Information Security BYOD Procedure

Section 1 - Procedure

Audience

(1) This document sets out the terms of use for 'bring your own device' (BYOD) within the University of Newcastle. The procedure applies to all employees of the University, including permanent and temporary staff, contractors, affiliates and students of the University.

(2) It affects any device or accompanying media that you may use to access the systems and data of the University, whether they are used within or outside your standard working or study hours.

Purpose

(3) Technology is part of the everyday life of the modern University worker. Consumer technology is evolving quickly and is often more advanced than the technology available in the workplace. Employees increasingly prefer to use their own smartphones, tablets and other devices to access corporate information. Empowering them to do so supports greater workplace mobility and flexibility.

(4) The purpose of this procedure is twofold. Firstly, it aims to allow you to 'bring your own device' (BYOD) for business purposes. You can access University information when and where you need to do so. Secondly, the procedure aims to ensure that University systems and data are protected from unauthorised access, use or disclosure.

(5) This BYOD Procedure has been informed by the NSW Government Mobility Solutions Framework. The Framework assists in defining the University's specific mobility strategy.

Terms and Conditions of BYOD Use

(6) The purpose of this procedure is to allow you to use a BYOD if you wish to do so, while also ensuring you take steps to minimise the risk of unauthorised access to University systems or unauthorised use or disclosure of the data held by the University.

(7) You must review this procedure before using any BYOD. Your acceptance of the terms of the Conditions of Use Policy also constitutes acceptance of the terms of this BYOD procedure.

(8) 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. In general, an acceptable BYOD would be one of the devices listed in the document referenced in the definition at Clause 3 of this procedure.
b. Minimum requirements – The burden of proof for meeting minimum requirement rests with you, the device owner.
c. Matching our requirements and your needs – BYOD capabilities and device profiles must match University requirements as well as the scenarios where you need to use a device for work. For example, if you are usually a consumer of information when mobile, the profile of a tablet or smartphone would be a good match. If you are

a ‘creator’ of information, a laptop or desktop profile would be a better match.

d. Authority – You agree to provide limited authority over the device for the sole purpose of protecting University data and access on the device. 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 information locally stored, the device and whether an MDM tool is used. The authority is to remain in place from the device is registered until it is de-registered.
e. Security – You are responsible for ensuring that your personal device is adequately secured against loss, theft or use by persons not authorised to use the device.
f. Support – You are responsible for replacing, maintaining and arranging technical support for your 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. Your access may be revoked at any time and for any reason.
h. Enforcement – All breaches of this procedure will be treated seriously. If you are found to have been in breach you may be subject to disciplinary action.

Requirements

Bring Your Own Device Minimum Requirements

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

Function	Minimum Requirement
Configuration Management	
Operating Systems	Your device must use a legitimate operating system that meets the defined minimum standards (i.e. you may not use a ‘jail broken’ device).
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	Your device will support password authentication and automatic locking that must be used at all times.
Automatic Device Lock	Your device must have the automatic lock enabled.
Device hygiene	Your device must have appropriate and up to date anti-virus and anti-spyware installed.
Lost and stolen devices	If your device is lost or stolen you must report the loss or theft immediately to the 17000 IT Service Desk.
Mobile device disposal	Any University data on your device must be removed from the device at the end of its use within the University environment.
Software licensing	Operating systems and applications running on or required by BYOD will be your sole responsibility as the device owner.
Security Management	
Mobile device management (MDM)	The University has the ability, through MDM capabilities of Office 365, 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	If your device is used for BYOD, and linked to the University's Office 365 platform, you agree to surrender limited authority over the device for the sole purpose of protecting University data and access on the device.
Mobile device application control	The University has implemented an MDM solution through Office 265, and has the ability to push and remove University data from your device to enhance its security or manageability.

Function	Minimum Requirement
Device Support	You and the device issuer are responsible for supporting your device.

Device Registration, Configuration and Management

(10) Your BYOD will be automatically registered within Office 365 upon first connection to the exchange mail service.

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

(12) You acknowledge that the University will directly and or remotely change security configurations of the device to protect University data and software stored on the device. These changes may include, but are not limited to:

a. 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 UON Network?".
b. Configuring certain security settings.
c. Preventing the user from changing certain security settings.
d. Applying a login code with an acceptable level of complexity to enable secure access to the device.
e. Automatically locking the device after an inactive timeout period (you will need to re-enter the login code).
f. Installing software and digital certificates necessary to maintain security.
g. Encrypting data stored on the device.
h. Automatically wiping (either all code and data OR all University code and data) depending upon University MDM, device capabilities and specific requirements from the device after a specific number of failed login attempts.
i. Should any configurations be removed that are required for proper use of the device with University systems, these may be re-applied or access to University systems, information and data will be prevented if the configurations cannot be maintained.

(13) You acknowledge that any University data stored on the BYOD remains the sole property of the University and that you have an obligations to protect the security of the data.

(14) You acknowledge that the University has a right to inspect University data held on your personal BYOD.

(15) You understand that the University may remotely monitor your device to ensure security and software configurations are maintained.

(16) You will not be prevented from installing the software or applications of your choice on your device. However, the University may block your access to University ICT services if any software / applications / data present a threat to University ICT services, information or data.

Device Usage and Support

(17) The service and its use are at your sole discretion and risk.

(18) The University does not impose a charge on you for registering your device.

(19) You are responsible for supporting your device. The University will only provide limited support for any applications the University has provided.

Support	BYOD
Physical provisioning	Device owner
Replacement of defective / damaged device	Device owner

Support	BYOD
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	17000 IT Service Desk
Device connectivity / access	**BYOD**
Mobile internet	Device owner
Home internet / broadband	Device owner
VPN client	17000 IT Service Desk
University wireless	17000 IT Service Desk

(20) The University is not responsible for any costs incurred by your use of your BYOD. The University will not reimburse any voice or data charges, software or application acquisition fees, and support or insurance costs associated with your device.

(21) The University is not responsible for any inconvenience that you may experience in connection with using University ICT services on your BYOD.

(22) You have sole responsibility for ensuring no other person has access to University software or data stored on your BYOD.

(23) The University will not monitor 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.

(24) The University will not monitor 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.

(25) The University may restrict access to internet websites, services or other elements for operational or policy reasons while your BYOD is connected to University networks including either wireless or cabled connections.

(26) The University may monitor your use of your BYOD while it is connected to the University network. This information may be collected and archived and may be subject to public access.

(27) You are responsible for abiding by all licence terms and conditions applicable to any software, apps, data or information provided by the University to your BYOD.

(28) You acknowledge that your use of a BYOD may involve the University:

a. Preventing you from accessing University ICT services
b. Locking your device
c. Wiping personal data from your device in accordance with the following circumstances:
    i. Your BYOD is reported as being lost/stolen to the 17000 IT Service Desk.
    ii. You cease employment / contract or studies with the University.
    iii. There is a suspected security breach, examples include but are not limited to modification of the device's operating system, breaching University policies, or detection of viruses or malware on the device.
    iv. The University may lock your device to prevent access to University information or data.
    v. Preventing your device from connecting to University ICT services.
    vi. Applying either a full or selective wipe of your BYOD.

vii. Applying a manual selective wipe of your BYOD.

(29) While the University will make all reasonable effort to ensure service is available, the University does not guarantee that access to University ICT services, information or data will be available at all times.

(30) 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. You must also:

a. undertake a device wipe as soon as practicable via the Office 365 portal or via a personal configuration / management utility.
b. take reasonable steps to ensure that it is replaced as quickly as possible.

Protection of University data on your BYOD

(31) University information, documents, and data classified as Highly-Restricted or that are subject to legal or professional privilege must not be stored on BYODs and/or unapproved cloud-based services.

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

(33) You should check your devise to ensure that automated cloud backup is disabled.

(34) 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.

(35) You are responsible for backing up and restoring the data and configuration settings of your BYOD. Personal data is not to be backed up or stored by the University. The University is not responsible for any personal loss or damage you may suffer by actions undertaken by the University to protect University data stored on your BYOD.

Device Deregistration

(36) The University at its own discretion, may de-register any BYOD at any time without warning.

(37) The University may de-register a BYOD that has not consumed University ICT services for more than 12 months.

(38) You can de-register your BYOD at any time by visting the Office 365 portal at http://outlook.office.com/owa/?path=/options/mobiledevice

(39) You will no longer be able to connect to University ICT systems and data, unless the device is re-registered.

(40) You are encouraged to remove any personal data if you are intending to dispose of your BYOD. If you intend to sell or gift the device to another person you should ensure that it is wiped.

Definitions in the Context of this Procedure

Defined Term	Meaning
Application	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.

Defined Term	Meaning
Device hygiene	BYOD must have appropriate and up-to-date 'hygiene' solutions installed. Device hygiene includes anti-virus, anti-spam and anti-spyware solutions.
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.
Mobility Framework	The NSW Government Mobility Solutions Framework. The Framework provides information and technical guidance to agencies when procuring mobility solution services.
Wipe	A security feature that rends the data stored on a device inaccessible. Wiping may be performed locally, via an MDM product, or remotely by a network administrator.

Related Documents

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

(42) You should also have regard to the statutory rules, policy documents and standards available in the associated information tab of this policy, or listed below. They provide direct or related guidance for the use of technology and the collection, storage, access, use and disclosure of data by the University and NSW public sector agencies:

a. AS/NZS ISO 31000 Risk Management – Principles and Guidelines.

Status and Details

Status	Historic
Effective Date	31st March 2017
Review Date	1st July 2018
Approval Authority	Chief Information Officer
Approval Date	29th May 2018
Expiry Date	16th June 2019
Responsible Executive	Morven Cameron 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.

"Term" - When referring to an academic period, term means a period of time aligned to an academic year for the delivery of a course in which students enrol and for which they are usually charged fees for example semesters, trimesters, summer, winter or full-year term. The academic year for a term is determined by the academic year in which the course commences, not concludes. For all other uses of this term, the generic definition applies.