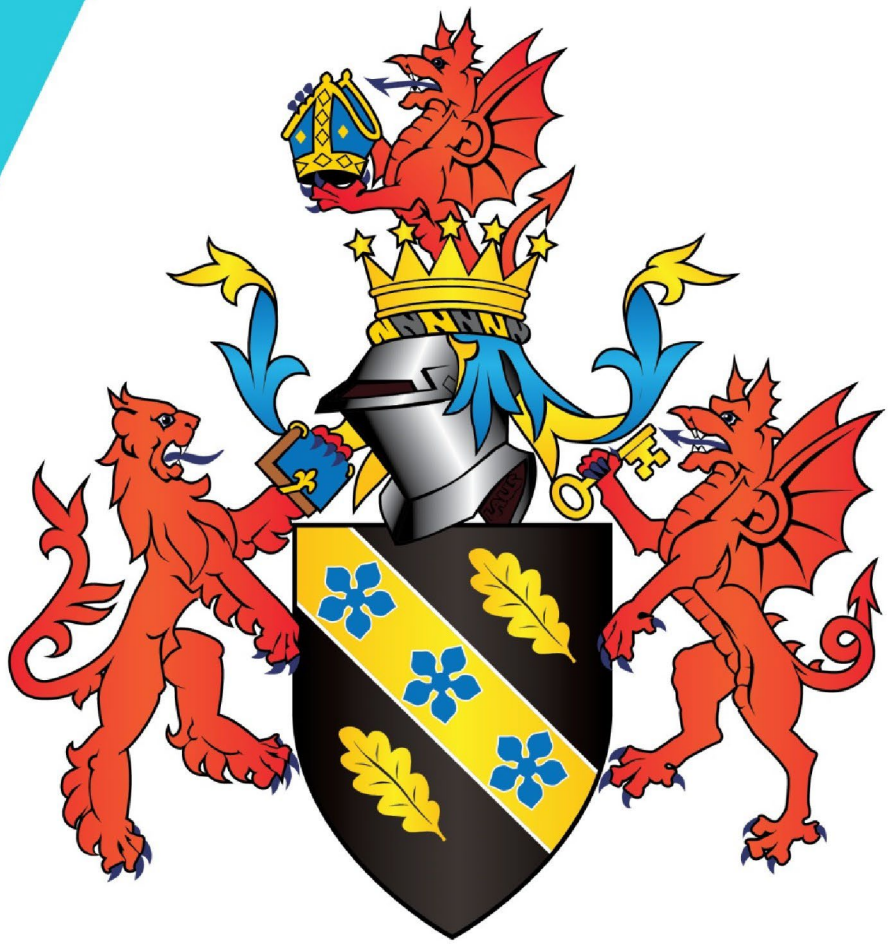
Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David



BYOD Policy

Contents

Introduction

This policy covers the use of personally owned electronic devices to access and store University information. Such devices include smart phones, tablets, laptops, desktop computers and similar technologies. This is commonly known as 'Bring Your Own Device' or BYOD.

All users who wish to use their personal devices must abide by the policy below.

The University must ensure that it remains in control of organisational 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.

Scope

This policy applies to all University staff, data processors, partners, suppliers and contractors and other authorised non-student users who have access to organisational data on BYOD devices.

For the purposes of this policy non-University managed or personal devices include, but are not limited to: home desktop PCs, tablets (iPads etc.), smartphones, laptops, video and audio recording equipment.

All devices accessing or processing organisational data are required to adhere to the Acceptable Use Policy. This policy should be read in conjunction with the IT Acceptable Use Policy.

The University wishes to support staff in the use of technology and BYOD devices however, this needs to be balanced with our legal duties and we must ensure that we remain in control of any organisational data for which the University is responsible, regardless of the ownership of the BYOD device being used to access this data.

In order to access University data when using a Personal BYOD device, there are security controls in place to protect University data. As a result, there are set processes which must be followed in order to access University data from a personal BYOD device.

The University recommends the following options in order of preference. These options are the required processes which must be followed to access University data from a personal BYOD device.

Option 1:
Wherever possible, users access university data and services from a university provided device.

Option 2:
If it is not possible to utilise a University provided device, then users should, where possible, only access University owned data and Cloud services such as Microsoft 365 Email from a BYOD device using an Internet Web Browser interface.

Option 3:
Users requiring access to University owned data and Cloud services such as Email via a mobile application or desktop application such as Office 365 will be required to enrol their device into the University's Mobile Device management (MDM) solution - Intune.

Device Enrolment

Device enrolment enables users to access UWTSD services such as Microsoft Teams, OneDrive and Email from an application such as Microsoft 365 installed on a mobile device or a laptop/desktop device.

Device enrolment registers your device with UWTSD and applies compliance policies which may include requirements such as ensuring that the device is running a supported operating system, Antivirus, Firewall etc. These compliance policies keep your BYOD device and UWTSD data secure from unauthorised access.

BYOD devices must satisfy the compliance policies or access to University owned data will be blocked.

Important Information

To ensure transparency, by enrolling your personal Windows 10, Windows 11 or Apple MacOS device in the University's MDM solution "Microsoft Intune"; Microsoft provides UWTSD with the functionality to remotely reset your device to its out of box experience. Although this functionality means it is technically possible to remotely reset this type of personally enrolled device, UWTSD policy is that it will never factory reset a personal device and we are actively engaging with Microsoft to determine if this functionality can be removed in the future. This functionality is not available to the University for any personal Android or Apple iOS devices which are enrolled.

Before taking the decision to enrol your device you must ensure that your data is backed up to an external source such as an external drive or cloud storage. How to Back Up Your Data and Keep Your Files Safe (techtarget.com)

By enrolling your device, you acknowledge that the University will not be responsible for any loss of data from your device.

Security Compliance Settings

By enrolling your device, you acknowledge that your personal device will have required security controls enforced on your personal device to ensure that University data is secure.

These security controls include, but are not limited to:

- If you device does not have a password/PIN set prior to enrolment, you will be required to set an appropriate password/PIN;
- If your device has a password/PIN set prior to enrolment which does not meet the required complexity requirements, you will be required to change your password/PIN to one which meets the security password minimum length requirement;
- Your device will be forced to automatically screen lock after period of inactivity.

Before taking the decision to enrol your device you must ensure that you have read and accepted the University's BYOD Security Compliance Settings requirements.

Access to Personal Data

The University cannot see any personal information on your Personal BYOD Device at any stage after you enrol your device in Microsoft Intune.

Enrolling your device does, however, make certain information, such as device model and serial number, visible to authorised UWTSD IT support staff with administrator access.

To find out more about what can and cannot be seen, please visit Microsoft's Device Enrolment Information webpage.

To help, we have summarised what can and cannot be seen on your Personal BYOD Device.

Information University IT Administrators CAN NEVER see:

- Calling and web browsing history
- Email and text messages
- Contacts
- Calendar
- Passwords
- Pictures, including what is in the photos app or camera roll
- Files

Information University IT Administrators CAN see:

- Device Owner
- Device name
- Device serial number
- Device model, such as Google Pixel
- Device manufacturer, such as Microsoft
- Operating system and version, such as iOS 12.0.1
- Device IMEI
- App inventory and app names, such as Microsoft Word
    - On personal devices, your organization can only see your University-managed app inventory, which includes work and school apps downloaded from the University company portal. Any personal apps cannot be seen.

Storing of Sensitive Information

- Users should not hold any information that is sensitive, personal, confidential or of commercial value on personally owned devices.
- If online access is not feasible and you legitimately need to access or store sensitive information, such as student or financial records on your own device for a limited period, you must seek authority from your Line Manager. The University may then need to monitor the device at a level that may impact your privacy by logging all activity on the machine. This is in order to ensure the privacy, integrity and confidentiality of that data.
- Where it is essential that information belonging to the University is held on a personal device it should be deleted as soon as possible once it is no longer required, including information contained within emails.
- It is the BYOD owner's responsibility to ensure that no University information is left on any personal device indefinitely and to make sure data is removed before a device is disposed of, sold or transferred to a third party.

Responsibility of Users

The University takes information and systems security very seriously and invests significant resources to protect data and information in its care. Individuals who make use of BYOD must take responsibility for their own device and it's security.

Mobile Devices

Users using mobile devices such as Tablets, Smart Phones etc. to access and process organisational data **must ensure that**:

- They read and comply with this BYOD policy and the University's Acceptable Use Policy.
- Devices must be kept up to date with manufacturer, vendor or network provided patches.
- Devices must only use the latest Operating Systems which are in support by the manufacturer/Vendor – https://endoflife.date/
- They only use Microsoft Outlook as the supported email client on mobile devices.
- They use device security features, such as a strong PIN/Password/Passphrase, Biometric and automatic lock to help protect the device when not in use which complies with the University's Security Compliance settings for BYOD.
- They use encryption to ensure the protection of data stored/information at rest.
- They install and configure tracking and/or wiping services, such as Apple's 'Find My iPhone', Android's 'Where's My Droid' or Windows 'Find My Phone', where the device has this feature.
- They only have trusted applications from reputable/official sources installed.
- They do not attempt to circumvent the device manufacturer's security mechanisms in any way, for example 'jailbreak' or "Root" 1 the device if it is being used to access University IT services.

End User Devices

Users using devices such as Windows Desktops/Laptops MacOS, Linux devices to access and process organisational data **must ensure that**:

- They read and comply with this BYOD policy and the University's Acceptable Use Policy.
- Devices must be kept up to date with manufacturer, vendor or network provided patches.
- Devices must Only use the latest Operating Systems which are in support by the manufacturer/Vendor – https://endoflife.date/
- Devices must have software & security updates installed within one week of their release.
- Devices must have recognised, up-to-date and enabled Anti-malware/Virus protection.
- Devices must have a local firewall enabled where available.
- They ensure device security features, such as a strong PIN/Password/Passphrase, Biometric and automatic lock to help protect the device when not in use which complies with the University's Security Compliance settings for BYOD.
- They only use Microsoft Outlook as the supported email client on mobile devices.
- They use encryption to ensure the protection of data stored/information at rest.
- They do not load pirated software or illegal content onto their devices.
- They do not attempt to circumvent the device manufacturer's security mechanisms in any way, for example 'jailbreak' or "Root" 1 the device.
- They only have trusted applications from reputable/official sources installed.
- They ensure that software on devices are appropriately licenced.

Consequences of Non-Compliance

The University reserves the right to refuse, prevent or withdraw access to users and/or devices or software where it considers that there are unacceptable security or other risks to its staff, students, business, reputation, services or infrastructure.

Loss of Device

In the event that your personal device is lost/stolen or its security is compromised in any way, you should report the issue immediately to the University IT Service Desk to enable the University to revoke access to University data from the lost BYOD device.

Monitoring and Access

The University will not routinely monitor personal devices. In the interest of protecting University data, if deemed required from a security perspective, if your device was suspected as being compromised or potentially a security risk to University data, it does reserve the right to:

- Prevent access for that device to either the University wired or wireless networks, or both;
- Prevent access to a particular University system;
- Take necessary and appropriate steps to revoke access to information owned by the University.

If the University is required to take any of these actions in order to help protect University data, the IT Service Desk will contact the owner of the personal BYOD device via official University contact methods.

Support of BYOD Devices

The University takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding employee-owned devices, or for any loss or damage, resulting from support and advice provided.

Related University policies, procedures and guidance

- IT Acceptable Use Policy
- Data Protection Policy
- BYOD-Security-Compliance-Settings.pdf (uwtsd.ac.uk)

Policy author(s):

Richard Thomas – Executive Endpoint Management & Security Engineer

Document version control

Version No:	Reason for change:	Author:	Date of change:
0.1	Draft	RT	19/05/2022
0.2	BT Review & content update	BT	01/06/2022
0.3	BT Review & content update	BT	09/12/2022
0.4	BT/JC Review, PO DPIA approval & content update	BT	09/02/2023
0.5	OLT review and approval	BT/JC/RD	22/02/2023
0.6	Senior Directorate review and approval	BT	28/02/2023

Current status of Policy: Approved

Date effective from: 14.03.2023

Policy review date: Annually