BYOD and Mobile Device Policy

Table of Contents

1. Purpose, Scope and Responsibilities

1.1 Policy Purpose

Unitec provides and manages electronic systems and devices for staff to undertake work and study related tasks. Nevertheless Unitec recognises that due to the changing needs of staff to be able to work and access Unitec systems anytime and anywhere Unitec is offering the option to all staff to Bring Your Own Device (BYOD). BYOD refers to the practice of staff and students bringing their own personal computing devices (laptops, tablets, smartphones) or other mobile devices with them to work or study.

The purpose of this policy is to provide a response to the changing requirements of our user community, such as:

- The rate of change in technology software and hardware generally exceeds the refresh rate of the Unitec's supplied equipment, resulting in staff having access to personal computer devices that are of higher specification that what is supplied.
- The technology support of the Living Curriculum and emerging pedagogical changes to include work integrated and online learning from locations outside Unitec campus.
- The demands of our staff for increased flexibility in accessing Unitec's information and electronics systems
- The improved productivity of staff on devices that they are familiar with as opposed to being limited to Unitec supplied and supported equipment only.

This policy specifies guidelines on how the use of personal devices can be used while protecting and maintaining the integrity of Unitec's responsibility by;

- Providing guidelines on the efficient, economical and ethical use of personal devices mobile services to access Unitec systems and information.
- Providing compliance with legislation and Unitec policies in the management and use of organisation and private information on mobile devices.
- Providing standards on the most cost efficient use of the BYOD and Mobile services that Unitec provides for staff, students and guests.
- Providing direction in relation to the allocation, access to, management and use of personal computing and mobile devices within Unitec.
- Provide the Unitec authority to address and mitigate the risks associated with the use of Unitec information, networks and systems on a personal device, such as:
    - **Device loss**. Devices used to store, transfer or transport information could be lost or stolen.
    - **Data loss**. Unitec and/or private information is compromised due to a lost, stolen or breached device.
    - **Malware**. Viruses, Trojans, worms, spyware and other threats can be introduced via a mobile device.
    - **Compliance**. Exposure or loss of information (Unitec and/or private) can result in a breach of legislation or Unitec policy.
    - **Cost control**. Inappropriate use resulting in significant cost liability to Unitec.

1.1.1 Mobile Service Guidelines

The Mobile Service Guidelines are located on the intranet (The Nest/Ask IMS) and define:

- The list of standard Unitec provided mobile services.
- The eligibility criteria, based on the business needs of different roles across Unitec.
- The appropriate level of access to information, networks and systems.
- The required security controls needed and the administration rights as part of your access to Unitec networks and systems (reference clause 4.1 and 4.2).

1.2 Policy Application and Scope

This policy applies to:

- All employees, full, part time or casual, consultants, contractors, volunteers and other agents working for or on behalf of Unitec (collectively referred to as "staff" in this policy).
- Unitec students are not covered under this policy as the provision for BYOD for students is already covered under the Electronic Devices and Systems Policy in addition to the student documentation for Unitec programmes.
- All mobile devices (Collectively referred to in this policy as "Any Mobile Device") that are used to gain access to Unitec information, networks and systems, whether:
  - Unitec provided.
  - Personally owned and used for business purposes under the BYOD programme.
  - Provided by other parties such as external consultants, contracting firms and outsourced providers, etc.).

1.3 Responsibilities

Role	Responsibilities
IMS	• Procuring and managing the services, infrastructure, hardware and applications to cater for Unitec's telecommunication needs and providing secure access to Unitec information, networks and systems at its sole discretion. • Defining the 'approved' list of mobile devices and plans that may be used to access Unitec information, networks and systems. • Defining Unitec's IMS Security Policy and Guidelines. • Provide controlled access to Unitec mobile services.
Managers	• Ensuring telecommunications and mobility needs of staff are met as directed by Unitec's policies and guidelines. • Managing the associated process and costs related to their staff as per Unitec's policies and guidelines.

	• Ensuring devices are returned to IMS when staff leave Unitec or no longer require the device.
Authorised budget approvers	• Authorising the allocation of Unitec mobile services as prescribed by the Mobile Service Guidelines.
Mobile device users	• Abiding by Unitec's policies, code of conduct and relevant legislation. • Ensuring Unitec information, networks and systems are kept secure.

2. Policy Statement(s) and Strategy

2.1 Unitec's BYOD (Bring Your Own Device) programme

2.1.1 About the BYOD programme

- Unitec offers an optional programme where staff may choose to use an approved personally owned computing and mobile devices to securely access and manage Unitec information.
- The purpose of the BYOD programme is:
  - To provide flexibility for staff who are eligible for a Unitec provided mobile service to use or upgrade to a different device of their choice.
  - To allow staff who are not eligible for a Unitec provided mobile service to securely access Unitec resources on their personally owned mobile device and plan.
  - To support productivity by allowing staff to use devices they are proficient with and which are configured for their personal use.
  - To reduce the cost of providing duplicate devices for business and personal usage.

2.1.2 BYOD Policy

- Staff who are eligible for a Unitec mobile service and choose to opt into the BYOD programme:
  - Must use a Unitec SIM card and plan with the Unitec preferred supplier with their personally owned device.
  - Are responsible for all initial and on-going costs, insurance, maintenance and support of hardware, operating software upgrades, non-business related software upgrades, repairs, retrieval of data or replacement associated with the use of their personally owned mobile device.
  - Please note that IMS teams will provide troubleshooting guidance for BYOD devices only, but will not support non Unitec devices.
- Staff who are not eligible for an Unitec provided mobile service:
  - Are responsible for all initial and on-going costs, insurance, support, repairs or replacement associated with the use of their personally owned mobile device and plan.
- The Mobile Service Guidelines will define:
  - The list of devices that are approved for use within the Unitec BYOD programme,
  - The appropriate level of access provided to Unitec information, networks and systems.
- If required, personal mobile numbers may be transferred into Unitec when staff begin and where possible, transferred back to the individual when they leave.
- Where a number belongs to a role, it may not be possible for staff to take the number with them when they leave.
- A manager is informed of what is permitted to be authorized for access to BYOD under the policy guidelines.
- Any charges payable as a result of a mobile number transfer will be borne by the user.

2.2 Usage

2.2.1 General Use

- Staff are required to read and adhere to all relevant Unitec policies and guidelines and sign the acceptance form before they use any mobile device for business purposes.
- Regardless of whether a Unitec provided or a personally owned device is being used, staff must ensure they are contactable as required by their roles.
- It is not acceptable to call staff outside their hours of employment unless there is a business emergency or the staff member is on call.
- Staff are expected to take all reasonable care of any Unitec provided mobile device and related accessories, noting they may be held accountable for any damage or loss.
- Staff agree to return any mobile hardware, accessories and software to Unitec at the end of employment or as instructed by their manager. If a staff member is leaving Unitec employment they have the option, with the agreement of their Manager, to purchase any mobile phone hardware used by them at the current retail cost less depreciation.
- Unitec provisioned and owned laptops and tablet computers cannot be authorised for sale to staff.

2.2.2 Prohibited use

- Unitec expects that any mobile device that is used to conduct business will be utilised appropriately, responsibly and ethically at all times.
- In addition to provisions in the Code of Conduct, Electronic Devices & Systems Policy and other relevant Unitec policies, the following are a list of actions & services (but not limited to) that are explicitly prohibited on any device used for business purposes:
    - Inappropriate, unsecured or unapproved consumption, storage or transmission of Unitec or private information.
    - Any premium rate services (such as 0900, text voting).
    - Gambling or gambling applications.
    - Consumption, storage or distribution of offensive, pornographic, racist and sexist content.
    - Consumption, storage or distribution of content or software which breaches the Copyright Act (e.g. pirated music, movies or software).

2.2.3 Usage overseas

- The use of any mobile device for ‘roaming’ while overseas is expensive, and as such for extended trips, Unitec recommends the use of a local pre-paid SIM card and secure Wi-Fi (such as in hotels etc.).
- Unintended ‘roaming’ while overseas can incur significant costs. Staff will be held accountable for any unapproved or excessive roaming charges.
- Where available, staff should make use of Eduroam wireless networks at participating tertiary institutions.
- If roaming services are required for business purposes, prior approval is required from a manager.

2.2.4 Mobile usage while driving

- It is an illegal to drive while using a hand held mobile device in New Zealand and in many other countries.
- Unitec's position is that no staff member is to use any mobile device while driving. Unitec accepts no responsibility for any incident, violation and/or legal action arising from illegal use of any device whilst driving.

2.3 Spend

2.3.1 Business and personal usage

- Unitec has a preferred mobile provider and plans. All staff eligible for Unitec subsidy for BYOD must use the preferred mobile provider.
- Unitec mobile plans are chosen and provided to meet the business requirements of staff roles at a cost effective rate.
- Unitec expects that the provided mobile plans contain sufficient inclusions (calling, messaging and data) for business usage as well as some personal usage.
- As such any usage above the standard Unitec plan may be considered personal usage and will be liable for reimbursement to Unitec.
- IMS will provide monthly reporting to cost centre managers on the following –
    - Pricing plans.
    - Cost of usage (phone and data).
    - Cost of roaming charges.

2.4 Security

2.4.1 Devices and content

- Only approved users with compatible devices will be authorised to access Unitec information, networks and systems. Details of the compatible devices can be found on the AskIMS intranet site.
- Staff are expected to secure and take all reasonable precautions to protect any mobile devices, access and content used for business purposes.
- Security and management tools may be used from time to time as part of Unitec's IMS environment to manage mobile device access to Unitec information, networks and systems.
- A passcode (PIN/password) is mandatory on any mobile device that is used for business purposes. Passwords or PIN numbers must be kept confidential and not disclosed to any other unauthorized person.
- Unitec will ensure that all business information and systems are backed up. However it is the personal responsibility of each staff member to regularly backup their own personal information, media, applications or settings. Unitec will not be held accountable for the loss of any personal content for any reason.

2.4.2 Unitec information, networks and systems

- Access to Unitec information, networks and systems on mobile devices is provided at Unitec's sole discretion. Unitec has the right to restrict, prevent or remove this access at any time.
- Staff must ensure that information (Unitec or private) is not stored or used on any device unless authorised access or applications are used. The use of device storage (device hard drive or removable storage) or cloud based consumer storage applications (such as Dropbox) to store information is unsafe and could lead to a breach of privacy or other legislation.
- Staff understand and accept that Unitec has the right to perform a "wipe" of all Unitec information from any mobile device at any time as part of the conditions of accessing Unitec systems, network and applications.
- Any attempt to contravene or bypass security settings or requirements on any mobile device used for business purposes is regarded as a security violation and thus a breach of the Unitec Code of Conduct.
- Any device that affects the performance of the Unitec network, Unitec business/reputation will have access blocked.

2.4.3 Lost, stolen or breached devices

- Due to the risk of a security breach, staff are expected to inform the Unitec ask IMS Service Desk and their own manager as soon as possible, but within 24 hours, if a device is lost, stolen or otherwise compromised in any way. Once advice is received the following guidelines will be enacted to help prevent a security breach:
  - If capability is available the device will be locked remotely and geo-located.
  - A remote "wipe" will be employed (removing all Unitec information and access).
  - The mobile plan will be blocked and the device blacklisted (where applicable).
  - If the device is stolen, the staff member is expected to file a police report within 24 hours.
  - If not located within 24 hours the staff member will be asked for permission to complete a Full Device Wipe. This will help protect Unitec information and any personal data still on the device.

2.4.4 Software and applications

- Unitec reserves the right to have visibility of all applications (but NOT the private content) installed on any mobile device used for business purposes.
- Unitec will provide and remove any software or applications (and related licensing) required for business purposes at its discretion.
- Staff are responsible for purchasing and paying for any other mobile applications or content they may choose to use.
- Unitec may maintain a list of "blacklisted" applications that are prohibited on any mobile device used for business purposes.
- Due to the risk of a security breach and consequent compromise of Unitec data, staff are prohibited from making unapproved modifications to the hardware or software (such as "Jailbreaking") of any device used for business purposes.

2.5 Support

2.5.1 Support for non Unitec devices

Unitec will provide the following support for personal mobile devices that are used for Unitec business;

- Access to Unitec Wi-Fi networks for staff with authorised network accounts.
- Network login account for secure access to Unitec electronic systems.
- Information on device compatibility criteria and connection support.
- Setting up mobile accounts with the Unitec mobile service provider for approved eligible staff.

Unitec will not provide hardware support for non Unitec owned mobile devices and cannot be held responsible for any damage to hardware occurring while being used for Unitec business.

Individuals are responsible for setting up and maintaining the required online app store accounts for downloading new applications to the device.

2.6 Legal and privacy

- In addition to all relevant Unitec policies, staff using mobile devices are to be aware of and comply with all relevant laws and regulations at all times.
- Any device used for business purposes (whether Unitec or personally owned), may be required in the event of a legal discovery process. If a mobile device contains information relevant to legal proceedings, the staff member is expected to make the device available upon such a request.
- Unitec will maintain its responsibility to respect and protect privacy of individuals at all times.
- With respect to the above, staff understand and accept:
    - Unitec ensures that any mobile device security initiative will not be used to deliberately access or capture/store personal content (such as text messages, personal email, photos).
    - Geo-location may be used to track Unitec devices only in the event that they are lost or stolen, or for other business specific purposes such as duress or security risk prevention initiatives. Staff will be advised in advance of such tracking in accordance with Unitec policy or legislation.
    - Unitec reserves the right to monitor any Unitec mobile service and any access to Unitec information, networks and systems. This is done to identify and optimise usage and/or spend, or to identify security threats.
    - Where applicable, Unitec reserves the right to provide or restrict access to Unitec information, networks or systems based on mobile device location services.
    - At any time Unitec may need to inspect any mobile device used for business purposes for the purpose of ensuring security compliance.

3. Breaches of policy

- If there are reasonable grounds to suspect that a person has breached this policy, an investigation will be carried out under the Disciplinary Policy (for staff), any other Unitec policy that may be in force from time to time, or as provided for under any other contractual arrangements that may be applicable.
- Subject to the outcome of any investigation, such action as is permitted under the Disciplinary Policy (for staff), and any other Unitec policy that may be in force from time to time, or contractual arrangements, may be taken.
- Whether or not disciplinary action is taken, a student who is found after appropriate inquiry to have misused Unitec's email and/or internet facilities may have their access to such facilities withdrawn for a period to be decided by the relevant Head of Department/Manager and the IMS Operations General Manager.
- Unitec reserves the right to suspend the access of any user to the email and/or internet facilities where it is believed on reasonable grounds that that user is breaching or has breached this policy. Such suspension may continue until such time as the matter has been dealt with to the satisfaction of Unitec, and will be managed in accordance with the provisions of the Disciplinary Policy (for staff).
- Where, following completion of an investigation, Unitec reasonably concludes that a user has breached the requirements of this policy, Unitec may terminate that user's access to Unitec's system/network.
- Where there is reasonable cause to believe that any New Zealand law has been contravened, law enforcement agencies may be advised.

4. Appendices

4.1 Definitions

Term	Definition
App Store	An app store (or app marketplace) is a platform for mobile apps in which users are able to purchase and download applications to run on specific devices, and are written for a specific operating system (such as iOS, Windows, or Android).
BYOD	Bring Your Own (personally owned) Device.
Eduroam	Education roaming. An international roaming service for users in research, higher education and further education. It provides researchers, teachers and students easy and secure network access when visiting an institution other than their own.
Jailbreaking	Process of removing operating system limitations on Apple devices such as iPhones, iPods and iPads.
Malware	Malicious software. Software which is specifically designed to disrupt or damage a computer system.
Mobile devices	Mobile phones, smart phones, portable electronic devices, portable digital assistants, tablets, mobile data cards and other portable internet connected devices. Excludes: laptop[s and other portable computers with non-mobile operating systems.
Mobile plans	Mobile SIM card and associated plan from a telecommunications provider.
Mobile services	Mobile devices, mobile plans and any related mobile telecommunications services.
Personal Devices	Includes personal owned Laptops, tablet computers and mobiles phones that are able to connect to internet and wireless networks

5. Reference Documents

5.1 Compliance with legislation

- Privacy Act 1993
- Public Records Act 2005
- Electronic Transactions Act 2002Privacy Act 1993
- Public Records Act 2005
- Electronic Transactions Act 2002

5.2 Compliance with international agreements

5.3 Compliance with government policies and guidelines

This policy takes into account the following government policies and guidelines:

5.4 Compliance with Unitec policies

- Electronic Devices & Systems Policy
- Unitec Code of Conduct
- Records Management Policy
- Privacy Policy
- Intellectual Property Policy Devices & Systems Policy
- Unitec Code of Conduct
- Records Management Policy
- Privacy Policy
- Intellectual Property Policy

6. Document Management and Control Details

6.1 Document Details

Version: 1.0	1.0	**Issue Date this Version: 13/01/15**	
This Version Approved by:	Leadership Team	**Date of Approval:**	March 2015
Document Owner: Owen Werner	IMS Operations General Manager	**Document Sponsor: Meredith Morgan**	Executive Director Organisational Development
Date of Next Review:	March 2017		
Date first version issued:		**Original Approval Body:**	

6.2 Amendment History

Version	Issue Date	Reason for Revision	Approved by
0.1	13/01/15	Draft document submitted for approval	