St Gerard's Catholic Primary School

Online safety, Mobile and Smart Technology Policy

Key Details

Designated Safeguarding Lead (s): Mr J Wilson

Named Governor with lead responsibility: H Macilwraith

Date agreed and ratified by Governing Body: November 2026

Date of next review: October 2028

1. Policy aims and scope

- This policy has been written by J Wilson, involving staff, children and parents/carers, building on our Local Councils LADO and 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' and 'Mobile Phones in Schools' .
- The purpose of this policy is to safeguard and promote the welfare of all members of our community when online, using mobile devices and smart technology.
    - St Gerard's recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all children 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), Mr J Wilson, 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 children, 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
    - Behaviour and discipline policy
    - Child protection policy
    - Staff code of conduct/staff behaviour policy
    - Confidentiality policy
    - Curriculum policies
    - GDPR
    - Staff Handbook

3. Safe use of mobile and smart technology expectations

- St Gerard's recognises that use of mobile and smart technologies is part of everyday life for many children, 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.
    - In regards to Pupils, only our Y6 children, who walk home, are allowed to bring in mobile phones, these should always be stored securely in the class teacher's cupboard.
- Mobile devices and other forms of smart technology are not permitted to be used in specific areas on site
- 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, behaviour and child protection policies
- All members of our 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 behaviour or child protection policies.

4. 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 behaviour/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 (locked in a drawer or cupboard) 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.
    - 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 children 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 and headteacher.
- Staff will only use school provided equipment (not personal devices):

    - to take photos or videos of children.
    - to work directly with children 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.

5. Children/pupils/students use of mobile and smart technology

'Behaviour in School: Advice for headteachers and school staff' states:

"Headteachers should decide if mobile phones can be used during the school day. Many pupils, especially as they get older, will have one of their own. Allowing access to mobiles in school introduces complexity and risks, including distraction, disruption, bullying and abuse, and can be a detriment to learning. Headteachers should consider restricting or prohibiting mobile phones to reduce these risks.

If headteachers decide not to impose any restrictions on mobile phones, they should have a clear plan to mitigate the risks of allowing access to phones. This plan, as part of the school's behaviour policy, should outline the approach to mobile phones and be reiterated to all pupils, staff and parents throughout the school year. Headteachers should ensure it is consistently and fairly applied."

Headteachers may also wish to access the non-statutory DfE Mobile Phones in Schools guidance as part of their decision making.

- Children 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 children as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources.
- Personal mobile or smart technology devices is not permitted on site for children
    - Children are not permitted to use personal mobile or smart devices whilst on the school/setting site. Where these are required, for example for safety reasons when children/young people are transporting to and from school, devices should be turned off/placed on silent and handed into the school/setting office in the morning. They can then be collected at the end of day.
    - Personal mobile or smart devices will not be used by children during lessons or formal educational time.
    - Staff will only allow children to use smart devices or school laptops that are monitored by our classroom.cloud system.

- Where staff believe children have used smart devices during less time- for example taking pictures, then that pupil will lose the right to walk home alone- school will ask parents to collect.
- Any arrangements regarding access to personal mobile or smart technology devices in exceptional circumstances will be documented and recorded by the school.

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 childrens' 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 child's personal mobile or smart technology device if they believe it is being used to contravene our child protection or behaviour policy.
- Personal mobile or smart technology devices that have been confiscated will be held in a secure place and released to parents/carers.
- 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 DSL (or deputy) urgently as they will be most appropriate person to respond.
- If there is suspicion that data or files on a child's personal mobile or smart technology device may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation

6. Policy monitoring and review

- Technology evolves and changes rapidly. St Gerard's will review this policy at least every two years. 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. Any issues identified as a result of our monitoring approaches will be incorporated into our action planning.

7. 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**.**
- Where children 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 children 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.
- Children's parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.