Trinity Multi Academy Trust

Policy:	Bring Your Own Device
Date of review:	October 2018
Date of next review:	October 2020
Lead professional:	Director of ICT and Data
Status:	Non-Statutory

Scope
This policy applies to anyone connecting to the Wi-Fi or using the trust provided Office 365 accounts on their own device at or from one of the trust's academies or organisations.

This policy should be read and considered alongside the "Procedures for the secure transfer of data" document for the trust and the Acceptable Use of ICT (staff) Policy.

1 Introduction

1.1 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. By personal devices we mean smart phones, 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 Trinity MAT systems via a local network or through the VPN.

1.2 However, we need to strike a balance between the convenience BYOD offers and the security of Trinity MAT data and the integrity of our systems.

1.3 Under the Data Protection Act 2018 (DPA), Trinity MAT must remain in control of the corporate data for which it is responsible, process it lawfully and 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 you were to use your own device to access your Trinity MAT email account, Trinity MAT needs to ensure that those emails (and any attachments, etc.) do not leave its control. As an employee you are required to play a role in keeping Trinity MAT data secure. Your attention is also drawn to Trinity MAT's Acceptable Use of ICT (staff) policy which requires you as an individual to process data in compliance with all aspects of the DPA and this applies equally to processing of data which takes place in the context of BYOD. Trinity MAT's Data Protection Policy is also available on the shared area.

1.4 As an employee you are also required to assist Trinity MAT in complying with Subject Access and other requests made under the Freedom of Information Act, which may include data stored on a personal device.

1.5 The use of home PCs to access the trust 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.

1.6 Any failure to comply with this policy will be managed in accordance with the Trinity MAT Disciplinary Policy (in particular sections 2.1 and 9.1(e).

2 What are the benefits?

2.1 Some people prefer to use their personal device for reasons of ergonomics, convenience, efficiency and Operating System preferences.

2.2 Trinity MAT's licensing for Microsoft Office can be extended to cover up to 5 personal devices.

3 What are the implications for employees who want to use their own device(s) under this policy?

3.1 Your device must use one of the Operating Systems listed in Appendix 1

3.2 You must agree to Trinity MAT installing appropriate policies and certificates on your devices to enable the protection and if necessary removal of data in the event of the device being lost/stolen/damaged beyond repair etc. You must accept that in the event of a remote wipe being necessary, you may also lose any personal data stored on the device.

3.3 You must agree to keep your 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.

3.4 You must agree to protect your device via a complex password (8 characters or greater, including numbers, letters, upper and lower case) or a biometric measure.

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

3.6 In the eventuality that your device is lost, stolen, destroyed, returned to the manufacturer, becomes end-of-life or stops being used by you for work, you must inform the ICT Support helpdesk and immediately change all passwords related to your access to Trinity MAT's systems.

3.7 You must keep any personal data separate from Trinity MAT data. The simplest way to achieve this is to use the One Drive or Sharepoint which the Help Desk will assist you in accessing if needed.

3.8 You must agree to co-operate with officers of Trinity MAT when they consider it necessary to access or inspect corporate data stored on your device.

3.9 You must agree that Trinity MAT is not liable for any costs relating to your device, including but not limited to: purchase, insurance, licensing, contract costs, call charges, repairs and peripherals/ accessories.

3.10 You must agree that Trinity MAT may at any point and without consultation rescind the right to use your device to access its systems and data.

3.11 You must agree that the ICT Support Helpdesk is not responsible for supporting your use of this device beyond initial set up of Trinity MAT systems and ongoing help to use these systems.

3.12 Trinity MAT will monitor the devices connecting to its networks and reserves the right to prevent access for any device that is considered a risk to the network's integrity and security.

3.13 Trinity MAT will not monitor private usage of the device. In exceptional circumstances Trinity MAT will require access to corporate data stored on your personal device. In those circumstances every effort will be made to ensure that Trinity MAT does not access the private information of the individual.

4 What is not allowed?

4.1 Data must at all times remain within Trinity MAT systems – emails should not be forwarded to private accounts and files should only be stored on network drives accessed remotely, your OneDrive folder or on the trust Sharepoint sites rather than saved elsewhere.

4.2 Transferring data out of Trinity MAT systems for use elsewhere using removable media (USB sticks, DVDs) or non-approved cloud storage services (Dropbox, Google Drive, etc.) is not permitted. Doing so heightens the risk that data will leave Trinity MAT's control.

4.3 Do not engage in risky activities using the BYOD device in your private life. For example, visiting websites with gambling, adult or illegal content would place the device at greater risk of malware infection and hijacking.

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

4.5 You must connect your device to the appropriate Trinity MAT guest networks.

4.6 You 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.

Appendix 1 – List of Approved Operating Systems

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