Bring Your Own Device Policy

Policy Type	Non statutory
Date	
To be reviewed	
On Website	**N/A**

This policy applies to anyone connecting to the Wi-Fi or using Elevate Multi Academy Trust (Elevate) accounts on their own device at or from one of Elevate's Academies or organisations.

To be signed by all Elevate employees to confirm they have read and understood this policy.

Introduction

This policy is intended to provide a clear framework for the secure use of personal devices for work purposes both in the workplace and at home.

Personal devices includes smart phones, smart watches, tablets, laptops and home computers that belong to the employee but which are used for work purposes as well as for private use. This is commonly known as 'bring your own device' or BYOD.

For the avoidance of doubt, this policy applies to accessing work files and email using Office 365 using a browser, as well as connecting to Elevate systems via a local network or through the VPN (virtual private network).

There needs to be a balance between the convenience BYOD offers and the security of Elavate's data and the integrity of its systems.

Under the **Data Protection Act 2018 (DPA),** Elevate must:

- remain in control of the corporate data for which it is responsible;
- process it lawfully;
- keep it for no longer than is necessary.

This obligation exists regardless of the ownership of the device used to carry out the data processing or storage.
For example, if a member of staff were to use their own device to access their Academy email account, Elevate needs to ensure that those emails (and any attachments, etc.) do not leave its control.

Elevate employees are:

- required to play a role in keeping Elevate data secure;
- required to assist Elevate in complying with Subject Access and other requests made under the Freedom of Information Act, which may include data stored on a personal device.

The use of home PCs to access Elevate network remotely should be limited to the remote access systems provided by the trust and Office 365 (email, One Drive & Sharepoint).
FILES SHOULD NOT BE SAVED ON PERSONAL DEVICES.

Any failure to comply with this policy will be managed in accordance with Elevate's Disciplinary Policy.

What are the Implications for Employees Who Want to Use their Own Device(s) Under this Policy?

Personal devices must use one of the following Operating Systems:

- iOS 10.2 or higher
- Android 7.1 or higher
- Windows 8.1 or higher
- OS X 10.12 or higher

Employees must:

- Inform Elevate that they have the appropriate policies and certificates on their devices to enable the protection and if necessary removal of data in the event of the device being lost/stolen/damaged beyond repair etc. Employees must accept that in the event of a remote wipe being necessary, they may also lose any personal data stored on the device;

- agree to keep their device up to date with the latest patches to its Operating System and other software (e.g. Office). Software companies regularly patch their products to protect users against emergent threats and exploits which have been discovered and unpatched devices are especially vulnerable to infection/data breach;

- agree to protect their device via a complex password (8 characters or greater, including numbers, letters, upper and lower case) or a biometric measure;

- set up any mobile device (phone, tablet, laptop) to auto-lock after a set period of idleness;

- In the eventuality that their device is lost, stolen, destroyed, returned to the manufacturer, becomes end-of-life or stops being used by you for work, must inform Elevate's Compliance Officer and immediately change all passwords related to their access to Elevate's systems;

- keep any personal data separate from Elevate data. The simplest way to achieve this is to use the One Drive or Sharepoint;

- agree to co-operate with Elevate's Central Services team when they consider it necessary to access or inspect corporate data stored on their device;

- agree that Elevate is not liable for any costs relating to their device, including but not limited to: purchase, insurance, licensing, contract costs, call charges, repairs and peripherals/ accessories;

- agree that Elevate may at any point and without consultation rescind the right to use an employee's device to access its systems and data;

- agree that Elevate is not responsible for supporting their use of this device beyond initial set up of the Trust's systems and ongoing help to use these systems.

Elevate will not monitor private usage of the device. In exceptional circumstances Elevate will require access to corporate data stored on an employee's personal device. In those circumstances every effort will be made to ensure that Elevate does not access the private information of the individual.

What is Not Allowed?

- **Emails:** Data must at all times remain within Elevate systems – emails should not be forwarded to private accounts and files should only be stored on network drives accessed remotely, a OneDrive folder or on Elevate's Sharepoint sites rather than saved elsewhere;

- **USB sticks/non approved cloud storage services:**
  USB: Employees should try and avoid using a USB stick to hold personal data but if they do it MUST be encrypted and password protected;

- **Reducing the risk of malware infection:** Employees should not engage in risky activities using the BYOD device in their private life. For example, visiting websites with gambling, adult or illegal content would place the device at greater risk of malware infection and hijacking;

- **Shared use:** If a device is in shared use by other family members, their user accounts must not have Administrator level privileges or unauthenticated access to Elevate's systems or files. This includes saving credentials to access Office 365 etc when the computer can be accessed without entering a password;

- Employees must not modify the Operating System in order to 'jailbreak' your device (this means attempting to remove restrictions which the manufacturer has built into their system). This weakens a device's security as usually software patches will not be installable from that point on.

Linked to: Elevate Acceptable use of ICT policy and staff
Elevate Data Protection policy
Elevate Information Security policy
Elevate Data Retention policy