Information Security BYOD Procedure

Section 1 - Audience

(1) This document sets out the terms of use for ‘bring your own device’ (BYOD) within the University of Newcastle (University).

(2) This procedure applies to all students, and employees, including permanent and temporary staff, contractors, conjoints, and affiliates, who utilise a physical or wireless connection to University network infrastructure.

Section 2 - Scope

(3) This procedure applies to any device or accompanying media that may be used to access the systems and data of the University, whether it is used within or outside your standard working or study hours.

Section 3 - Purpose

(4) Technology is part of the everyday life of the modern University student and worker. Consumer technology is evolving quickly and is often more advanced than the technology available in the classroom or the workplace.

(5) Students and staff increasingly prefer to use their own smartphones, tablets and other devices to access information. Empowering them to do so supports greater mobility and flexibility.

(6) The purpose of this procedure is to:

a. allow users to ‘bring your own device’ (BYOD) for study or work purposes, and access University information when and where it is needed; and to
b. ensure that University systems and data are protected from unauthorised access, use or disclosure.

(7) This BYOD Procedure has been informed by the NSW Government Mobility Solutions Framework.

Definitions in the Context of this Procedure

Defined Term	Meaning
Application or App	Computer software designed to assist end users to carry out useful tasks. Examples of applications may include the Microsoft Office suite of products or smartphone applications such as Google Maps.
Bring Your Own Device (BYOD)	Any electronic device owned, leased or operated by an employee, contractor, affiliate or student of the University which is capable of storing data and connecting to a network, including but not limited to mobile phones, smartphones, tablets, laptops, personal computers and netbooks.
Data	Any and all information stored or processed through a BYOD. University data refers to data owned, originating from or processed by University systems.
Device hygiene	BYOD must have appropriate and up-to-date ‘hygiene’ solutions such as anti-virus software installed.

Defined Term	Meaning
Minimum requirements	The minimum hardware, software and general operating requirements for a BYOD.
Mobile Device Management (MDM)	Solution which manages, supports, secures and monitors mobile devices.
Wipe	A security feature that renders the data stored on a device inaccessible. Wiping may be performed locally or remotely, via an MDM product, or by a system administrator.

Related Documents

(8) This procedure supplements the University's Information Technology Conditions of Use Policy.

(9) Device Owners should also have regard to the statutory rules, policy documents and standards available in the associated information tab of this policy. They provide direct or related guidance for the use of technology and the collection, storage, access, use and disclosure of data by the University.

Section 4 - Terms and Conditions of BYOD Use

(10) This procedure must be reviewed before using any BYOD. Acceptance of the Information Technology Conditions of Use Policy also constitutes acceptance of the terms of this BYOD Procedure.

(11) Acceptance indicates agreement to the following standard terms:

a. acceptable BYOD – any device may be considered for use as a BYOD providing it meets the minimum requirements set out in this document;
b. minimum requirements – the responsibility to meet the minimum requirement outlined in section 5 rests with the device owner;
c. matching University requirements and user needs – BYOD capabilities and device profiles must match University requirements as well as user requirements for study or work. For example, a tablet or smartphone might be suitable for information consumers, whilst a laptop or desktop profile would be a better match for information creators;
d. authority – users agree to provide limited authority over the device for the sole purpose of protecting University data on BYOD. This authority includes permission to wipe the device in the event of loss or disposal. This may include personal data, address books and e-mail depending on the data classification of University information stored locally on the device and whether an Mobile Device Management (MDM) tool is used. This authority remains in place from the time the device is registered until it is de-registered;
e. security – users are responsible for ensuring that personal devices are adequately secured against loss or theft;
f. support – users are responsible for replacing, maintaining and arranging technical support for BYOD. The University will only provide best efforts support for any applications that the University has provided and for network connection troubleshooting;
g. access at University's discretion – access to University systems and data is provided at the sole discretion of the University. Access may be revoked at any time and for any reason;
h. enforcement – all breaches of this procedure will be treated seriously and may result in disciplinary action.

Section 5 - Requirements

Bring Your Own Device Minimum Requirements

(12) The table below summarises the University's minimum requirements for BYOD:

Function	Minimum Requirement
Configuration Management	
Operating Systems	BYOD must use a legitimate, up to date, and vendor-supported operating system. This excludes 'jail broken' devices.
Network authentication	Network authentication is subject to the University's requirements, being 802.1x for wireless or wired connection, and authentication via an SSL VPN for remote access to the network.
Password protection / User authentication	BYOD must support password, PIN or biometric authentication.
Automatic Device Lock	BYOD must have the automatic lock enabled.
Device hygiene	BYOD must have appropriate and up to date anti-virus installed.
Lost and stolen devices	If a BYOD is lost or stolen, and it contains University data, the loss or theft must be immediately reported to the 17000 IT Service Desk.
Mobile device disposal	All University data must be removed from the BYOD at the end of its use within the University environment.
Software licensing	Users are responsible for ensuring that appropriate licensing exists for operating systems and applications running on BYOD.
Security Management	
Mobile device management (MDM)	The University has the ability, through MDM capabilities, to enforce certain policies on mobile devices, including BYOD, to ensure the security of University data. This includes, but not limited to, enforcing screen locks, pin codes and the ability to remotely wipe University data.
Service Management	
BYOD authority	Where a device is used for BYOD, and contains University's data, the device owner agrees to provide the University with physical or logical access to the device for the sole purpose of protecting University data on the device.
Mobile device application control	The University may push and remove University data to and from BYOD to enhance its security or manageability through the use of MDM software.
Device Support	Each user is responsible for the management and support of their own BYOD. Refer clause (22).

Device Registration, Configuration and Management

(13) Each BYOD will be automatically registered within the University's Office 365 platform upon first connection to the exchange email service.

(14) The Office 365 platform incorporates MDM capabilities which can enforce security configurations on BYOD.

(15) A limit may apply to the number of devices that can be registered.

(16) Device owners acknowledge that:

a. the University may directly and/or remotely change the security configurations of your BYOD to protect University data and software stored on the device. These changes include, but are not limited to:
   i. refusal to register a device that fails minimum requirements (outlined above) or that currently has installed banned software and services listed at "What Applications are Forbidden on the University Network?";
   ii. configuring certain security settings;
   iii. preventing the user from changing certain security settings;
   iv. applying a login code with an acceptable level of complexity to enable secure access to the device;

v. automatically locking the device after an inactivity timeout period;
vi. installing software and digital certificates necessary to maintain security;
vii. encrypting data stored on the device;
viii. automatically wiping either all data OR all University data (depending upon the BYOD’s capabilities) after a specific number of failed login attempts;
ix. should any configurations be removed that are required for proper and secure use of the device with University systems, these may be re-applied or access to University systems and data will be restricted if the configurations cannot be reinstated;

b. any University data stored on the BYOD remains the sole property of the University;
c. the University has a right to inspect University data held on BYOD;
d. the University may remotely monitor your device to ensure security and software configurations are maintained.

(17) Device Owners will not be prevented from installing software or applications on their device. However, the University may block access to University ICT services if any software, applications or data present a threat to University's ICT environment.

Device Usage and Support

(18) The use of University services are at the sole discretion and risk of the device owner.

(19) The University does not impose a charge on device owners for registering BYOD on the University network.

(20) Device Owners are responsible for supporting their own devices. The University will only provide limited support for any applications the University has provided.

Support	Responsibility
Physical provisioning	Device owner
Replacement of defective / damaged device	Device owner
Operating system support including licensing	Device owner
Application support of device including licensing	Device owner
University provided / supported mobile applications	17000 IT Service Desk
University provided / supported thin-client applications such as Citrix	17000 IT Service Desk
Device connectivity / access	**Responsibility**
Mobile internet	Device owner
Home internet / broadband	Device owner
VPN client	17000 IT Service Desk
University wireless	17000 IT Service Desk

(21) The University is not responsible for:

a. any costs incurred through BYOD use. The University will not reimburse any voice or data charges, software or application acquisition fees, nor support or insurance costs associated with BYOD use;
b. any inconvenience that may be experienced in connection with using University ICT services on BYOD.

(22) The University will not monitor:

a. the phone call or text message history of a BYOD. Where needed (for example, in the case of a disciplinary matter) the call and text messages may be requested;
b. the web browser history on your BYOD when not connected to University network(s), unless the web traffic is directed through the University's network infrastructure.

(23) The University may:

a. lock access to a BYOD;
b. prevent a BYOD from connecting to University ICT services;
c. restrict access to internet websites or network services for operational or policy reasons while a device is connected to University networks, including either wireless or cabled connections;
d. monitor use of BYOD while it is connected to the University network. This information may be collected and archived, and may be subject to public access under the Government Information (Public Access) Act 2009;
e. wipe personal and/or University data from a device in accordance with the following circumstances:
    i. a BYOD is reported as being lost/stolen to the 17000 IT Service Desk;
    ii. the device owner ceases employment, affiliation or studies with the University;
    iii. there is a suspected security breach. Examples include, but are not limited to, modification of the BYOD’s operating system, breaching University policies, or the detection of viruses or malware on the device.

(24) Device Owners are responsible for abiding by all license terms and conditions applicable to any software, apps, or data provided by the University.

(25) While the University will take all reasonable efforts to ensure service is available, the University does not guarantee that access to University ICT services or data will be available at all times.

(26) If your BYOD is lost or stolen, you are responsible for reporting the event as soon as practicable to the 17000 IT Service Desk on +61 2 492 17000.

Protection of University data on your BYOD

(27) University data classified as Highly-Restricted or that is subject to legal or professional privilege must not be stored on BYOD.

(28) University data must only be backed up to approved locations within University systems.

(29) You should check your BYOD to ensure that automated cloud backup is disabled. This is to ensure that University data is not inadvertently leaked, compromised or mishandled.

(30) You should take reasonable steps to reduce the risk of losing your personal data. You may, for example, store your personal data separately from University data through file partitions or using a separate memory card.

(31) You are responsible for backing up and restoring the data and configuration settings of your BYOD.

(32) The University is not responsible for any personal loss or damage suffered as a result of actions undertaken by the University to protect University data stored on BYOD.

Device De-registration

(33) The University at its own discretion, may:

a. de-register any BYOD at any time without warning; or
b. de-register a BYOD that has not consumed University ICT services for more than 12 months.

(34) Device Owners can de-register BYOD at any time by visiting the Office 365 portal. The device may not be able to connect to University ICT systems and data, unless it is re-registered.

(35) Device Owners are encouraged to wipe or remove personal data from devices before being disposed, sold or gifted.

Status and Details

Status	Historic
Effective Date	17th June 2019
Review Date	17th June 2021
Approval Authority	Chief Information Officer
Approval Date	17th June 2019
Expiry Date	13th November 2022
Responsible Executive	David Toll Chief Operating Officer
Enquiries Contact	Information Security Team

Glossary Terms and Definitions

"University" - The University of Newcastle, a body corporate established under sections 4 and 5 of the University of Newcastle Act 1989.

"Risk" - Effect of uncertainty on objectives. Note: An effect is a deviation from the expected, whether it is positive and/or negative.

"Student" - A person formally enrolled in a course or active in a program offered by the University or affiliated entity.

"Staff" - Means a person who was at the relevant time employed by the University and includes professional and academic staff of the University, by contract or ongoing, as well as conjoint staff but does not include visitors to the University.