THEDWASTRE
Education Trust

Policy Name: USE OF PERSONAL DEVICES POLICY

Author: SBM/SR

Date ratified by the Trust Board: May 2018

Date for review: May 2020

Publish on Trust website: No

Publish on Academy websites: No

Issue to all staff and visitors: Yes

Signed:

Contents

Bring Your Own Device Policy

Part 1 Introduction

Thedwastre Education Trust recognises the benefits of mobile technology and is committed to supporting staff in the acceptable use of mobile devices.

This policy describes how non-school owned electronic devices, e.g. laptops, smart phones and tablets, may be used by staff members and visitors to the school. This practice is commonly known as 'bring your own device' or BYOD, and these devices are referred to as 'personal devices' in this policy. If you are unsure whether your device is covered by this policy, please check with the Data Protection Officer (via SBM Services).

Part 2 Organisational Arrangements

Overall Responsibility

The governing board of Thedwastre Education Trust is responsible for the approval of this policy and for reviewing its effectiveness. Monitoring at individual academy level is the responsibility of each local governing body.

Roles & Responsibilities

Staff members will:

- Familiarise themselves with their device and its security features so that they can ensure the safety of academy information.
- Install relevant security features and maintain the device appropriately.
- Set up passwords, passcodes, passkeys or biometric equivalents on the device being used.
- Set up remote wipe facilities if available, and implement a remote wipe if they lose the device.
- Encrypt documents or devices as necessary.
- **Report the loss of any device containing school information, or any security breach immediately to the Data Protection Officer**.
- Ensure that no academy information is left on any personal device indefinitely. Particular care must be taken if a device is disposed of / sold / transferred to a third party.
- Not share information from personal devices via social media and will not keep academy information indefinitely.

Visitors will:

- Familiarise themselves with the use of personal devices at the academy.
- Only use personal devices for agreed purposes at the academy and with parental or the relevant permission.
- Not share information from personal devices via social media and will not keep academy information indefinitely.

Part 3 Detailed Arrangements & Procedures

Use of personal devices at the school

Staff and visitors to the academy may use their own devices in the following locations:

- In the classroom with the permission of the teacher
- In the school environments eg hall, meeting room, with the permission of the headteacher.

Personal devices must be switched off when in a prohibited area, and / or at a prohibited time, and must not be taken into controlled assessments and / or examinations unless special circumstances apply.

The school reserves the right to refuse staff and visitors permission to use their own device on school premises.

Use of cameras and audio recording equipment

Parents and carers may take photographs, videos or audio recordings of their children at school events for their own personal use.

Other visitors and staff may use their own personal devices to take photographs, video, or audio recordings in school provided they have checked that parental permission has been received by the academy. This includes people who may be identifiable in the background.

Photographs, video or audio recordings made by staff on their own devices must be deleted as soon as reasonably possible after they have been used, e.g. uploaded for use on one of the school's social media sites. Photographs, video or audio recordings to be retained for further legitimate use, should be stored securely on the school network.

Photographs, video or audio recordings should not be published on blogs, social networking sites or in any other way without the permission of the people identifiable in them.

Devices must not be used to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely to take photographs, video or audio recordings in school.

Access to academy internet connections

Wireless networks for staff and visitors are not available at the time of writing this policy.

Should access be agreed in the future, the following points must be followed:

- Access to the wireless network is at the discretion of the academy, and the academy may withdraw access for anyone it considers is using the network inappropriately.
- The academy cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk.
- The academy is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the school's network.
- The academy will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's network.

Access to the school's systems

Staff are permitted to connect to or access the following academy services from their device:

- The academy email system.
- The academy management information system/assessment tracking system

Staff may use the systems to view school information via their personal devices, including information about pupils. Staff must not store the information on their devices, or on cloud servers linked to their device. In some cases, it may be necessary for staff to download school information to their personal devices in order to view it (e.g. an email attachment). Staff shall delete this information from their device as soon as they have finished viewing it.

Staff must only use the IT systems and any information accessed through them for work purposes. Academy information accessed through these services is confidential, in particular information about pupils. Staff must take all reasonable measures to prevent unauthorised access to it. **Any unauthorised access to, or distribution of, confidential information must be reported to the academy as soon as possible, and to the DPO if a breach has occurred.**

Staff must not send school information to their personal email accounts.

Monitoring the use of personal devices

Academies may use technology that detects and monitors the use of personal and other electronic or communication devices which are connected to or logged on to the academy's wireless network or IT systems. By using a device on the academy's network, staff and visitors agree to such detection and monitoring. The academy's use of such technology is for the purpose of ensuring the security of its IT systems and tracking school information.

The information that the school may monitor includes, (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms, information uploaded or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Staff who receive any inappropriate content through academy IT services or the academy internet connection must report this to the school as soon as possible.

Security of staff personal devices

Any member of staff wishing to use their own device must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption. This should be more than a simple password protection.

Staff must ensure that personal devices are set to lock with encrypted passcodes to prevent unauthorised access. The device should be locked if they are unattended or set to auto-lock if it is inactive for a period of time.

Staff must never attempt to bypass any security controls in academy systems or others' own devices.

Staff must ensure that appropriate security software is installed on their personal devices and must keep the software and security settings up-to-date.

Staff must ensure that passwords are kept securely and are not accessible to third parties. Automated log on processes to store passwords must not be used.

Support

The trust takes no responsibility for supporting staff's own devices, nor does an academy have a responsibility for conducting annual PAT testing of personal devices. However, the academy will support staff in ensuring that they have appropriate levels of security in place.

Compliance, sanctions and disciplinary matters for staff

Non-compliance of this policy exposes both staff and the school to risks. If a breach of this policy occurs, the Staff Disciplinary & Misconduct policy will be applied.

Incidents and reporting

Each academy, on behalf of the trust, takes any security incident involving a staff member's or visitor's personal device very seriously and will always investigate a reported incident. This will be reported to the trust board without delay. Loss or theft of the device should be reported to the academy office in the first instance. Data protection incidents should be reported immediately to the trust's Data Protection Officer.