Information Security BYOD Policy

Section 1 - Audience

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

Section 2 - Scope

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

Section 3 - Purpose

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

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

(5) The purpose of this Policy is to:

a. allow the use of BYOD's for study or work purposes, and access University systems and data when and where it is needed;
b. ensure that University systems and data are protected from unauthorised access, use or disclosure; and
c. set out the terms of use for BYOD's, the University's rights, and the responsibilities of the University and BYOD owners.

(6) This Policy has been informed by the NSW Government Mobility Solutions Framework and should be read in conjunction with the Digital Technology Conditions of Use Policy.

(7) BYOD owners should also have regard to statutory rules, policy documents and standards available in this document's associated information tab in the Policy library. 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 its staff.

Section 4 - Definitions

(8) In the context of this document the following definitions apply:

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.

Defined Term	Meaning
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.
Jail Broken Device	A device that has been tampered with to permit full access to the operating system, allowing the download of additional applications, extensions and themes that are unavailable through official means.
Minimum requirements	The minimum hardware, software and general operating requirements for a BYOD.
Mobile Device Management (MDM)	A solution which manages, supports, secures and monitors mobile devices.
Wipe / Wiping	A security feature that renders the data stored on a BYOD inaccessible. Wiping may be performed locally or remotely, via an MDM product, or by a system administrator.

Section 5 - Terms of BYOD Use

(9) This Policy must be reviewed before using a BYOD. Acceptance of the Digital Technology Conditions of Use Policy also constitutes acceptance of the terms of this Policy and indicates agreement to the standard terms of use outlined in this Section.

(10) Any BYOD must meet the minimum requirements set out in this Policy.

(11) The responsibility to meet the minimum requirements set out in this Policy rests with the BYOD owner.

(12) BYOD capabilities and 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.

(13) BYOD users agree to provide limited authority to the University to allow for the protection of University data on the BYOD. This authority remains in place from the time the device is registered until the time it is de-registered, and includes:

a. permission to wipe the BYOD in the event of loss or disposal. This may include the wiping of personal data, address books, and e-mail depending on the data classification of University information stored locally on the BYOD, and whether a MDM tool is used; and
b. permission to directly and/or remotely change the security configurations of a BYOD. These changes include, but are not limited to:
    i. refusing to register a BYOD that fails the BYOD minimum requirements set out in this Policy, 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 after a specific number of failed login attempts;

and

ix. should any configuration 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.

(14) Users are responsible for ensuring that personal devices are adequately secured against loss or theft.

(15) Users are responsible for replacing, maintaining and arranging technical support for their BYOD. The University will only provide best effort support for any applications that the University has provided, and for network connection troubleshooting.

(16) Access to University systems and data is provided at the sole discretion of the University and access may be revoked at any time and for any reason.

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

(18) 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.

(19) All University data must be removed from the BYOD at the end of its use within the University environment.

(20) Users are responsible for ensuring that appropriate licensing exists for operating systems and applications running on a BYOD.

(21) Users acknowledge and accept the University's rights, and all other provisions and requirements set out in this Policy.

Section 6 - The University's rights

(22) The University's rights are:

a. any University data stored on a BYOD remains the sole property of the University;
b. the University has a right to inspect University data held on BYOD;
c. the University may remotely monitor a BYOD to ensure security and software configurations are maintained;
d. the University may enforce policies on a BYOD to ensure the security of University data. This may include but is not limited to enforcing screen locks, pin codes and the ability to remotely wipe University data.
e. the University may push and remove data to and from a BYOD to enhance its security or manageability through the use of MDM;
f. the University may request an inspection of a BYOD in the owner's presence prior to them leaving the University to confirm there is no University data stored on the BYOD; and
g. the University has a right to enforce any provision or requirement of this Policy.

Section 7 - Requirements

Bring Your Own Device Minimum Requirements

(23) The University's minimum requirements for BYOD's are outlined in the following table:

Function	Minimum Requirement
Configuration Management	
Operating Systems	A 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	A BYOD must support password, PIN or biometric authentication.
Automated Cloud Backup	Automated cloud back up must be able to be disabled.
Automatic Device Lock	A BYOD must have an automatic lock enabled.
Device hygiene	A BYOD must have appropriate and up to date anti-virus installed.

BYYOD Registration, Configuration and Management

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

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

(26) A limit may apply to the number of BYOD’s that can be registered for a single person.

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

Device Usage and Support

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

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

(30) The University will not impose a charge on BYOD owners for registering BYOD on the University network.

(31) BYOD owners are responsible for supporting their own devices. The University will only provide limited support for any applications the University has provided.

(32) The following table outlines responsibilities:

Support	Responsibility
Physical provisioning	BYOD owner
Replacement of defective / damaged BYOD	BYOD owner
Operating system support, including licensing	BYOD owner
Application support of BYOD, including licensing	BYOD owner
University provided / supported mobile applications	17000 IT Service Desk
University provided / supported thin-client applications such as Citrix	17000 IT Service Desk
Backing up and restoring data and configuration settings	BYOD owner
Device connectivity / access	**Responsibility**

Support	Responsibility
Mobile internet	BYOD owner
Home internet / broadband	BYOD owner
VPN client	17000 IT Service Desk
University wireless	17000 IT Service Desk

Minimum requirements	Responsibility
Meeting the minimum requirements outlined in this Policy	BYOD Owner

(33) The University is not responsible for:

a. any costs incurred through BYOD use. The University will not reimburse costs incurred by a BYOD owner or user in association with BYOD use, including but not limited to:
    i. voice or data charges;
    ii. software or application acquisition fees;
    iii. support or insurance costs.
b. any inconvenience that may be experienced in connection with using University ICT services on a BYOD.

(34) 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 a BYOD when not connected to University network(s), unless the web traffic is directed through the University's network infrastructure.

(35) The University may:

a. 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;
b. collect information while monitoring the use of a BYOD while it is connected to the University network. This information may be archived and subject to public access under the provisions of the Government Information (Public Access) Act 2009;
c. wipe 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 BYOD owner ceases employment, affiliation or studies with the University;
    iii. there is a suspected security breach for example but not limited to, modification of the BYOD's operating system, breaching University policies, or the detection of viruses or malware on the BYOD.
d. wipe personal data if it is stored with University data within University supplied applications in the circumstances listed in clause 35c.

Protection of University data on your BYOD

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

(37) The University may reset a password or access code, only in consultation with the BYOD owner.

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

(39) BYOD owners should check their BYOD to ensure that automated cloud backup is disabled to ensure that University data is not inadvertently leaked, compromised or mishandled.

(40) Users should take reasonable steps to reduce the risk of losing personal data. For example, storing personal data separately from University data through file partitions or using a separate memory card.

Device De-registration

(41) 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.

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

Status and Details

Status	Current
Effective Date	14th November 2022
Review Date	14th November 2025
Approval Authority	Chief Information Officer
Approval Date	4th October 2022
Expiry Date	Not Applicable
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.

"Policy library" - The repository of policy documents published on the University website.

"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.