



Bring Your Own Device Policy

Scope

The guidelines set out in this document apply to all United Church Schools Trust (UCST) and United Learning Trust (ULT) Central Office employees; including fixed-term, part-time, full-time and permanent staff. The application of this policy to temporary staff will be determined on a case by case basis. The two companies (UCST and ULT) are referred to in this policy by their trading name, 'United Learning'.

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 United Learning 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 United Learning data and the integrity of our systems.
- 1.3 Under the Data Protection Act 1998 (DPA), United Learning 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 United Learning email account, United Learning 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 United Learning data secure. Your attention is also drawn to United Learning's IT Acceptable Usage 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. United Learning's Employee Data Protection Policy is also available on United Hub.
- 1.4 As an employee you are also required to assist United Learning 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 extraordinary use of home PCs in the event of an unplanned Disaster Recovery scenario will be dealt with on a case-by-case basis and employees do

not need to sign this policy for that purpose. In these circumstances, access to United Learning systems and data will be provided via VPN and the browser-based Office 365 toolset.

- 1.6 Any failure to comply with this policy will be managed in accordance with the United Learning 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 United Learning's licensing for its Anti Virus software and for Microsoft Office can be extended to cover your personal device.

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 United Learning installing Mobile Device Management software on your device. This is to enable remote wiping of data should the device be 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 install United Learning's Anti Virus software on the device, or provide evidence of an equivalent which is deemed satisfactory.
- 3.4 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.
- 3.5 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.
- 3.6 You must set up any mobile device (phone, tablet, laptop) to auto-lock after a set period of idleness.
- 3.7 Where possible, the hard drive of any mobile device must be encrypted.
- 3.8 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 Technology service desk and immediately change all passwords related to your access to United Learning systems.

- 3.9 You must keep any personal data separate from United Learning data. The simplest way to achieve this is to use the OneDrive client which the Service Desk will assist you in setting up.
- 3.10 You must agree to co-operate with officers of United Learning when they consider it necessary to access or inspect corporate data stored on your device.
- 3.11 You must agree that United Learning 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.
- 3.12 You must agree that United Learning may at any point and without consultation rescind the right to use your device to access its systems and data.
- 3.13 You must agree that the Service Desk is not responsible for supporting your use of this device beyond initial set up of United Learning systems and ongoing help to use these systems.
- 3.14 United Learning 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.
- 3.15 United Learning will not monitor private usage of the device. In exceptional circumstances United Learning will require access to corporate data stored on your personal device. In those circumstances every effort will be made to ensure that United Learning does not access the private information of the individual.
- 3.16 United Learning will maintain a register of devices being used by employees under this policy.

4 What is not allowed?

- 4.1 Data must at all times remain within United Learning systems – emails should not be forwarded to private accounts and files should only be stored within the OneDrive folder rather than saved elsewhere.
- 4.2 Transferring data out of United Learning 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 United Learning'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.
- 4.5 You must not attempt to connect your device to United Learning networks except for Guest networks. This connection must be set up by the Technology service desk. This does not include connecting via VPN.
- 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.

5 What do you need to do if you want to BYOD?

- 5.1 Request the agreement of your Line Manager. They may have good operational reasons why this is not suitable.
- 5.2 Sign a copy of this policy and submit it to the Group Director of Technology for approval.
- 5.3 If approved, the Technology service desk will request your assistance to get your device set up to operate safely on our networks and with United Learning data.

6 Revisions

Version number:	1.4	Target Audience:	All Central Office staff
UCST/ULT/Both:	Both	Reason for version change:	New ICO guidance
Date Authorised:	23.1.17	Name of owner/author:	Technology Department
Date issued:	30.04.18	Name of individual/department responsible:	Tom James, Trust Board Member
Review Cycle:	Every 2 years		

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