MOBILE PHONE AND BRING YOUR OWN DEVICE (BYOD) POLICY

THIS POLICY APPLIES TO THE HOPE TRUST BOARD, ALL TRUST SCHOOLS AND THE HOPE TEACHER TRAINING PARTNERSHIP

Document Management:

Date Approved: July 2019
Next Review Date: July 2021
Version: 1.4
Approving Body: Resources Committee

Contents

Statement of Intent

Hope Learning Trust York (HLTY) appreciates that at times staff, supply teachers, volunteers, governors, Trustees or other legitimate visitors to the school may have reason to bring and use a personal device (Bring Your Own Device – BYOD) at the Trust offices/school/academy.

HLTY embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, HLTY aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

In addition, HLTY has a legal obligation to protect personal data under the General Data Protection Regulations (GDPR).

The purpose of this policy is to ensure so far as possible that personally-owned devices used by members of staff, governors, Trustees, supply teachers, visitors and volunteers (hereafter collectively referred to as "users") are used in a manner which protects personal confidentiality, personal data and the confidentiality and security of communications. This policy supplements the **E-Safety and Acceptable Use Policy – Staff and Visitors**.

Definitions

Personal device relates to any mobile phone, smartphone, tablet or laptop and other 'smart' devices that enable access to mobile platform/internet and are owned by an individual and not by the Trust/Academy.

BYOD (bring your own device) is the increasing trend toward employee-owned devices within a business. Smartphones are the most common example, but employees also take their own tablets, and laptops into the workplace.

Portable Storage Devices are small, mobile hard drives designed to hold digital data, typically called USB hard drives, 'flash drives', etc.

The Trust are working towards eliminating the use of portable storage devices (i.e USB hard drives and USB flash drives) in our Trust/academies. **Cloud based facilities should be used as an alternative whenever possible.**

If portable storage devices are used, these must be purchased by the school and registered with the IT Network Manager, and they must be encrypted.

Signed by:

_____	Chief Executive Officer	Date: _____
_____	Chair of Resources Committee	Date: _____

1. Legal Framework

This policy has due regard to legislation, including but not limited to:

- The General Data Protection Regulations (GDPR)
- The Safer Recruitment Consortium's guidance 2015
- Bring Your Own Device Guidelines ICO

This policy will be implemented in conjunction with the following other Trust/Academy documents:

- HLTY Data Protection Policy 2018
- HLTY E-Security Policy
- HLTY E-Safety and Acceptable Use Policy – Staff and Visitors
- HLTY Social Media Policy
- HLTY Photography and Videos at School Policy
- HLTY GDPR Privacy Notice – Pupils

2. Principles

Bring Your Own Device (BYOD) raises a number of data protection concerns due to the fact that the device is owned by the user rather than the data controller. It is crucial that the data controller ensures that all processing for personal data which is under his control remains in compliance with GDPR. Protecting data in the event of loss or theft of the device will need to be considered.

3. Scope

This policy applies to all users. The purpose of this policy is to establish the criteria of using personal owned PCs, laptops, smartphones, tablets and/or any other mobile devices with which the owner has established access to the school's network.

4. User Responsibility

Users agree to a general code of conduct that recognises the need to protect confidential data that is stored on, or accessed using, a mobile device. This code of conduct includes but is not limited to:

4.1. Registration

Any personal device used for work purposes must be registered with the relevant establishment. A secure list will be held by either the IT Network Manager or in the absence of this post, the Office Manager.

4.2. Security

The user is responsible for securing their device to prevent sensitive data from being lost or compromised and to prevent viruses from being spread. Removal of security controls is prohibited.

The device must only be used to access cloud/server-based information/data. It must not be used to download or store school data.

4.3. Passwords

- Change default passwords (e.g. '1234', 'admin') and secure approved devices by a password or a biometric access control (e.g. fingerprint scanner or facial recognition). Passwords should be sufficiently memorable that the user can avoid writing them down, but not obvious or easily guessed. Long passwords are best, as a short password can be cracked more easily by hacking software. A combination of alphanumeric characters is required.

- The same password must not be used for all devices, services and websites. Passwords must be changed if a password is disclosed to another person or discovered, and in any event every six months.
- Approved devices must be configured so that they are automatically locked after being left idle for a set time of no more than 5 minutes in the case of mobile devices and 10 minutes in the case of desktop computers.
- Passwords to approved devices must be kept confidential and must not be shared with family members or third parties.
- Passwords must not be 'remembered' by the system. This exposes the data to a high security risk.
- Approved devices must not be used by family members or other persons unless either the device has been configured for separate logins to ensure restricted access to files, or the user reserves the device for work using only school/academy remote access.

4.4. Confidentiality

- Care must be taken to avoid using approved devices in a manner which could pose a risk to confidentiality, whether by clicking on links in suspicious emails, accessing potentially harmful websites, using potentially harmful application software, using wi-fi facilities in public places (e.g. coffee shops or airports), or otherwise. Some apps for smartphones and tablets may be capable of accessing sensitive information.
- User is forbidden from copying sensitive data from email, calendar and contact applications to other applications on the device or to an unregistered personally owned device
- Preventing the storage of sensitive personal data in unapproved applications on the device.
- Ensuring the device's security controls are not subverted via hacks, 'jailbreaks', security software changes and/or security setting changes

4.5. Maintenance

The personal smartphone and tablet devices are not centrally managed by HLTY. For this reason, a support need or issue related to a personally owned device is the responsibility of the device owner. Specifically, the user is responsible for:

- Maintaining the software configuration of the device – both the operating system and the applications installed.
- Settling any service or billing disputes with the carrier
- Purchasing any required software not provided by the manufacturer or wireless carrier
- Device registration with the vendor and/or service provider
- Maintaining any necessary warranty information
- Battery replacement due to failure or loss of ability to hold a charge
- Backing up all data, settings, media, and applications
- Installation of software updates/patches

4.6. Report of loss

In the event that an approved device is (or is suspected of being) lost or stolen or compromised, the school/academy **E-Safety Officer** and **HLTY Data Protection Officer** must be informed as soon as possible so that such steps as may be appropriate may be taken to delete from the device the work email account and other data belonging to the Trust/school/academy, and to report the loss of the device.

4.7. Termination of employment/contract

Users must sign a declaration on termination of employment or severance of their contract with the Trust, to confirm that they have deleted all Trust-related links, information and downloads relating to Hope Learning Trust York from all and any device used. This will form part of the exit process. This evidence is essential to comply with the policy.

The register will then be updated to reflect the action and close relevant permissions.

5. Trust/School/Academy Responsibility

The Trust/school/academy will maintain a register of approved devices setting out:

a) The name of the user
b) the type and model of each device
c) the date on which the device was registered
d) the signature the user of that device.

By registering and signing the document, employees agree to adhere to the rules set out in this policy.

6. Enforcement

Any user found to have violated this policy may be subject to disciplinary action, including but not limited to:

- Account suspension
- Revocation of device access to the school network
- Data removal from the device
- Employee Termination