BYOD
(Bring Your Own Device) Policy

Introduction

The Forge Trust recognises the benefits that can be achieved by allowing staff to use their own devices when working, whether that is at home, on site or while travelling. This includes laptops, smart phones, tablets and any other connected device which connect to academy systems. The practice is commonly known as 'bring your own device' or BYOD. The trust is committed to supporting staff in this practice and ensuring as few technical restrictions as responsibly possible are imposed on accessing academy provided services on BYOD, whilst maintaining data security and GDPR compliance.

The use of such devices to create and process trust information and data create issues that need to be addressed, particularly in the area of information security.

The trust must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empowering staff to ensure that they protect their own personal information.

This policy covers users own device use as detailed below, for which permission must be sought prior to use/access, using appendix 1.

- Any device which connects to the academy Wi-Fi to access either the network or the Internet.
- Any device which is connected physically to a network point or switch within the academy, to access either the network or the Internet.
- Any device which is able to receive mail from the user's academy mailbox, other than webmail.
- Any device which shares files with the academy network through the use of a VPN or cloud-based storage applications (e.g. Dropbox), whether the account used was provided by the academy or not.

Information Security Policies

All relevant trust policies still apply to staff using BYOD. Staff should note, in particular, the trusts Acceptable Use Policy.

The Responsibilities of Staff Members

Individuals who make use of BYOD must take responsibility for their own device and how they use it. They must:

- Familiarise themselves with their device and its security features so that they can ensure the safety of the trusts information (as well as their own information).
- Invoke the relevant security features.
- Maintain the device themselves ensuring it is regularly patched and upgraded.
- Ensure that the device is not used for any purpose that would be at odds with aims and ethos of the academy and its policies.

STAFF SHOULD NOT USE JAILBROKEN DEVICES

Staff using BYOD must take all reasonable steps to:

- Prevent theft and loss of data.
- Keep information confidential where appropriate.
- Maintain the integrity of data and information, including that on site.
- Take responsibility for any software they download onto their device.
- Ensure that work done on a BYOD is transferred or copied onto the academies computer systems.

The academy understands that some users will require different levels of settings for their devices depending on what the resource is used for and what it is.

Mobile phones, smart phones and "tablet" devices

- Configure your device to enable you to remote-wipe it should it become lost (E.g. "Find my iPhone" app for Apple devices).
- If your device is second hand, restore to factory settings before using it for the first time.
- Only download applications ('apps') or other software from reputable sources.

IF YOU SELL YOUR DEVICE OR GIFT IT TO SOMEONE ELSE, IT SHOULD BE PUT BACK TO FACTORY SETTINGS

All type of devices

- Set and use a passcode (e.g. pin number or password) to access your device. Whenever possible, use a strong passcode. Do not share the passcode with anyone else. We recommend the use of biometric authorisation over passcodes where available.
- Set your device to lock automatically when the device is inactive for more than a few minutes.
- Take appropriate physical security measures. Do not leave your device unattended.
- Keep your software up to date.
- Make arrangements to back up your documents.
- Keep master copies of work documents on an academy server.
- If other members of your household use your device, ensure they cannot access academy information, for example, with an additional account passcode. (Our preference is for you to not share the device with others.)
- Regularly review the information on your device. Delete copies from your device when no longer needed.
- When you stop using your device (for example because you have replaced it) and when you leave the academy's employment, securely delete all academy information on your device.
- Ensure that no academy information is left on any personal device indefinitely and only kept while needed.
- Encrypt the device (to prevent access even if someone extracts the storage chips or disks and houses them in another device).
- Report any data breaches in accordance with GDPR policies.
- Configure your device to maximise its security. For example, each new technology brings new enhanced security features. Take time to study and discover how to use these and decide which of them are relevant to you. Seek help from the IT support team if necessary.
- Use anti-virus software and keep it up to date if required for your device.

Using wireless networks outside the academy

- Control your device's connections by disabling automatic connections to open, unsecured Wi-Fi networks and make risk conscious decisions before connecting.

Monitoring and Access

The trust will not routinely monitor personal devices. However, it does reserve the right to:

- Prevent access to a particular device from either the wired or the wireless networks or both.
- Prevent access to a particular system.
- Take all necessary and appropriate steps to retrieve information owned by the academy.

Data Protection, GDPR and BYOD

The trust must process 'personal data' i.e. data about identifiable living individuals in accordance with GDPR. Sensitive personal data is information that relates to race/ethnic origin, religious beliefs, health details or any information, which can identify an individual. This category of information should be handled with a higher degree of protection at all times.

The trust recognises that there are inherit risks in using BYOD to hold and process personal data. Therefore, staff must follow the guidance in this document when considering using BYOD to process personal data and permission to use a device for this purpose must be sought.

A breach of GDPR can lead to the academy being fined up to €20 million. Any member of staff found to have deliberately breached the directive may be subject to disciplinary measures, having access to academy systems withdrawn, or even criminal prosecution.

Responsibility and Damage

While trust IT staff will always endeavour to assist colleagues wherever possible, the trust cannot take responsibility for supporting devices it does not provide.

Staff, who use their personal devices for trust purposes do so at their own risk. Staff are expected to act responsibly with regards to their own device, keeping it up to date via regular anti-virus and operating system updates and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

The Forge Trust is in no way responsible for:

- Personal devices that are broken whilst at school or during school-sponsored activities.
- Personal devices that are lost or stolen at school or during school-sponsored activities in terms of replacement, but the academy would need to be informed immediately about any data held on the device.
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).
- Staff should ensure they have adequate insurance cover in place to cover the cost of repair/replacement of a personal device in the event of loss/damage to the device.

Obsolete or out of Date Devices

Please note staff/ trustees must not access trust/ academy data on an out of date device e.g. Android over 3 years old.

Smart Watches and Tablets

Staff/ Trustees are not permitted to access trust/ academy data on Smart Watches or shared tablets.

Blank for double sided copying

BYOD (Bring Your Own Device) Policy - Appendix 1

BYOD Request Form

Date: _____

Staff Member Name: _____

Job Title: _____

Please now provide details of the device you wish to use.

Manufacturer: _____

Device (e.g. iPad, Smart Phone, Laptop): _____

Please tick the appropriate boxes for this device.

☐ I wish to connect this device to the academy network either by wire or Wi-Fi to only access the Internet.

☐ I wish to use this device to use an application or program to access my academy email account.

☐ I wish to use this device for work purposes in line with my job, which will involve storing and processing information, some of which will be personal information about adults or children.

Please now read the statements below.

I have read and understand the BYOD policy.
I understand the settings needed to use my device and these settings are in place.
I understand that the device is used at my own risk.
I understand that any issues regarding a data protection breech on a BYOD must be reported to SMT immediately, no matter how small.

Signed: _____

Approved by CEO/ Finance Director: _____

If not approved, please see below.

_____
_____
_____