



Trust Issued Portable Electronic Device Policy

This policy has been approved by Directors and the Operations Board

A handwritten signature in black ink, appearing to read "Alley".

Date Policy was created: **January 2021**

Date of next renewal: **January 2022**

1. Scope

- This policy applies to all employees who have been issued with a portable electronic device, such as a laptop, iPad, tablet or phone, for work purposes. All devices are owned by Skills for Life Trust and the user must agree to this policy or return the device to the IT Network Team.
- The policy describes the safe and acceptable usage of portable electronic devices supplied to Trust employees.
- The policy only relates to Trust owned portable electronic devices and does not cover the use of privately owned portable electronic devices to connect to the School's ICT facilities.
- The primary contact for all queries and requests related to Trust portable electronic devices is the Trust IT Network Manager or either the Primary or Secondary IT Network Manager.

2. Personal use of Trust portable electronic devices

Users are permitted to use Trust portable electronic devices for personal use providing they adhere to the following:

- Any personal calls or messages that are not covered by the tariff may incur a charge.
- Personal use of data services is only permitted when the device is connected to Wi-Fi, not when using cellular data.
- The purpose of use is not for financial or any other form of commercial gain to the user or other organisation.
- Trust purchased devices are Trust property. They are not a user's personal property, nor are they available for individual resale or remuneration.

3. Responsibilities

The responsibility for the appropriate use of portable electronic devices rests with the designated user, who must:

- Take reasonable precautions to avoid loss, misuse of, or damage to the device. Intentional or repeated loss, misuse or damage **may** result in disciplinary action and the recovery of any costs incurred by the Trust.
- Return the portable electronic device to either the Primary or Secondary IT lead when employment with the Trust ends.
- Return the device to a member of the IT Network Team if it is in need of repair. It should be noted that manufacturer's warranty does not normally cover damage caused by misuse or neglect and that the cost of such repairs **may** be borne by the user.

4. Security

- All Trust portable electronic devices will be uniquely identified and registered in the IT asset register.
- All Trust devices must have an appropriate passcode and/or fingerprint lock enabled.
- All Trust devices that require an Apple ID are set up by the IT Network Team in order to activate the appropriate security features. The password for the Apple ID will be set by the IT Network Team and must not be changed.
- Users are not permitted to add personal Apple IDs or email accounts to Trust devices.

- All Trust devices may be recalled and checked by the IT Network Team with no prior warning/notice.
- Each Trust device may only be used by the designated user. It is the user's responsibility to ensure that any passcodes or passwords associated with the device are known only to them and not divulged to any unauthorised person.
- In the event that a passcode or password is forgotten, users must contact a member of the IT Network Team for assistance. On some devices, after 10 wrong attempts the data will be erased.
- Users are responsible for the physical security of the portable electronic device issued to them and must not leave it unattended or in an insecure location. All devices should be secured, when unattended, with a minimum of 2 barriers, i.e. building controls and locked office or locked drawers/cabinet.
- Users should not connect to unsecured Wi-Fi networks.
- All Skills for Life Trust purchased and issued portable electronic devices must be returned upon termination of employment. If they are not returned, after a reminder process, the trust may take further action for recovery, including civil litigation.
- The IT Network Team will securely erase data on all returned devices and reformat the device before being reissued to another user. The device will also be securely erased when disposed of at the end of its lifecycle.
- The loss of devices that can send, store and retrieve e-mail or access Skills for Life Trust information systems has potentially serious repercussions for the Trust because of the sensitivity of the information that may be stored on them. Sensitive, confidential or otherwise valuable information should therefore not be permanently stored on Trust devices.
- All losses of portable electronic devices must be reported to the IT Network Team as soon as possible within working hours. The IT Network Team will remotely wipe the device and if appropriate, arrange for a replacement unit to be delivered. **If the device is lost, the cost of the replacement unit may be covered by the user.**

5. Permitted Use of Mobile Communications Devices

- Trust issued mobile phones are the property of Skills for Life Trust and should normally be used for legitimate business purposes only. However, it may be necessary from time to time to make a personal call or send a personal text message. Users will be required to identify such personal use where it is not covered by the standard tariff, at which point a charge may be incurred.
- Devices capable of transmitting and receiving data information should only be used for the purposes for which they were supplied.
- Users **must not** use, try to use, or let anyone else use staff portable electronic phones for:
 - Anything that is illegal or immoral;
 - Making offensive, threatening or harassing calls;
 - Taking photographs of students, **unless meeting the requirements set out in section 6;**
 - Use of the Short Message System (SMS), multimedia messaging or e-mail to send or receive inappropriate or offensive remarks, graphics or images;
 - Use in contravention of Regulation 104 of the Road Vehicles (Construction & Use) Regulations 1986, i.e. using a portable electronic phone whilst driving.

- The sending or receiving of SMS text messages for the purposes of downloading, or accessing, ring tones, games, commercial competitions, sports report services and other non-business related activities or applications **is not permitted**. It should be noted that many of these services operate on an on-going subscription basis, and can be charged at anything up to £5 per item. **Any unauthorised cost will be charged to the user.**
- Free apps may be downloaded if appropriate and for educational/work purposes. If you require an app that needs to be purchased, please follow the Trust order procedures.
- Where the user cannot justify call usage and costs on a repeated basis, it is at the discretion of the line manager to initiate disciplinary action in line with the Staff Disciplinary Policy.
- Voicemail is automatically provided on all phones. Voicemail greetings should be personalised with a suitable message inviting the caller to leave a message. A voicemail PIN will be set up by the IT Network Team.
- Trust phones are configured to standard builds, either for an individual user or to be used as a 'pool phone'.
 - Individual user: apple ID, iCloud backup, find my iPhone, appropriate academy Wi-Fi connections, work email accounts and work calendar will be set up by the IT Network Team.
 - 'Pool phone': apple ID, iCloud backup, find my iPhone and appropriate academy Wi-Fi connections will be set up by the IT Network Team. Email accounts or calendars are not to be added to these phones.
- All Trust phones are configured to a standard tariff band before delivery to the user.
- If a user requires international calls and coverage, this must first be agreed by their line manager. If users are in any doubt as to coverage in the country they intend to visit, please contact a member of the IT Network Team for further details. While there may be a cost for allowing international access, depending on location, it should be noted that it can be expensive both to make **and receive** calls and use cellular data whilst abroad; secured Wi-Fi should be used where possible.
- Users of mobile data must contact the Trust IT Network Manager before travelling abroad, in order to arrange for an appropriate roaming data bundle to be added.

6. Social Media and Photographs

- Users are permitted to take photographs of students using Trust issued electronic devices, however, this can only be for the purposes of learning, or when promoting the Trust or one of the Trust schools.
- The following rules must be adhered to when taking photographs of students for this purpose:
 - Any students included in a photograph must have appropriate consent
 - Photographs must be deleted from the device as soon as they have been uploaded to a learning journal, social media account or website