Title	**Accessing United Learning Data Using Your Own Device Policy (Bring Your Own Device - BYOD)**
Policy Owner	**Director of IT**
Effective Date	**May 2021**
Last Revised	**June 2023**
Next Review Date	**June 2024**

1. Scope

The policy and procedure set out in this document applies to all Trustees and Governors, and to all staff employed by United Church Schools Trust ("UCST") and United Learning Trust ("ULT") including teaching, non-teaching, fixed term, part-time, full-time, permanent, and temporary staff.

2. Introduction

2.1 Under the GPDR and the Data Protection Act (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 your United Learning data secure. Your attention is also drawn to the ICT Acceptable Usage Policy which requires you as an individual to process data in compliance with all aspects of the GDPR and this applies equally to processing of data which takes place in the context of BYOD.

2.2 This policy is intended to provide a clear framework for the secure use of personal devices in the workplace and at home; "personal devices" includes but is not necessarily limited to mobile phones (both standard and smart), 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**' (BYOD).

2.3 This policy provides guidelines for staff to access their Microsoft Office 365 accounts through a browser, without undertaking the full BYOD process.

2.4 The policy aims to find a balance between the convenience that BYOD offers and the security of United Learning data and the integrity of our systems.

2.5 As an employee, you are also required to assist United Learning in complying with Subject Access Requests and other requests made under the Freedom of Information Act, which may include data stored on a personal device if it is being used for work purposes.

2.6 Compliance with this policy forms part of the employee's contract of employment and failure to comply may constitute grounds for action under United Learning's disciplinary policy.

3. Benefits of BYOD

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

3.2 United Learning's licensing for Microsoft Office covers your personal devices if required.

N.B Office 365 enables remote workers to use the software within a browser eliminating the need for a local installation or any local copies of data and therefore avoids the requirement for the full BYOD approval process.

4. General principles for keeping data secure

4.1 Data must always remain within United Learning systems – **emails must not be forwarded to private accounts** and files should only be stored within your work OneDrive rather than saved locally (to the desktop/my documents or C drive for example).

4.2 Data containing Personally Identifiable Information (PII) must not be used in a locally installed program in the Office 365 suite. PII must only be used in the cloud/browser-based versions of the software therefore if you are handling personal information, you should avoid using any full applications from the Office suite e.g. Word/Excel.

4.3 Transferring data out of United Learning systems for use elsewhere using non-approved cloud storage services (e.g. Dropbox) or removable media (USB sticks, DVDs) is not permitted.

4.4 Do not engage in risky activities using your BYOD personal device in your private life. For example, visiting websites with gambling, adult or illegal content as this places the device at greater risk of malware.

4.5 You must not allow any non-employee of United Learning to access your BYOD device (including family members). This is an important consideration when deciding whether you wish to use your own device for work. This is especially true of mobile phones and tablets where it is unlikely that separate accounts can be set up. Family use of Windows PCs/Apple Macs is allowed only if: separate accounts are set up, the account being used for work is separate, account details are not shared, and passwords meet the required United Learning complexity levels. Other accounts on the device must not be 'Admin' type accounts that grant access to other areas of the device.

4.6 You must not attempt to connect your BYOD approved device to any United Learning networks except guest networks. Your local IT Help Desk can assist with this if necessary.

4.7 BYOD approved devices must not be jailbroken, rooted or have any software/firmware installed designed to allow access to unofficial applications. This weakens device security.

5. What you need to do if you want to use BYOD

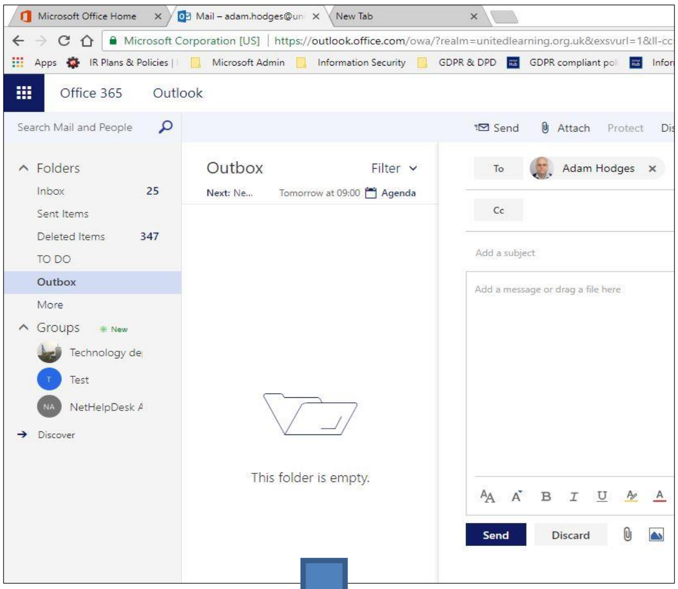
5.1 Ensure you complete the correct checklist relevant to your device (see below). Your local IT Helpdesk can support you to ensure checklist requirements are in place.

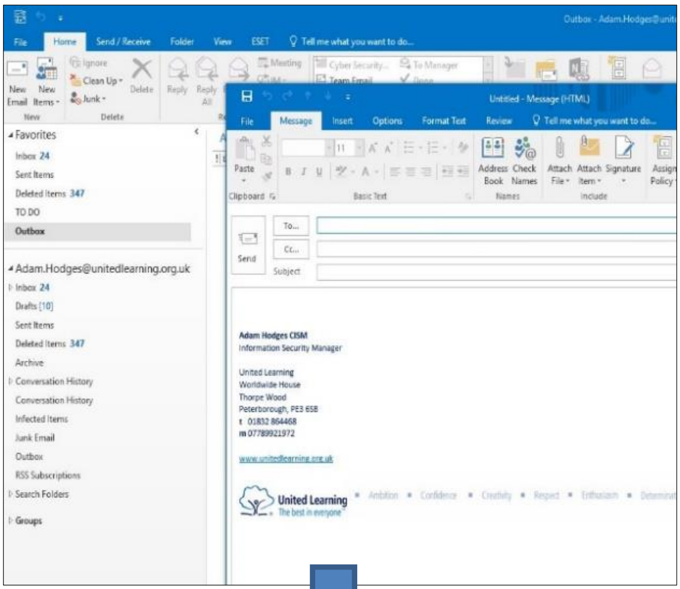
5.2 Submit the signed policy and relevant checklists to your line manager for approval.

How will you access data?

You must sign Section A and/ or Section B, depending on how you will be accessing data and systems:

I only want to read emails, check my calendar or access other United Learning or school data from within a web browser and never download data to my device.	I want to download United Learning or school data to my device and work on these with the native/ desktop applications e.g., Mail for iPhone, MS Office, Outlook.
Cloud/Browser access only For example: the email below has been composed within the latest version of Chrome. Provided that this is all done from within a browser then BYOD compliance is not needed as no personal data is stored on the device.	**Locally installed access** For example: to send the email below, the Outlook desktop application is being used to compose an email. For this scenario BYOD compliance is necessary as personal data is stored on the device.





Adam Hodges CISM
Information Security Manager

United Learning
Worldwide House
Thorpe Wood
Peterborough, PE3 6SB
t 01832 864468
m 07789921972

www.unitedlearning.org.uk

United Learning The best in everyone ▪ Ambition ▪ Confidence ▪ Creativity ▪ Respect ▪ Enthusiasm ▪ Determinat

You must complete Section A	**You must complete Section B**

SECTION A

Accessing data and systems through a browser

1. I will only access Microsoft O365 (Word, PowerPoint, Outlook, OneDrive, SharePoint etc) applications from within a current browser. Office 365 is designed to work with the current versions of Chrome, Edge, Firefox, and Safari. Internet Explorer is not supported and should not be used.
2. No documents, presentations, emails, or other files are to be downloaded to the device on which you are running the browser session. All work must be carried out within the browser-based versions of Office 365 (Outlook, Word, etc). Do not use the OneDrive sync client as it stores a copy of your files locally.
3. The device must have a current & supported Operating System and be kept up to date.
4. For all devices, an up-to-date anti-virus program must be installed.
5. School/United Learning passwords must not be stored (saved) on the device, and do not select the option to stay 'logged in'.
6. If the device is lost/stolen/sold/returned to the manufacturer or vendor, you must change your United Learning system passwords at the earliest possible opportunity.
7. Accessing your United Learning Office 365 account from an internet café (or similar) is not permitted, unless in the event of exceptional circumstances. It is always safer to use your own phone/ tablet on a hotel Wi-Fi than to entrust your credentials to a shared computer in an Internet cafe.

Signature: ……………………………………………………………………………………….

Print name: ……………………………………………………………………………………..

SECTION B Using your own device

1. I agree:

1.1 That my device will comply with the relevant checklist below, ensuring that:

- Operating Systems are supported and up to date.
- Suitable virus protection is in place.
- Hard drives/storage are encrypted.
- Device access security is in place (password/PIN/biometric).
- Office applications must be up to date i.e. Microsoft 365 Office downloaded as part of my school/work licence.

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

2.1 Your device must use one of the Operating Systems and versions listed in Appendix 1

2.2 Devices (where they reasonably can be) must be encrypted. You are strongly advised to read the advice below (see Frequently Asked Questions) on encryption and recovery keys.

2.3 You must agree to install and keep up to date satisfactory anti-virus program on Windows/MAC-OS devices used for BYOD under this policy.

2.4 You must agree to keep your device up to date with the latest operating system patches and other software (e.g. Microsoft Office 365). Software companies regularly patch their products to protect users against emergent threats and exploits which have been discovered and unpatched devices are especially vulnerable. In summary – keep your device up to date.

2.5 You must agree to protect your device via a complex password (8 characters or greater, including three of the following - numbers, upper case, lower case letters and special characters), a suitable PIN (if a password is not possible) or a biometric measure. Please see here for the United Learning Password Policy.

2.6 The United Learning Clear Desk Policy must be adhered to at all times with particular care when working on your BYOD approved device.

2.7 You must set up any mobile device (phone, tablet, and laptop) to auto-lock after a set period of idleness – a maximum of 5 minutes is suggested. Desktop devices must also be set with a timeout to prevent other users being able to view the screen.

2.8 In the event that your device is lost, stolen you must inform your IT Help Desk at the earliest opportunity (within a maximum of 48 hours) and immediately change all passwords related to your access to United Learning systems.

2.9 If your device is destroyed, returned to the manufacturer, becomes end-of-life or stops being used by you for work, you must immediately change all passwords related to your access to United Learning systems and inform your IT Help Desk.

2.9 You must keep any personal data separate from United Learning data. The simplest way to achieve this is to use the OneDrive client which your IT Help Desk can help set up for you which will store the United Learning data.

2.10 You must agree to co-operate with officers of United Learning when it is necessary to access or inspect corporate data stored on your device.

2.11 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.

2.12 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.

2.13 You must agree that the IT Help 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.
2.14 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.
2.15 United Learning will not monitor private usage of the device. In exceptional circumstances, United Learning may require access to corporate data stored on your personal device. In those circumstances, every effort will be made to ensure that a United Learning employee does not access the private information of the individual.
2.16 Your local school/centre will maintain a register of devices used by employees under this policy.

3. BYOD Checklist – Computer or Laptop

Please ensure that you understand the risk associated with encrypting hard drives should the encryption key be lost (see FAQs below).

Your name and line manager approval:

Employee Name	
Line manager approval	Signed by Click or tap here to enter text.

Now that you have authorisation to use your own device you need to complete and confirm the items below. ***Please see the FAQ section below for guidance on how to set up your device.*** It must then be checked by your local IT Helpdesk. With agreement, these two steps could be done at the same time.

		Device Owner	Technician Check
1.	What is the operating system on your personal device?		☐
2.	Do you ensure that updates are regularly applied?	Choose an item.	☐
3.	Is an appropriate Anti-Virus product installed? If so, which Anti-Virus product is installed?	Choose an item. Click or tap here to enter text.	☐ ☐
4.	Is the device protected by a compliant password/PIN/biometric?	Choose an item.	☐
5.	Is an auto lock enabled?	Choose an item.	☐
6.	Does each user of the device have their own account?	Choose an item.	☐
7.	Does the applicant have the only Admin account	Choose an item.	☐
8.	Is the device encrypted?	Choose an item.	☐

9.	Has the process for reporting a lost device been explained?	Choose an item.	□
10.	Has the level of support been explained?	Choose an item.	□
11.	Has the register of devices been updated?	Enter Device Name.	□

Signed by User: Click or tap here to enter text. **Signed by Technician**: Click or tap here to enter text.

4. FAQ – Frequently Asked Questions

Q: How can I make sure my device is updating?
A: Windows PC: Follow the link - https://support.microsoft.com/en-gb/help/12373/windows-update-faq - and select "How do I keep my PC up to date?" which will explain how to do it for Windows 10 and Windows 11
Mac OSX: Follow the steps in this link - https://support.apple.com/en-gb/HT201541

Q: Where can I get Anti-Virus software?
A: All platforms have free or paid for antivirus, talk to your technical teams for further guidance if needed.

Q: How do I password protect my device?
A: All devices must have a password/passcode to make it harder to access data if it is lost or stolen. Remember not to lose it or share it with anyone else:
Windows 10 PC: follow the advice here - https://support.microsoft.com/en-us/windows/change-or-reset-your-windows-password-8271d17c-9f9e-443f-835a-8318c8f68b9c

macOS: follow the advice here - https://support.apple.com/en-gb/HT202860

Apple Devices (iPhone, iPad, or iPod touch): - https://support.apple.com/en-us/HT204060
Android Devices: - https://www.howtogeek.com/253101/how-to-secure-your-android-phone-with-a-pin-password-or-pattern/

Q: How can I lock my screen?
A: For Windows: Follow the link https://support.microsoft.com/en-us/help/17185 - about personalising your lock screen. Alternatively you can alter your screensaver settings https://support.microsoft.com/en-us/windows/change-your-screen-saver-settings-a9dc2a0c-dc8e-9161-d270-aaccc252082a

For macOS: Follow this link - https://support.apple.com/en-gb/HT204379

Q: How can I create accounts for each user on my PC or Mac?
A: In order to password protect your PC or Mac you will need to create user accounts for each person who uses it

Windows 10 PC: follow the advice here - https://support.microsoft.com/search/results?query=create+account+windows+10

macOSX: follow the advice here - https://support.apple.com/en-gb/HT204316 and https://support.apple.com/en-gb/HT201084

Q: How do I encrypt my home PC or Mac Computer?
A: For Windows: Turn on Bitlocker.

For Mac: Turn on FileVault which is built into every new Mac Operating System - https://support.apple.com/en-gb/HT204837

Q: What is the risk of encrypting my personal device?
A: It makes it impossible to recover any data on the device if the encryption key is not kept securely (not on the device itself). Do not lose the encryption key.

Q: Why do I need to encrypt my device?
A: Encrypting the device will prevent someone, who does not know the encryption key, from accessing data on the device should it leave your control in the future.

Q: How do I encrypt my home mobile device?
A: iPhone or iPad: enabling a passcode automatically encrypts it.
Android device: follow the advice in your phone manual or check the link here. Your device encryption might already be enabled by default. https://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/

Q: How do I report the loss of my device?
A: In the first instance, you must inform your local IT Help Desk in an emergency contact ServiceDesk@unitedlearning.org.uk.

APPENDIX 1

Approved Operating Systems

- Windows 10 or later
- Apple iOS 11 or later
- Android 8 or later
- macOS 10.13 (High Sierra) or later
- Chrome OS within five years of release date