V1

Bring Your Own Device (BYOD) Policy

BATH SPA
UNIVERSITY

1. Purpose

1.1 This policy defines acceptable use by staff whilst using a personally owned device to access University systems, services, and data. This policy applies to staff and other users, it does not apply to students

2. Definitions

2.1 BYOD / Bring Your Own Device

BYOD / Bring Your Own Device refers to personally owned devices (devices not provided to you by the University) that access organisational data or services. This does not include personally owned devices that are only used for the purpose of:

- Native voice applications (cellular phone calls and Wi-Fi enabled calling)
- Multi-factor authentication (MFA) applications

Personal devices include all items that have processing ability or internet connectivity. This includes all types of assistance, organisational or internet of things (IoT) devices.

2.2 Cyber Essentials

Is an effective, government-backed scheme that helps organisations protect themselves against common cyber-attacks. It is a certification scheme that demonstrates an organisation meets the minimum level of cyber security as defined by the National Cyber Security Centre (NCSC).

2.3 Data Controller

Bath Spa University is the Data Controller, which holds responsibility for and determines the purposes and means of processing personal data.

2.4 User

A member of staff, student, contractor, or another person authorised to access the University's systems.

2.5 Mobile Device Management

A methodology and toolset that provides a workforce with mobile productivity tools and applications while keeping organisational data secure.

2.6 Mobile Application Management

A service that secures, manages and distributes mobile apps used in an organisation.

3. Policy

This policy covers non-University owned devices (BYOD) that are used by staff to access University systems or data. Such devices include but are not limited to smart phones and tablets.

The University would like to support staff using their own personal devices; however, it also needs to comply with security standards such as Cyber Essentials. Legal duties as a data controller exist to protect the information held pertaining to staff, students and others. This policy is about reducing the risk when using a personal device, which includes devices being used by others, exploited in such a way to put University data at risk, lost or stolen.

Although this policy defines how a member of staff may be able to access University data and services using a personal device, it is recommended that:

University data and services should be accessed using a University-managed device wherever possible.

3.1 BYOD information security controls

The University takes information security very seriously and invests significantly to protect the data it holds. To be able to gain access to University data from a personal device, there are technical controls that must be put in place; these controls can benefit the device owner and provide a level of assurance as to the secure configuration of a personal device.

Technical controls ensure that a device is compliant with the latest Cyber Essentials standards, and may include details such as:

- Device security features are appropriately enabled such as a PIN, password or biometric lock;
- Automatic screen lock is enabled to protect the device when not in use, with a maximum 5 minute idle time;
- The device runs a supported operating system, and has the latest security updates installed;
- The University can identify the make and model of devices accessing business data to check they receive security updates, other technical details may be recorded in accordance with the cyber essentials standards;

It is important to note that these technical controls will not enable the University to see any personal data. Further details of the activities permitted by Bath Spa's MDM are set out in the table below.

The University cannot:	*The University can:*
- View call and web history - Access device location - View text messages - View personal email accounts, documents or photos - View contacts or personal calendars - Access or reset your personal passwords	- View the device's make, model and serial number - View the version of the Operating System on your device - View the names of installed Applications - View the name and phone number associated with your device

- Remove your personal data, photos or apps from your device	

Table 1: Summary of University MDM controls

3.2 Implementation of technical controls

The University works with a leading MDM solution from Microsoft. It provides a secure cloud-based service that can monitor and manage the security of an enrolled device, or isolate university data on a registered BYOD device using Mobile Application Management.

Enrolment, or registration of a device into this solution is an enabler for access to University data that the device owner has permission to access. Not all data is available when using BYOD and the University does retain the right to remove access. Enrolment or registration invokes the technical controls as defined within the BYOD technical standards document. Should a device fail to meet the Cyber Essentials requirements in the future, access to University data will be revoked.

At the time of writing, the following operating systems are supported for access:

- Android
- iOS
- iPadOS

The University is currently unable to support Windows or macOS for BYOD. Microsoft 365 services (including email) can therefore only be accessed from the following:

- A managed University device, or
- A compliant BYOD device (Android, iOS, iPadOS)

Where possible, the University will require technical controls for BYOD that have the minimum impact on a user's device, whilst still maintaining the standards required. This includes the use of Mobile Device Management (MDM) and Mobile Application Management (MAM) where appropriate. Mobile Device Management (MDM) entails personally owned devices being enrolled to provide the university a degree of control over the device and its security settings, which is often referred to as 'partly managed'.

With Mobile Application Management (MAM), the user manages all aspects of the device, except for the work applications, which are held in a container on the device and managed by the organisation. Utilising this method provides the university ownership of its data and resources stored within a container on the device, while preserving the privacy of other content stored by the owner of the device.

Changes may occur throughout the life of this policy. IT Services maintain documentation and guidance and can advise on the continually adapting certification requirements that reflect the cyber threat landscape.

3.3 Using BYOD is a choice, not a requirement

If you do not wish to enrol or register your personal devices, then you should not use your personal devices for work purposes other than as defined within the BYOD / Bring Your Own Device definition. Using an authenticator app for MFA as an example does not require device enrolment.

3.4 Monitoring of User-Owned devices

The University will not monitor the content of personal devices; however the University can monitor and log network traffic transferred between personal devices and organisational systems, which includes access via internal networks and when accessing the University from the internet.

In rare circumstances the University may request an employee's support in resolving requests that may relate to data residing on a personal device. The University may be required to comply with its legal obligations or obliged to do so by a law enforcement authority.

3.5 Support

If you need any assistance with enrolment or registration of your personal device, please visit the IT Services website. You will find guides and access to MyServices, your self-service portal for problem solving and requesting support.

https://www.bathspa.ac.uk/it-services/

The University takes no responsibility for maintaining or repairing an employee-owned device, or for any damage or loss that may be incurred through its use. Personal device enrolment is at the discretion of the user.

3.6 Disciplinary Matters

Any breach of policy may result in disciplinary action being taken. Please refer to the disciplinary policy for more details.

Document Details

Responsible Office: IT Services

Responsible Officer: Chief Information Officer

Approving Authority: Senior Leadership Group

Date of latest approval: 4 March 2024

Effective Date: 1 July 2024

Related Policies and Procedures: Data Protection Policy, Information Classification Scheme, Regulation for using Computer Facilities.

Supersedes: New

Next review due: March 2029