MOBILE PHONE AND BRING YOUR OWN DEVICE (BYOD) POLICY

THIS POLICY APPLIES TO THE HOPE SENTAMU LEARNING TRUST BOARD,
LOCAL GOVERNING COMMITTEE (LGC) MEMBERS, THE CENTRAL TEAM,
ALL TRUST SCHOOLS/ACADEMIES AND THE WORKFORCE DEVELOPMENT TEAM

Document Management:

Date Policy Approved: July 2019

Date Amended: April 2022

Date amended version approved: 25th April 2022

Next Review: April 2024

Version: 1.5

Approving Body: Resources Committee

Contents

	Policy updates	3
	Statement of Intent	4
1.	Legal Framework	5
2.	Principles	5
3.	Scope	5
4.	User Responsibility	6
5.	Trust/School/Academy Responsibility	8
6.	Enforcement	8
7.	Remote Learning	8
8.	Review and monitoring	8
Appendix A	Bring Your Own Device Form	10

Policy updates

Date	Page	Policy updates
April 2022	Whole document	Reference to the Trust's Data Protection Policy, updated to read Data Protection (UK GDPR) Policy and reference to GDPR, updated to read UK GDPR
April 2022	p4, Statement of Intent	Further detail added relating to best practice and the steps taken to reduce the risk of data and confidentiality breaches. Some points clarified and updated
April 2022	p5, item 1.1 and 1.2	Legislation, guidance and policy listings have been updated
April 2022	p5, item 2.2 and 2.4	Guidance added from the Bring Your Own Device ICO Guidelines
April 2022	p5, item 2.3	Addition: What action will be taken if senior management has reason to believe that a user is misusing their device
April 2022	p6, item 4.1	Registration - users are directed to complete Appendix A
April 2022	p6, item 4.2	Guidance added from the Bring Your Own Device ICO Guideline. Additional items - two-factor authentication and the prohibited use of personal email accounts for work purposes
April 2022	p6, item 4.3	Addition details added to strengthen the password section, including guidance from the Bring Your Own Device ICO Guidelines
April 2022	p7, item 4.4	Addition details added to strengthen the confidentiality section, including guidance from the Bring Your Own Device ICO Guidelines
April 2022	p7, item 4.5	Section added: Data Breaches
April 2022	p8, item 7	Section added: Remote learning
April 2022	p9, item 8	Section added: Reviewing and monitoring
April 2022	p10, Appendix A	Bring Your Own Device Form added and updated

Signed by:

_____ Chief Executive Officer Date: _____

_____ Chair of Resources Committee Date: _____

Statement of Intent

Hope Sentamu Learning Trust (HSLT) appreciates that at times staff, supply teachers, volunteers, governors, Trustees (hereafter collectively referred to as "users") or other legitimate visitors to the school/academy may have reason to bring and use a personal device (Bring Your Own Device - BYOD) at the Trust offices/school/academy. Generally the most secure option is for the Trust to provide devices to users, but this is not always possible. Members, Trustees and Governors would, for instance, not be issued with a Trust device. However, wherever possible, the Trust will provide devices such as cameras and mobile phones to staff rather than expecting staff to use their own (e.g. on school trips, remote teaching, etc).

HSLT 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, HSLT 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, HSLT has a legal obligation to protect personal data under the UK General Data Protection Regulations (UK GDPR). This policy supplements the **E-Safety and Acceptable Use Policy - Staff and Authorised Users**.

The purpose of this policy is to ensure so far as possible that personally-owned devices used by 'users' are used in a manner which protects personal confidentiality, personal data and the confidentiality and security of communications. Trustees and Governors are all issued with a Trust email address, through which all governor business must be conducted. Meeting papers are managed and stored on a password protected online portal. These steps have been taken to reduce the risk of data and confidentiality breaches.

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. Given the ever-changing world of technology it should be noted that this list gives examples only and is not exhaustive.

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, laptops and other hand-held devices 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 schools/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/academy and registered with the IT Technician, and they must be encrypted.

1. Legal Framework

1.1. This policy has due regard to legislation and guidance, including but not limited to:

- The UK General Data Protection Regulations (UK GDPR)
- The Safer Recruitment Consortium's Guidance for safer working practice for those working with children and young people in education settings 2022
- Bring Your Own Device Guidelines ICO

1.2. This policy will be implemented in conjunction with the following other Trust documents:

- Data Protection (UK GDPR) Policy
- Data Breach Policy and Procedures
- E-Safety and Acceptable Use Policy - Staff and Authorised Visits
- Social Media Policy
- Photography and Videos at School Policy
- GDPR Privacy Notice - Pupils
- GDPR Privacy Notice - Staff
- GDPR Privacy Notice - Members/Trustees/Governors

2. Principles

2.1. 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 their control remains in compliance with UK GDPR. Protecting data in the event of loss or theft of the device will need to be considered.

2.2. Under no circumstances should staff be expected or allowed to use their personal equipment to take images of students at or on behalf of the school/academy. All settings should have arrangements in place with regard to the taking and the use of images, which is linked to the Trust's Child Protection and Safeguarding Policy and the Photography and Videos at School Policy.

2.3. If Senior Management has reason to believe that a user is misusing their device or has taken and/or is storing images or videos of students on their device the Trust reserves the right to search the device.

2.4. In the event of any indecent images of children or unsuitable material being discovered on a device the equipment should not be tampered with in any way. It should be secured and isolated from the network, and the Data Protection Officer / Chief Operating Officer contacted without delay. Adults should not attempt to investigate the matter or evaluate the material themselves as this may lead to a contamination of evidence and a possibility that they will be at risk of prosecution themselves.

3. Scope

3.1. 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 Trust'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 'Bring Your Own Device' form (**Appendix A**) **MUST** be completed and returned to the IT Technician or in the absence of this post, the Office Manager. A secure list will be held by the IT Technician/Office Manager.

4.2. **Security**

The Trust is aware that allowing users to use their own devices to access the Trust network carries with it some security risks. Out of date and unpatched operating systems or security software may be vulnerable to exploitation including loss or compromise of personal data. Inadequate access control, eg weak laptop passwords, may result in personal data being easy for unauthorised individuals to access.

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/academy data.

The Trust utilises two-factor authentication for access from devices that are not owned by the network. Staff will be prompted to use the two-factor authentication when logging into the Google Workspace.

Staff MUST NOT use their personal email account for work purposes.

4.3. **Passwords**

Users must comply with the following:

- 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. Staff should keep their passwords confidential and not allow unauthorised access to equipment.
- 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 (or when prompted to do so by the network).
- 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. The device owner's data and the Trust's data should be separate. Users should not be able to inadvertently or deliberately move the Trust's data into their personal storage on the device or onto separate personally-owned devices.
- 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.
- Users are forbidden from copying sensitive data from email, calendar and contact applications to other applications on the device or to an unregistered personally owned device, USB stick or external hard drive.
- 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. **Data Breaches**

Users, whether they are using their own device or a Trust-provided device are responsible for understanding what constitutes a Data Breach. All users need to familiarise themselves with the procedures relating to when and how to report potential data breaches.

4.6. **Maintenance**

Personal smartphones and tablet devices are not centrally managed by HSLT. 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

4.7. **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 **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 belonging to the Trust/school/academy, and to report the loss of the device.

4.8. **Termination of employment/contract**

Staff 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 Sentamu Learning Trust 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

5.1. The Trust/school/academy will maintain a register of approved devices setting out (**see Appendix A**):

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 of 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

7. Remote learning

7.1. When selecting a platform for online / virtual teaching, in the event of a pandemic or similar, the Trust will ensure that appropriate levels of security are maintained. For full detail see the Online Live Learning Support Addendum. Wherever possible, staff should use school/academy devices and contact students only via their school/academy email address / log in. This ensures that the Trust's filtering and monitoring software is enabled.

8. Review and monitoring

This policy is reviewed every two years by the Resources Committee. Any changes made to this policy by the

Trust will be communicated to all members of staff. All members of staff are required to familiarise themselves with all protocols outlined in this policy. The next scheduled review date for this policy is listed on the cover page of the policy.

Appendix A

Hope SENTAMU LEARNING TRUST

Bring Your Own Device			
Name		**Job Title**	
School / Area			
Type of Device		**Make**	
Model		**Serial Number**	
Number (where applicable)			
Users agree, by registering their personal device, to adhere to the regulations set out in the HSLT Mobile Phone and Bring Your Own Device Policy.			
Date Registered			
Signed			
This form to be returned and kept in the relevant staff members/users personnel file. The bottom section of this form is only to be completed when/if a member of staff/users wishes to remove their personal device from use.			
Date Removed from Register			
Signed			
Actioned By (Print)			
Actioned By (Signed)			