The Dunstan Catholic Educational Trust

Mobile Smart Technology Policy

Agreed by the DCET Executive on: 30th August 2024

Review Date: August 2025

Signed: Helen Taylor

Version Number	Date Amended	Comments and Changes	Date Approved	Author	Approved By
1	30.08.24		30.8.24	Own	Executive Team

This policy applies to all academies within the DCET

Contents

1 - Policy aims and scope 3
2 - Links with other policies 3
3 - Safe use of mobile and smart technology expectations 4
4 - School provided mobile phones and devices 4
5 - Staff use of mobile and smart technology 5
5.1 Staff Smart watches 6
6.1 Pupil use of smartwatches 7
7 - Visitors' use of mobile and smart technology 7
8 - Policy monitoring and review 8
9 - Responding to policy breaches 8

1 - Policy aims and scope

- This policy has been written by The Dunstan Catholic Educational Trust and is an extension of the Online Safety Policy.
- The purpose of this policy is to safeguard and promote the welfare of all members of the school setting when using mobile devices and smart technology.
    - The Trust recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm when using mobile and smart technology.
    - Please see the school's website for the name of the Designated Safeguarding Lead (DSL) who has overall responsibility for online safety.
- This policy applies to all who have access to and use 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 or images.
- This policy applies to pupils, parents/carers and all staff, including the governing body, leadership team, teachers, support staff, Trust Central Team, Directors, 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
    - IT Acceptable Use Policies (AUP)
    - Behaviour and discipline policy
    - Safeguarding Policy
    - Code of conduct
    - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
    - Data Protection Policy
    - Online Safety Policy

3 - Safe use of mobile and smart technology expectations

The Dunstan Catholic Educational Trust recognises that use of mobile and smart technologies is part of everyday life for many learners, staff, and parents/carers.

- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of The Dunstan Catholic Educational Trust 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 strong passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on their phones or devices. A strong password is at least 8 characters and include numbers, upper case and a special character.

- Mobile phones and personal devices are not permitted to be used throughout the school day unless this is on their own break/lunch time or have permission from the headteacher.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community, any breaches will be dealt with in line with our anti-bullying, behaviour, safeguarding and disciplinary policies
- All members of The Dunstan Catholic Educational Trust 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 - School provided mobile phones and devices.

- Members of staff will be issued with a mobile phone and/or mobile device in addition to their work email address, where it is a necessary requirement for them to do their job. Mobile phones will be provided by the organisation and therefore choice of phone/contract is at their discretion.
- School provided mobile phones and devices must be suitably protected via a strong password/PIN and must only be accessed by the individual it is given to. A strong password is defined as one that is at least 8 characters long, includes numbers and upper/lower case, as well as a special character.
- School provided mobile phones and devices will always be used in accordance with the IT acceptable use policy and other relevant policies.
- Staff with school provided mobile phones and devices 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.

- Work mobile phones may at times be needed to be used in the presence of pupils in order for the employee to do their job.

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 trust policy and procedures, such as confidentiality, Safeguarding, data security, code of conduct and IT Acceptable Use Policies.

- Staff will be advised to:

    - Keep personal mobile phones and personal devices in a safe and secure place (e.g. locker/draw) during lesson time.
    - Keep personal mobile phones and 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.
    - Not use personal devices during teaching periods unless written permission has been given by the headteacher, such as in emergency circumstances.

- Personal mobile phones must not be used to contact pupils or parents. During school outings, nominated staff will have access to a school mobile phone which can be used for emergency or contact purposes.
- Personal mobile or smart devices are not allowed to join the main school WiFi unless permission has been given by the Headteacher.

- Staff will only use trust provided equipment to:

    - to take photos or videos of learners in line with our image use policy.
    - to work directly with learners during lessons/educational activities.
    - to communicate with parents/carers.

- Where remote learning activities take place, staff will use trust provided equipment. If this is not available, staff will only use personal devices with prior approval from the headteacher.
- If a member of staff breaches our policy, action will be taken in line with our staff disciplinary procedure.
- 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 staff disciplinary procedure.

5.1 Staff Smart watches

- Staff are allowed to use smartwatches, but they follow the same policy as mobile phones:

    - Staff are not to use their watch to send messages, photos, make phone calls or transfer any other kind of data whilst working with children. Any communications using their smartwatch must be during their own lunch/break time and away from children.
    - Staff are not permitted to take or store images of pupils on their smartwatch.
    - Personal information about staff, pupils or the school is not to be taken on a smartwatch.
    - Smartwatches are not allowed to join the school WiFi
    - Notifications must be turned off whilst using your smartwatch at school.

6 - Pupil's 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.
- Mobile phones and/or personal devices *will* not be used on site by learners. Pupils in KS2 may bring in a mobile phone into school.

    - Mobile phones or personal devices will not be allowed to be kept in the classroom; all devices must be handed into the office at the start of the day. They must also be turned off.
    - Pupils will not be allowed to use their mobile phone or personal devices during the school day, this includes before and after-school whilst on school site.
    - Mobile phones and personal devices can only be used in the school day if agreed with the headteacher.

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

    - Parents are only allowed to contact their child via the school office phone/email. Any exception must be agreed by the headteacher first.

- 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, and a risk assessment put in place.

- Any arrangements regarding access to personal devices in exceptional circumstances will be documented and recorded by the school.
- Any exceptional circumstances agreements (including sanctions for misuse) will be provided in writing and agreed by the pupil and their parents/carers before use is permitted.
- Mobile phones and devices that have been confiscated will be held in a secure place and released to parents/carers at the end of the day, unless subject to a police enquiry.
- Concerns regarding policy breaches by learners will be shared with parents/carers as appropriate.
- Where there is a concern that a child is at risk of harm, we will Children's Social Care in line with our Safeguarding Policy.
- If there is suspicion that material on a pupil'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.

5.2 Pupil use of smartwatches

- Smartwatches will be allowed in school under the following directive:

    - Smartwatches with cellular data are not permitted.
    - Smartwatches with cameras are not permitted.
    - Mobile phones linked to smartwatches must be turned off.
    - Smartwatches follow the same policy as mobile phones and are not to be used during the school day, including before/after school whilst on site.

7 - Visitors' use of mobile and smart technology

- Parents/carers and visitors, including volunteers and contractors, are expected to ensure that:

    - Mobile phones are not to be used in the classroom or when around any children. Use of mobile phones should only be during break/lunch time and in private areas (i.e. staffroom or meeting rooms).
    - Personal devices will not be allowed to join the main WiFi unless permission is given by the Headteacher.
    - Personal devices are not allowed to take or store images of pupils for any purpose.
    - Keep personal mobile phones and 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.

- Appropriate signage and information are in place at the school entrance to inform visitors of our expectations for safe and appropriate use of personal devices and mobile phones.
- Visitors, including volunteers and contractors are expected to use mobile and smart technology in accordance with our acceptable use of technology policy and other associated policies, including child protection. Our IT Acceptable Use Policy has been put on our sign-in systems and all visitors accept this when signing in.
- 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. The Dunstan Catholic Educational 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 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.

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.
- 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.