BIRCHINGTON CE PRIMARY SCHOOL

LEARNING AND GROWING; SAFE IN GOD'S LOVE

MOBILE AND SMART TECHNOLOGY POLICY

Key Details

Designated Safeguarding Leads:

Mrs Louise Wilson (Lead)
Mr Jonathan Forwood
Mrs Katie Downs
Mrs Sarah Cooper

Named Governor with lead Safeguarding responsibility:

Ms Loraine Bant

Date written:
December 2024

Date agreed and ratified by Governing Body:
To be ratified December 2024

Date of next review:
September 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.*

This policy is based on the 2024-25 Online Safety Policy template provided by KCC's Education Safeguarding Service.

1. Policy aims and scope

- This policy has been written by Leaders at Birchington CE Primary School, involving staff, learners and parents/carers, building on the Kent County Council's Education Safeguarding Services policy template, with specialist advice and input as required
- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2024, Early Years and Foundation Stage 2023, 'Working Together to Safeguard Children' 2018, and our local Kent Safeguarding Children Multi-Agency Partnership (KSCMP) procedures and support from the Kent County Council LADO and Education Safeguarding Advisory Service .
- The purpose of this policy is to safeguard and promote the welfare of all members of the Birchington CE Primary School community when using mobile devices and smart technology.
    - Birchington 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), Louise Wilson (Headteacher), is recognised as having overall responsibility for online safety.
- All aspects of safeguarding, including the use of mobiles and other smart technology, are an integral part of our school's Christian Vision.
- This policy applies to 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
    - Staff Code of Conduct
    - Behaviour Policy
    - Child Protection Policy
    - Confidentiality Policy
    - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHCE), Citizenship and Relationships and Relationship & Sex Education (RSE)
    - GDPR and Data Protection
    - Image Use Policy
    - Online Safety Policy
    - Social Media

3. Safe use of mobile and smart technology expectations

- Birchington 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 the Birchington CE 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 other forms of smart technology are not permitted to be used in specific areas on site, such as such as classrooms when children are getting changed and the 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 Policy, Staff Code of Conduct, Behaviour Policy and Child Protection Policy.
- All members of the Birchington CE Primary School community are advised to ensure that their personal mobile devices and/or smart technology do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our Code of Conduct and Child Protection Policy.

4. Staff use of 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 other members of staff or parents/carers is required.
- Staff providing formal remote learning will do so using Birchington CE Primary School provided equipment in accordance with our Remote Learning AUP.
- Birchington CE Primary School provided personal mobile devices and/or smart technology will be suitably protected via a passcode/password/pin and must only be accessed or used by the member of staff to whom the phone has been given. Matt Horsburgh – IT Network Manager – will have the list of all passcodes. This must not be changed without the Headteacher's permission and with the knowledge of the IT Network Manager
- Staff will only use Birchington CE Primary School provided equipment:
    - 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 or other staff during school hours.
    - to conduct any remote learning
- Birchington CE Primary School mobile phones and devices will always be used in accordance with our Staff Code of Conduct, Behaviour Policy, and Online Safety and Acceptable Use of Technology Policy
- Where staff are using Birchington CE Primary 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 Birchington CE Primary School policy and procedures, such as Confidentiality, Child Protection Policy, Staff Code of Conduct and Acceptable Use Policies.
- Staff will be advised to:
    - Keep personal mobile phones and personal devices in a safe and secure place (for example, locked in a drawer or in an inaccessible 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.
    - Ensure that any content bought onto site via personal mobile or smart technology is compatible with their professional role and our behaviour expectations.
- Members of staff are not permitted to use their own 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 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 only use Birchington CE Primary School provided equipment.
- If a member of staff breaches our policy, action will be taken in line with our Staff Code of Conduct and Managing 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 Managing 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.
- Year 5/6 children may bring a mobile phone to school if they need to and they adhere to the following rules:
    - mobile phones must be turned off and not used the whole time the children are on the school site – this includes walking to and from their classrooms at the start and end of the school day

    - the mobile phones will be kept in a box by the class teacher and they will be returned to the children when the class is dismissed at the end of the day
    - parents and carers are told that their children must not bring in a mobile phone that has social media apps on it
    - If there are incidents of misbehaviour on social media apps that are reported to the school, the school may decide to withdraw permission for that smartphone to be brought to school. Parents and carers may then choose to have their child bring a non-smartphone instead.
- 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 Computing Policy
- Personal mobile or smart technology devices will not be used on site by pupils
- If parents or carers need to be contacted during the school day about their child, this will be done by a member of the school office
    - Parents are advised to contact their child via the school office
- If a pupil requires access to a personal device in exceptional circumstances for example medical assistance and monitoring, this will be discussed with the Headteacher prior to use being permitted.
    - Any arrangements regarding access to personal 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/or their parents carers before use is permitted.
- Where pupils' personal devices, or school provided devices, are used when learning at home, this will be in accordance with our Remote Learning AUP.
- Mobile phones and personal devices must not be taken into tests. Pupils found in possession of a mobile phone or personal device which facilitates communication or internet access during a test will be reported to the appropriate agency responsible for testing. This may result in the withdrawal from that test.

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 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, Online Safety and Behaviour.
- Staff may confiscate a pupils' 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 the school office and released to parents/carers and 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 DSL or a 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 device 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 Headteacher 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 Headteacher 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 only permitted for specific purposes and within specific areas:
    - Photos/videos (at school performances/Sports Days). Any photos/videos taken must be for personal use only. Parents and carers are reminded at performances that photos/videos of children are not to be uploaded to social media unless a parent/carer has the permission of all the parent/carers of the children in the photos/videos.
    - Parents and carers are allowed use mobile phones at drop off and pick up, if necessary
    - Parents/carers/professional visitors: mobile phones only to be used in offices, meeting rooms and in halls (for school performances – see above)
    - Contractors: if necessary and only for the nature of their reason to be on the school site
- Appropriate signage and information are in place in the school office to inform visitors of our expectations for safe and appropriate use of personal mobile or smart technology device.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use personal mobile or smart technology devices in accordance with our Acceptable Use of Technology Policy and other associated policies, including Child Protection.
- If visitors require access to personal mobile or smart technology devices, 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 personal mobile or smart technology devices and will inform the Headteacher of any breaches of our policy.

8. Policy monitoring and review

- Technology evolves and changes rapidly. Birchington 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 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.

- To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.

- The named Governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.

- All members of the community will be made aware of how our school will monitor policy compliance.
- All members of the community will be made aware of how the school will monitor policy compliance. This will be achieved by AUPs, staff training and classroom management.

9. Responding to Online Risks and/or Policy Breaches

- All members of the community:
    - are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence.
    - are informed of the need to report policy breaches or concerns in line with existing school policies and procedures. This may include:
        - Child Protection Policy.
    - will respect confidentiality and the need to follow the official procedures for reporting concerns.
    - will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
    - will be made aware of how the school will monitor policy compliance by:
        - AUPs, staff training, classroom management.
    - are expected to adopt a partnership with the school to resolve issues.

- If appropriate, after any investigations are completed, the DSL and leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.

- If we are unsure how to proceed with an incident or concern, the DSL/Headteacher or Deputy DSL will seek advice from KCC's Education Safeguarding Service in accordance with our Child Protection Policy.

- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm.

- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local schools are involved or the wider public may be at risk, the DSL/Headteacher will speak with the police **or** KCC's Education Safeguarding Service first, to ensure that potential criminal or child protection investigations are not compromised.