Garlinge and Parkside Schools and Nurseries Federation

Mobile and Smart Technology Policy

Key Details

Designated Safeguarding Leads (DSL)		
Anna Northrop	Head of School (Lead DSL)	Garlinge
James Williams	Executive Headteacher	Garlinge
Stephen Cope	Head of School	Garlinge
Sarah Mansfield	Safeguarding Officer	Garlinge
Alison Gillatt	Family Liaison Officer	Garlinge
Anthea McLevy	Head of School (Lead DSL)	Parkside
Kirsty Thompson	SENCO	Parkside

Named Governor with lead responsibility: **Hannah Perry**

Date written/updated: **June 2024**

Date agreed and ratified by the Senior Leadership Team: **24 June 2024**

Date of next review: **June 2025**

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.

Contents

1. Policy aims and scope

- This policy has been written by Garlinge and Parkside Schools and Nurseries Federation, building on Kent County Councils Education Safeguarding Service's mobile and smart technology policy template, with specialist advice and input as required.

- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education', 'Early Years and Foundation Stage', 'Working Together to Safeguard Children', 'Behaviour in Schools Advice for headteachers and school staff', Searching, screening and confiscation at school' 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 school community when using mobile devices and smart technology.

  - The 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 Policies, the Designated Safeguarding Lead (DSL), Anna Northrop (Garlinge) and Anthea McLevy (Parkside) are 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 teams, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of Garlinge Primary School and Nursery and Parkside Community Foundation Primary School (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
  - Image Use policy
  - Child Protection policy
  - Staff Code of Conduct
  - Curriculum policies, such as: Computing, Personal Social Health and Economic (PSHE) and Relationships and Sex Education (RSE)

o Data security
o Online Safety policy
o Social Media policy

3. Safe use of mobile and smart technology expectations

- The school recognises that use of mobile and smart technologies is part of everyday life for many pupils, staff, parents and 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:

  o 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.
  o 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; this includes medical rooms, changing rooms and toilets.

- 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, child protection and online safety policies.

- All members of the 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, child protection or online safety policies.

4. School provided mobile phones and devices

- Some members of staff will be issued with a work phone number in addition to their work email address, where contact with pupils or parents and carers is required.

- Staff providing formal remote/online learning will do so using school provided equipment in accordance with our Acceptable Use Policy (AUP).

- School mobile phones, iPads, laptops, tablets and computers will be suitably protected via a password and must only be accessed or used by members of staff and/or pupils.

- School mobile phones and/or devices will always be used in accordance with our staff code of conduct/behaviour policy, online safety and acceptable use of technology policies and other relevant policies.

- Where staff and/or pupils 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, wearable technology and other mobile/smart devices, will take place in accordance with the law, as well as relevant school policy and procedures, including child protection, data security, staff code of conduct, online safety and acceptable use of technology policies.

- Staff will be advised to:

  o Keep personal mobile and smart technology devices in a safe and secure place such as a locked drawer or locker during lesson time.
  o Keep personal mobile phones and devices switched off or set to 'silent' or 'do not disturb' modes during lesson times.
  o Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
  o Not use personal mobile or smart technology devices during teaching periods, unless written permission has been given by the Senior Leadership Team such as in emergency circumstances.
  o 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 unless authorised by the Senior Leadership Team.

  o Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the Senior Leadership Team.

- Staff will only use school provided equipment (not personal devices):

  o to take photos or videos of pupils in line with our image use policy.
  o to work directly with pupils during lessons/educational activities.
  o to communicate with parents and 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 Senior Leadership Team, following a formal risk assessment. Staff will follow clear guidance outlined in the acceptable use of technology policies.

- If a member of staff breaches our policy, action will be taken in line with our child protection policy, staff code of conduct and discipline and conduct policy and procedure.

- 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 discipline and conduct policy and procedure.

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 for example, Computing, PSHE and RSE.

- Personal mobile or smart technology devices is not permitted for use on site for pupils.

  - Pupils are not permitted to use personal mobile or smart devices whilst on the school site. Where these are required, for example for safety reasons when pupils are transporting to and from school, devices should be turned off and handed into the class teacher or school office in the morning where they will be locked away until the end of day when they can be collected.

- If a pupil needs to contact their parents or carers whilst on site, they will be allowed to use a school office phone.

  - Parents are advised to contact their child via the school office.

- If a pupil requires access to personal mobile or smart technology devices in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the Senior Leadership Team 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 learner and/or their parents or 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 of technology policies.

- 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, behaviour, child protection, online safety.

- Staff may confiscate a pupils' 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 such as a locked drawer or cupboard in the classroom and released to parents and carers at the end of the day.

- 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 pupil'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.

- If deemed to be necessary and appropriate, searches of personal mobile or smart technology devices may be carried out in accordance with our child protection 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 a 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.

- The Designated Safeguarding Lead (or a 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 and the DfE 'Searching, Screening and Confiscation' guidance, the Executive Headteacher or authorised members of staff may examine or erase data or files if there is a good reason to do so.

  o In determining whether there is a 'good reason' to examine images, data or files, the Executive 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.

  o 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.

  o If the data or files are not suspected to be evidence in relation to an offence, the Executive 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 Executive 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 not permitted to use mobile phones and personal devices.

- Appropriate signage and information are in the main school entrance 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 ensure they have permissions from a member of the management team 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 Executive Headteacher or department manager prior to use being permitted.

  o Any arrangements regarding agreed visitor access to mobile/smart technology will be authorised by the SLT, documented and recorded by the school.

- 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 a deputy) of any breaches of our policy.

8. Policy monitoring and review

- Technology evolves and changes rapidly. The 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 and online safety policies. Any issues identified as a result 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 and 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. This includes anti-bullying, behaviour, child protection, staff code of conduct, online safety and social media polices.

- Where pupils breach this policy:

  o appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy.
  o concerns will be shared with parents and carers as appropriate.
  o 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) will seek advice from Kent County Councils Education Safeguarding Service or other agency in accordance with our child protection policy.