond.
- Where a concern involves potentially indecent images/videos of children, including images/videos generated by Artificial Intelligence (AI), on a pupil's personal mobile or smart technology device, staff will respond in line with our child protection policy; they will confiscate devices, avoid looking at any content and refer the incident to the DSL (or deputy) urgently.
- If there is suspicion that data or files on a pupil's personal mobile or smart technology device may be illegal, or may provide evidence relating to a criminal offence, the device will be confiscated and handed over to the police for further investigation.
- If deemed to be necessary and appropriate, searches of personal mobile or smart technology devices may be carried out in accordance with our behaviour policy and 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 pupil's electronic device that they reasonably suspect are likely to put a person at risk.
- The Designated Safeguarding Lead (or deputy) will always be informed of any searching incidents where authorised members of staff have reasonable grounds to suspect a pupil was in possession of prohibited items, as identified in our behaviour policy.
- The Designated Safeguarding Lead (or deputy) will be involved without delay if staff believe a search of a pupil's personal mobile or smart technology 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 pupil 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.

7. Visitors' use of mobile and smart technology

- Parents/carers and visitors, including volunteers and contractors, are expected to ensure that:
  - mobile phones and personal devices are not used in any area except the office waiting area, unless permission is granted by the headteacher/deputy headteacher for use for a specific purpose, for example, as part of multi-agency working arrangements.
- Appropriate signage and information are in place in the office entrance and St James' Safeguarding Leaflet to inform visitors of our expectations for safe and appropriate use of personal mobile or smart technology.
- 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 pupils as part of multi-agency activity, this will be discussed with the headteacher 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 of any breaches of our policy.

8. Policy monitoring and review

- Technology evolves and changes rapidly. St James' CE Primary School 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 monitor internet and technology use taking place via all school provided devices and systems and regularly evaluate online safety mechanisms to ensure this policy is consistently applied. Full information about the appropriate filtering and monitoring systems in place are detailed in our Child Protection Policy. Any issues identified as part of the implementation of our monitoring approaches will be incorporated into our action planning.
- All members of the community will be made aware of how the school will monitor policy compliance, through AUPs, staff training, classroom management.

9. 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 (child protection and behaviour policies).
- Where pupils breach this policy:
    - appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy.
    - concerns will be shared with parents/carers as appropriate.
    - we will respond in line with our child protection policy, if there is a concern that a child is at risk of harm.
- 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 pupils 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.
- Pupils' 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 will seek advice from the local authority or other agencies, as appropriate, in accordance with our child protection policy.