MOBILE AND SMART TECHNOLOGY POLICY

Autumn 2023

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 procedure

Updates on the previous policy are as follows:

- New wording that incorporates “personal mobile devices and other forms of smart technology”.
- Staff personal mobile devices and/or smart technology are not to be connected to the school/Trust wifi system.
- Staff providing formal remote learning will do so using school provided equipment in accordance with our Acceptable Use Policy (AUP). If this is not possible, a discussion needs to take place with the Headteacher.
- 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 Trust policies and procedures, including confidentiality, child protection & safeguarding, data security, staff code of conduct and Acceptable Use Policy.
- Keep personal mobile phones and devices safe and secure in a cupboard during lesson time.
- Safe and appropriate use of mobile phones 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, for example, PSHE and Computing.
- If a child needs to contact their parents or carers whilst on site, they will be allowed to use a school phone. Parents are advised to contact their child via the school office; exceptions may be permitted on a case-by-case basis, as approved by the Headteacher.
- If a child requires access to personal mobile phone 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 the school/setting.
    - Any specific agreements and expectations (including sanctions for misuse) will be provided in writing and agreed by the child and their parents/carers before use is permitted.
- We monitor internet and technology use taking place via all school and Trust 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 safeguarding 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 Trust are made aware that the Trust will monitor policy compliance, as set out in our online safety policy and AUP.

Important Contacts

Designated Safeguarding Lead:

- Kelly Brown (Trust)
- Helen Thompson (St Martins)
- Casey Hall (Priory Fields)
- Lisa Sprigmore (Vale View)

Named Safeguarding Trustee:

- Tricia Sherling

Policy aims and scope

- This policy has been written by the Whinless Down Academy Trust, taking into account the DfE statutory guidance 'Keeping Children Safe in Education', Early Years and Foundation Stage, 'Working Together to Safeguard Children', 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 the Whinless Down Academy Trust community when using mobile devices and smart technology.
    - Whinless Down Academy 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 & Safeguarding Policy, the Designated Safeguarding Lead (DSL), the Headteacher, is recognised as having overall responsibility for online safety, and the Executive Lead/CEO has the responsibility of overseeing this.
- 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 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 all governance, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the Trust (collectively referred to as "staff" in this policy).

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 Policy (AUP)
- Behaviour policy
- Image use policy
- Child protection and safeguarding policy
- Staff code of conduct
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE) etc
- GDPR
- Online Safety
- Social media

Safe use of mobile and smart technology expectations

Whinless Down Academy Trust 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 Whinless Down Academy Trust 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 personal phones or devices.

- Staff mobile devices and other forms of smart technology are not permitted to be used on site, except for in staff only designated areas e.g. staffroom, personal offices etc.
- 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 the Whinless Down Academy Trust 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 behaviour or child protection policies.
- Staff personal mobile devices and/or smart technology are not to be connected to the school/Trust wifi system.

School provided mobile phones and devices

- Some members of staff may be issued with a work phone in addition to their work email address, where contact with parents/carers is required.
- Staff providing formal remote learning will do so using school provided equipment in accordance with our Acceptable Use Policy (AUP). If this is not possible, a discussion needs to take place with the Headteacher.
- School mobile phones and devices will be suitably protected via a passcode or pin 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 and acceptable use policy and other relevant policies.
- Where staff 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.

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 Trust policies and procedures, including confidentiality, child protection & safeguarding, data security, staff code of conduct and Acceptable Use Policy.
- Staff will be advised to:
    - Keep personal mobile phones and devices safe and secure in a cupboard during lesson time.
    - Keep personal mobile phones and smart devices switched off or set to 'silent' mode during lesson times.
    - Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
    - No use personal mobile phones and smart 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 smart devices is compatible with their professional role and our behaviour expectations.
- Members of staff are not permitted to use their own personal mobile phones or smart 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 Headteacher.
- Staff will only use school provided equipment (not personal devices):
    - 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. Staff will follow clear guidance outlined in the Acceptable Use Policy.
- If a member of staff breaches our policy, action will be taken in line with our staff code of conduct and allegations policy.
- If a member of staff is thought to have illegal content saved or stored on a personal mobile phone or smart 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.

Children 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 phones 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, for example, PSHE and Computing.
- Personal mobile phones and/or smart devices will not be used on site by children. If they bring them to school they need to be handed into a designated adult, following the individual school expectation.
- If a child needs to contact their parents or carers whilst on site, they will be allowed to use a school phone. Parents are advised to contact their child via the school office; exceptions may be permitted on a case-by-case basis, as approved by the Headteacher.
- If a child requires access to personal mobile phone 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 the school/setting.
    - Any specific agreements and expectations (including sanctions for misuse) will be provided in writing and agreed by the child and their parents/carers before use is permitted.
- Where children's mobile phones or personal devices are used when learning at home, this will be in accordance with our Acceptable Use Policy.

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 personal mobile phones or smart devices 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 personal mobile phone or smart device if they believe it is being used to contravene our child protection or behaviour policy. Personal mobile phones and smart 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 Designated Safeguarding Lead urgently as they will be most appropriate person to respond.
- If there is suspicion that data or files on a child's personal smart 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 personal mobile phones or smart devices 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 and safeguarding 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 decide if any searching incidents may need to happen, where staff have reasonable grounds to suspect a pupil was in possession of prohibited items, as identified in our behaviour policy.
- The Headteacher/DSL will be involved without delay if staff believe a search of a pupil's mobile phone or smart device has revealed a safeguarding risk.

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 not permitted and are only permitted within adult only areas of the school e.g. staffroom.
- Appropriate signage and information are in place to inform visitors of our expectations for safe and appropriate use of personal mobile phones and smart devices.
- 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 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.

Policy monitoring and review

- Technology evolves and changes rapidly. The Whinless Down Academy Trust 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 and Trust 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 safeguarding 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 Trust are made aware that the Trust will monitor policy compliance, as set out in our online safety policy and AUP.

Responding to policy breaches

- All members of the Trust 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.
- If we are unsure how to proceed with an incident or concern, the Headteacher will seek advice from Kent County Councils Education Safeguarding Service or other agency in accordance with our child protection and safeguarding policy.