## Castle Hill CP School

# **Mobile and Smart Technology Policy**



#### **Key Details**

Designated Safeguarding Lead: Pete Talbot, Headteacher

Deputy Designated Safeguarding Leads: Sarah Merritt, Sue Stockley

Named Governor with lead responsibility: Rebecca Farrell-Southin

Date written/updated: September, 2023

Date agreed and ratified by Governing Body: October, 2023

Date of next review: October 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 Castle Hill CP School, involving staff, children and parents/carers, building on Kent County Council's 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 '<u>Keeping Children Safe in Education</u>', <u>Early Years and Foundation Stage</u>, '<u>Working Together to Safeguard Children</u>', '<u>Behaviour in Schools Advice for headteachers and school staff</u>', '<u>Searching</u>, <u>screening and confiscation at school</u>' and the local <u>Kent Safeguarding Children Multi-agency Partnership</u> (KSCMP) procedures.
- The purpose of this policy is to safeguard and promote the welfare of all members of Castle Hill CP School's community when using mobile devices and smart technology.
  - Castle Hill CP 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), Pete Talbot, Headteacher is recognised as having overall responsibility for online safety.
- This policy applies to all who have 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, iPads, 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, guidance, practices and action plans, including but not limited to:
  - o Acceptable Use Policies (AUP)
  - o Anti-bullying
  - o Behaviour for Learning
  - o Child Protection
  - Staff Code of Conduct
  - o Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
  - o Data protection and information sharing
  - o Image Use
  - o Searching, screening and confiscation
  - o Social media



#### 3. Safe use of mobile and smart technology expectations

- Castle Hill CP 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 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 changing rooms and toilets or specific areas off-site such as changing rooms, toilets and 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, Behaviour for Learning, Code of Conduct and Child Protection policies.
- All members of the Castle Hill CP 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 for Learning, Code of Conduct or Child Protection policies.

#### 4. Castle Hill CP School's 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.
- Staff providing formal remote/online learning will do so using Castle Hill CP School's provided equipment in accordance with our Acceptable Use Policies (AUP).
- Castle Hill CP School's mobile phones and devices will be suitably protected via a passcode/password/PIN where possible and must only be accessed or used by delegated members of staff and/or children.
- Castle Hill CP School's mobile phones and devices will always be used in accordance with our staff Code of Conduct, Behaviour for Learning and Acceptable Use Policies.
- Where staff and/or children are using Castle Hill CP 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 Castle Hill CP School policy and procedures,



including Confidentiality, Child Protection, Data protection and information sharing, 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 e.g. locked in a locker/drawer during lesson time.
- Keep personal mobile phones and devices switched off or set to 'silent' or 'do not disturb' modes when they are with the children.
- Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled when they are with the children.
- Not use personal mobile or smart technology devices when they are with the children unless 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/carers.
  - Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the DSL/Headteacher.
- Staff will only use Castle Hill CP School provided equipment (not personal devices):
  - o to take photos or videos of children in line with our Image Use policy.
  - to work directly with children during lessons/educational activities.
  - o to communicate with parents/carers.
- Where remote learning activities take place, staff will only use Castle Hill CP School provided equipment.
- If a member of staff breaches our policy, action will be taken in line with our staff Code of Conduct policy.
- If a member of staff is thought to have illegal content saved or stored on a personal mobile
  phone 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 staff Code of Conduct.

#### 6. Children's use of mobile and smart technology

- 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 eg our RSE, Computing Schemes of Work and Project
  Evolve.
- Personal mobile or smart technology devices are not permitted on site for children.



- Ochildren are not permitted to use personal mobile or smart devices whilst on the school site. Where these are requires, eg for safety reasons when children walk themselves to and from school, devices should be turned off/placed on silent and handed into the school office in the morning. They can then be collected at the end of the day.
- If a child needs to contact their parents or carers whilst on site, they will be allowed to use the school office phone under staff supervision.
  - Parents are advised to contact their child via the Castle Hill CP School office.
- If a child 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 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 Castle Hill CP School.
  - Any specific agreements and expectations (including sanctions for misuse) will be provided in writing and agreed by the learner and their parents/carers before use is permitted.
- Where children's personal mobile or smart technology devices are used when learning at home, this will be in accordance with our Acceptable Use Policies.
- Personal mobile or smart technology 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 a test or 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's 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 for Learning.
- 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 for Learning policy.
- Personal mobile or smart technology devices that have been confiscated will be held in a secure place and released to parents/carers at an agreed time.
- 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'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 Behaviour for Learning 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 for Learning 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 for Learning policy 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.
- 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:
  - o mobile phones and personal devices are not used in areas where there are children. There will be exceptional circumstances, where agencies eg STLS, Speech & Language will use work provided mobile phones and/or smart devices in line with their own policies and with prior agreement from the Headteacher of Castle Hill CP School.
- Appropriate signage and information is in place 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 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 Castle Hill CP 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 / Headteacher of any breaches of our policy.



#### 8. Policy monitoring and review

- Technology evolves and changes rapidly. Castle Hill CP 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 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 Castle Hill CP School will monitor policy compliance: for example, AUPs, observations.

#### 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 Castle Hill CP School policies and procedures. This includes our Child Protection, Behaviour for Learning and Code of Conduct.
- Where children 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/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/Headteacher (or a
  deputy) will seek advice from Kent County Council's Education Safeguarding Service or
  other agency in accordance with our Child Protection policy.

S. Stockley (Assistant Head for Access and Inclusion) September 2023

