Bring Your Own Device Policy (BYOD)

The Purpose of this Document: This document describes acceptable use pertaining to using your own device whilst accessing University systems, services and data.

This document will be reviewed every 12 months

Document Control
Reference: BYOD Policy
Issue No: 2 Issue Date: 24.05.2018
Author: Director of IT Services

Executive Summary

This policy defines acceptable use by University users whilst using "their own" devices, systems and applications, for accessing, viewing, modifying and deleting of University held data and accessing its systems.

Intended Audience

This policy document applies to:

• All Users accessing Newman University systems, services and data

• Any auditor, internal or external, appointed to review the process

Assumptions and Constraints

Newman University ("the University") is a data controller, for the General Data Protection Regulation (GDPR), 2018. It is assumed that all staff have an awareness of the GDPR and the consequences of the loss of University owned personal data, as GDPR training is mandatory.

Governance

IT management is regulated by the Information Security Policy and suite of IT User Policies including the Information Security Policy. The BYOD policy will be subject to review, in line with University guidelines, for effectiveness.

Definitions

BYOD / Bring Your Own'

BYOD / 'Bring Your Own' refers to Users using their own device or systems (which are not owned or provided to you by the University) or applications, to access and store University information, whether at the place of work or remotely, typically connecting to the University's Wireless Service or VPN

Data Controller

The Data Controller is a person, group or organisation (in this case the University) who determines the purposes for which and the manner in which any personal data are, or are to be, processed.

User

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

Policy

1. Introduction

This policy covers the use of non-University owned/issued electronic devices which could be used to access corporate systems and store University information, alongside their own data. Such devices include, but are not limited to, smart phones, tablets, laptops and similar technologies. This is commonly known as 'Bring Your Own' or BYOD. If you wish to BYO to access University systems, data and information you may do so, provided that you follow the provisions of this policy and the advice and guidance provided through the IT Helpdesk. It is the University's intention to place as few technical and policy restrictions as possible on BYOD subject to the University meeting its legal and duty of care obligations.

The University, as the Data Controller, remains in control of the data regardless of the ownership of the device. As a User you are required to keep University information and data securely. This applies to information held on your own device, as well as on University systems. You are required to assist and support the University in carrying out its legal and operational obligations, including co-operating with IT Services or the Data Protection Officer (DPO) should it be necessary to access or inspect University data stored on your personal device. The University reserves the right to refuse, prevent or withdraw access to Users and/or particular devices or software where it considers that they are unacceptable in terms of security, or other risks, to its staff, students, business, reputation, systems or infrastructure.

2. Advice and Guidance

Advice and guidance on all aspects of this Policy are available via the IT Helpdesk or by contacting the Director of IT Services.

3. System, Device and Information Security

The University takes Information and Systems Security very seriously and invests significant resources to protect data and information in its care. The use of your own device MUST adhere to the IT User Policies, namely the Information Security Policy, Bring Your Own Device (BYOD) Policy, General Conditions of Use of Computing and Network Facilities and Wireless Networking Policy.

In particular, when you use your own device as a work tool, you MUST maintain the security of the University's information you handle (which includes but is not limited to viewing, accessing, storing, sharing, deleting or otherwise processing).

From time to time, the University may require that you install or update University-approved device management software on your own device.

It is your responsibility to familiarise yourself with the device sufficiently to keep data secure. In practice this means:

- Preventing theft and loss of data (using Biometric/PIN/Password/Passphrase lock)
- Keeping information confidential, where appropriate.
- Maintaining the integrity of data and information.

3.1 You MUST:

3.1.2 Use the device's security features, such as a Biometric, PIN, Password/Passphrase and automatic lock to help protect the device when not in use.

3.1.3 Keep the device software up to date, for example using Windows Update or Software Update services.

3.1.4 Activate and use encryption services and anti-virus protection if your device features such services.

3.1.5 Install and configure tracking and/or wiping services, such as Apple's 'Find My iPhone app', Androids 'Where's My Droid' or Windows 'Find My Phone', where the device has this feature. This is to enable you to locate or wipe your device should it go missing.

3.1.6 Remove any University information stored on your device once you have finished with it including deleting copies of attachments to emails, such as documents, spreadsheets and data sets as soon as you have finished using them.

3.1.7 Remove all University information from your device and return it to the manufacturers' settings before you sell, exchange or dispose of your device.

3.2 You MUST NEVER:

3.2.1 Retain personal data from University systems on your own device. During the process of receiving a password protected attachment, the file may automatically store on your device. This file should be deleted as soon as it has been used or if it needs to be kept, transferred to onto a USB (either an encrypted USB or as a password protected attachment).

3.2.2 If you are in any doubt as to whether particular data can be stored on your device you are required to err on the side of caution and consult with your manager, or seek advice from the IT Helpdesk.

3.2.3 Personal data as defined by the GDPR may not be stored on personal cloud services. You should use the University provided storage (such as the S-drive and Z-drive).

3.2.3 The loss of theft of a device

3.3.1 In the event that your device is lost or stolen or its security is compromised, you MUST promptly report this to the IT Helpdesk, in order that they can assist you to

change the password to all University services (it is also recommended that you do this for any other services that have accessed via that device, e.g. social networking sites, online banks, online shops).

3.3.2 In the event that it is necessary to do so, you must also cooperate with Director of IT Services in wiping the device remotely, even if such a wipe results in the loss of your own data, such as photos, contacts and music.

3.3.3 You MUST NOT attempt to circumvent the device manufacturer's security mechanisms in any way, for example to 'jailbreak' the device.

3.3.4 Further advice on securing personal devices (including advice on the risks of downloading untrusted Apps) is available from the IT Helpdesk.

4. Monitoring of User Owned Devices

4.1 The University will not monitor the content of your personal devices, however the University reserves the right to monitor and log data traffic transferred between your device and University systems, both over internal networks and entering the University via the Internet.

4.2 In exceptional circumstances, for instance where the only copy of a University document resides on a personal device, or where the University requires access in order to comply with its legal obligations (e.g. under the GDPR 2018, the Freedom of Information Act, or where obliged to do so by a Court of law or other law enforcement authority) the University will require access to University data and information stored on your personal device. Under these circumstances all reasonable efforts will be made to ensure that the University does not access your private information.

4.3 Under some circumstances, for example where you legitimately need to access or store certain types of information, such as student or financial records on your own device, you must seek authority from your Line Manager. The University may then need to monitor the device at a level which 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.

4.4 You are required to conduct work-related, online activities in line with the University's Computer Use Regulations. This requirement applies equally to using devices of your own used for work purposes.

5. Responsibilities regarding Device Support

5.1 Where possible the University supports all devices, but you have a responsibility to learn how to use and manage your device effectively in the context of this policy. Help and advice is available on a reasonable endeavours basis, via the IT HelpDesk, including help installing and configuring apps and other software. Helpguides are available on SharePoint and IT Newsletters are available here IT support forums are maintained on Moodle.

5.2 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.

6. Working Off-Site

6.1 The University is working towards a secure VPN system. Until that time, if you need to access work-related personal data on your own device you should map the Z-drive, or if that is unavailable on your device, password protect the files containing personal data on a USB / flash drive.

6.2 The files containing work-related personal data should remain on the USB / flash drive and not be stored on your own device.

7. Compliance Sanctions and Disciplinary Matters

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

8. Equality and Diversity

This Policy has been reviewed for accessibility and inclusion purposes and has positive benefits, allowing the use of a broad range of devices to meet individual needs.

9. Feedback and Further Information

The University welcomes feedback on this Policy. If you would like to comment or need further information on BYOD please contact the IT Helpdesk or the Director of IT Services.

10. This policy is related to the following policies and procedures:

Data Breach Reporting Procedure
Data Protection Glossary
Data Protection Policy
Email Procedures regarding Data Protection
Encrypting and Decrypting files and folders using 7-Zip
General Conditions of Use of Computing and Network Facilities
Information Classification Table
Procedure for Responding to a Data Subject Access Request
Virus Management Policy
Wireless Networking Policy