Mobile and Smart Technology Policy



Key Details

Designated Safeguarding Lead (s): Lianne Jones Named Governor with lead responsibility: Myriam Bournki

Date written/updated: Sept 2023

Date agreed and ratified by Governing Body: Awaiting Date of next review: Sept 2024

This policy will be reviewed <u>at least</u> 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 Sandgate Primary School involving staff, children and parents/carers, building on The Education People's mobile and smart technology policy template with specialist advice and input as required, taking into account the DfE statutory guidance 'Keeping Children Safe in Education' 2022, Early Years and Foundation Stage 2021, 'Working Together to Safeguard Children' 2018, 'Behaviour in Schools Advice for headteachers and school staff' 2022, and the local Kent Safeguarding Children Multiagency Partnership (KSCMP) procedures.
- The purpose of this policy is to safeguard and promote the welfare of all members of the Sandgate Primary School community when using mobile devices and smart technology.
 - Sandgate Primary School 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), Lianne Jones, Deputy Headteacher, 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 mobile 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
 - Acceptable Use Policies (AUP)
 - Behaviour and policy
 - Child protection policy
 - Code of conduct/staff behaviour policy
 - Confidentiality policy
 - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
 - Data security

3. Safe use of mobile and smart technology expectations

- Sandgate Primary School 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 the Sandgate Primary School community are advised to:
 - take steps to protect their mobile phones or personal 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 their phones or devices.
- Mobile phones and personal devices are not permitted to be used in specific areas on site, such as changing rooms, toilets and cloakrooms
- The sending of abusive or inappropriate messages or content, including via personal smart devices and mobile phones 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 Sandgate Primary School community are advised to ensure that their mobile phones and personal 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. Sandgate Primary 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 children or parents/carers is required. **This is applicable for school trips and the Year 6 residential trip.**
- Staff providing formal remote/online learning will do so using school provided equipment in accordance with our Acceptable Use Policy (AUP)/remote learning AUP.
- School mobile phones and devices will be suitably protected via a passcode 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/behaviour policy, acceptable use of technology policy and other relevant policies.
- Where staff and/or children are using school provided mobile phones and/or 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 and mobile devices, will take place in accordance with the law, as well as relevant school policy and procedures, such as confidentiality, child protection, data security staff behaviour/code of conduct and Acceptable Use Policies.
- Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place (classroom cupboard) during lesson time.
- Keep personal mobile phones and devices switched off or set to 'silent' mode during lesson times.
- Not use personal devices during teaching periods unless permission has been given by the headteacher such as in emergency circumstances.
- Ensure that any content bought onto site via personal mobile phones and devices is compatible with their professional role and our behaviour expectations.
- Members of staff are not permitted to use their own personal phones or 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
- Staff will only use school provided equipment (not personal devices):
 - \circ to take photos or videos of children in line with our image use policy.
 - 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. Staff will follow clear guidance outlined in the Acceptable Use Policy and/or remote learning AUP.
- If a member of staff breaches our policy, action will be taken in line with our staff behaviour policy/code of conduct and allegations policy.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal 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. Children's use of mobile and smart technology

'Behaviour in School: Advice for headteachers and school staff' 2022 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."

- 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. Further information is contained within our child protection and relevant specific curriculum policies insert name of policies, for example, RSE and Computing.
- Mobile phones and/or personal devices will not be used on site by children/pupils/students.
- Sandgate Primary School expects children/pupils/students' personal devices and mobile phones to be kept safe and secure when on site. Phones are switched off and looked after by the class teacher in a locked cupboard. See separate Child Friendly Mobile Phone policy.
- If a child needs to contact their parents or carers whilst on site, they will be allowed to use an office phone.
- Where children mobile phones or personal devices are used when learning at home, this will be in accordance with our Acceptable Use Policy and/or Remote Learning AUP.
- Mobile phones and personal devices must not be taken into examinations. Children 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 Screening, searching 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 children use of mobile technology or policy breaches, they will be dealt with in accordance with our existing policies, including anti-bullying, child protection, online safety and behaviour.
- Staff may confiscate a child's mobile phone or device if they believe it is being used to contravene our child protection or behaviour policy.
- Mobile phones and devices that have been confiscated will be held in a secure place and released to parents/carers. **They will be held in the school office.**
- 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.

- If there is suspicion that data or files on a child/pupils/student's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.
- If deemed to be necessary and appropriate, searches of mobile phones or personal devices may be carried out in accordance with our behaviour policy.
- 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 be involved without delay if staff believe a search of a pupil's device has revealed a safeguarding risk.
- In exceptional circumstances and in accordance with our behaviour policy (link) and the DfE <u>`Searching, Screening and Confiscation'</u> guidance, the headteacher or authorised members of staff may examine or erase data or files if there is a good reason to do so. Ensure your policy is in line with the DfE <u>`Searching, Screening and Confiscation'</u> guidance. The DfE <u>`Searching, Screening and Confiscation'</u> guidance states (77 79)
 - 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: phones are on silent when in the school building. Phones and devices must not be used around children nor shown to them. Phones and devices should not be used around any child nor should they be used in corridors or classrooms.
- Appropriate signage and information are in place (**list details of how your setting does this, for example, posters, leaflets**) to inform visitors of our expectations for safe and appropriate use of personal devices and mobile phones.

- 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 children 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. Sandgate 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 will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied. Any issues identified will be incorporated into our action planning.
- All members of the community will be made aware of how the school will monitor policy compliance. This is achieved via annual child protection training, through AUPS, Staff Code of Conduct and bulletin reminders.,

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.
- 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, 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 <u>Education People's Education Safeguarding Service</u> or other agency in accordance with our child protection policy.