Electronic Devices and Systems Policy

Table of Contents

1. Purpose, Scope and Responsibilities

1.1 Policy Purpose

Unitec provides and manages electronic systems and devices for staff and students to undertake work and study related tasks. This policy ensures that Unitec operates a secure, minimal risk information technology environment, while enabling all authorised users' access to those approved electronic devices and systems.

The policy supports Unitec's strategic plan by:

- Achieving business and systems excellence.
- Supporting innovation in teaching and learning strategy.
- Enhancing the student experience.
- Meeting the needs of our communities (regional and national).
- Avoiding risks inherent in the use of electronic devices and systems, including:
  - Inappropriate or illegal use of information.
  - Loss of information.
  - Sharing of information with parties the author did not intend.
  - Risks associated with unauthorised access.
  - Exposure of the network to computer viruses & malware.

The purpose of providing staff and student's access to electronic devices and systems is to:

- Foster collaboration and communities of practice in teaching, learning and research - internally, nationally and internationally.
- Facilitate communication between Unitec campuses.
- Minimise the use of paper as a means of communication and engagement.
- Encourage collaboration.
- Provide a cost-effective and speedy means of communication for the Unitec community.
- Enable access to information and resources that staff and students need to complete their work or study.

1.2 Policy Application and Scope

- This policy applies to all users (including staff, students, contractors and guests) of all electronic Unitec devices and systems.
- Additionally, all users using non-Unitec electronic devices connecting to Unitec's wireless network are subject to this policy (*refer also to* Mobile Policy Device).

1.3 Responsibilities

Role	Responsibilities
IMS Operations General Manager	• Provide written approval for installation of software and games for educational use on Unitec electronic devices and systems • Authorises generic user accounts in consultation with the relevant Head of Department • Authorises in consultation with the relevant Head of Department automatic forwarding of emails addressed to a staff Unitec email address to a personal external email address when appropriate • Authorises extension of access to an account that is to be closed • Ensuring compliance with legislation.
IMS Services	• Manage all technical aspects of access to and control of Unitec's electronic devices and systems, including creating user accounts and back-up of user accounts • Coordinates and arranges relevant software licenses • Allocates email accounts • Registers internet domain names associated with Unitec • Closing, suspending and deleting of user accounts with appropriate authorisation
Unitec Users	• Abide by the provisions set out in this policy and any associated processes and guidelines • Use the devices and systems provided by Unitec in a professional and ethical manner while undertaking Unitec related activities. • Protect your account from unauthorised use by not sharing log in information with others

1.4 Compliance requirements

The use of all Unitec's electronic devices and systems must be in accordance with this policy, and any associated procedures/guidelines, to ensure the rights (in law) of all users, and reduce Unitec's exposure to risk.

2. Policy Statement(s) and Strategy

2.1 Allocating user accounts

Information Management Services shall be responsible for the allocation of all user and email accounts;

- All students shall receive a user account (with a unique account identifier) at the commencement of their course of studies.
- All other users shall receive a user account (with a unique account identifier) upon the request and authorisation of their manager.
- Only authorised users may use and /or access Unitec's electronic devices and systems.
- All users receiving a user account must keep their password confidential. Under no circumstances whatsoever may they disclose this password to another staff member, student or other individual or body.
- The creation of Generic User Accounts (e.g. 'facultytemp' as opposed 'jsmith') must be authorised by the IMS Operations General Manager and the relevant Head of Department.
- Email addresses shall follow a standard Unitec convention defined by Information Management Services and approved by the Chief Executive.
- Information Management Services will be responsible for the registration of any internet domain names associated with Unitec.
- Emails addressed to a staff Unitec email address are not to be automatically forwarded to a personal external email account without the direct authorisation of the IMS Operations General Manager and the Head of Department concerned.

2.2 Monitoring and auditing use

All information managed over Unitec's electronic devices and systems is subject to scrutiny and management by Unitec. Unitec reserves the right, in its absolute discretion to:

- Manage, analyse, limit or bar any information using Unitec's electronic devices and systems, where this information breaches policy or law.
- Block any data flow that may cause, performance or security issues or any other adverse risks to Unitec's electronic devices or systems.
- Monitor the use of Unitec electronic devices and systems and the information held within Unitec user accounts for the following purposes:
    - To investigate activities where the Chief Executive, or his or her delegate, has authorised an investigation into a breach of any Unitec policy, statute or NZ law.

  - To audit this or other Unitec policies or statutes.
  - To ensure the security of Unitec's electronic devices and systems and protect them from risk.
  - To meet operational maintenance requirements e.g. problem resolution, system management, capacity planning, mail delivery breakdowns.
  - Manage the costs associated with use of email and internet access.
  - Restrict user access to the internet and to websites on the basis of content.
  - To limit hours of internet connection time, the use of internet bandwidth and the quantity of data able to be transferred by applying volume-based and/or throughput-based policies; and to introduce a charging system for the use of any Unitec electronic device or system.
- As part of a monitoring process, Unitec may review records of individual internet usage, including information about particular sites accessed by individuals.
- A Unitec manager may, and only with the written authorisation from their immediate manager and the Executive Director, Organisational Development or the IMS Operations General Manager, access the content of a user account to ensure that any urgent and essential business needs of Unitec are met.

2.3 Provision and use of electronic devices and systems

- Electronic devices and systems provided by Unitec are provided for: business purposes, and primarily to support its teaching, research, outreach and administrative services.
- Unitec retains ownership of Unitec provided electronic devices and systems (including all information sent, received or captured within such systems) at all times.
- Information Management Services shall manage all technical aspects of access to and control of Unitec's electronic devices and systems, including the creation of User Accounts, the back-up of user accounts as part of the regular information technology back-up management processes and the application of this policy to Unitec's electronic devices and systems.

2.4 Software, hardware, licenses

- Software, including games, shall only be installed onto Unitec's electronic devices and systems with the prior approval of the IMS Operations General Manager.
- All approved software installed must be a legal copy and must be for business and/or educational use only.
- All approved games installed must be used for educational purposes only.
- All software licenses must be coordinated and arranged through Information Management Services.

2.5 Closing user accounts

Access to a Unitec user account shall cease upon the occurrence of the first of the following events:

- When employment with Unitec ceases.
- Ninety days after a student's last Unitec class ends.
- At the conclusion of a contract.
- As and when the Chief Executive, or his or her delegate, otherwise approves the cessation of the account.
- The IMS Operations General Manager and the relevant Head of Department can, in exceptional circumstances, approve continued access to a user account beyond any event that would normally cease access.
- A Unitec staff member or contractor's immediate Unitec manager shall be responsible for ensuring that:
  - Information Management Services is notified of the request to cease access to the Unitec user account in question (use the Employee Clearance Form), and
  - Information held in the user's account is appropriately managed and stored, in line with any approved Unitec records classification scheme and all relevant retention and disposal requirements.
  - a request for an account to be suspended without deletion be submitted.
- Once a user's access to their Unitec user account has ceased, emails or other documents held in the user's account must not be forwarded by any person to a personal email address, unless approval from the IMS Operations General Manager and the users immediate manager (for staff) or the relevant Head of Department (for students) has been provided.
- User account data will be deleted (if appropriate) within a maximum of 2 months from the date of account closure.
- A user is responsible for transferring all personal emails or personal documents to their own personal electronic devices or systems, prior to the cessation of their Unitec user account.

2.6 Acceptable and unacceptable use of Unitec electronic devices and systems

- Use of Unitec's electronic devices and systems must fall within the boundaries of normal and appropriate practice and New Zealand law.
- Access to external chat rooms, blogs or other similar services is allowed as long as such use:
  - Furthers the quality of teaching, learning and research, and / or

- Enables the discovery of new ways of using resources to enhance teaching, learning and research and /or
- Promotes staff and student development.

2.6.1 Personal use

Reasonable and occasional use of Unitec's electronic devices and systems for personal use is acceptable in some circumstances. Such use must not:

- Interfere unduly with Unitec's information technology systems.
- Be for personal gain (except as permitted by any other Unitec policies).
- Conflict with the user's employment obligations.
- Promote business, political, religious or any personal views in a manner that appears to have the endorsement of Unitec.
- Burden Unitec with incremental costs.
- Conflict in any way with Unitec policies or be contrary to any applicable law.

2.6.2 Illegal Activity

Use of Unitec's electronic devices and systems *must* not be used in any illegal activity, including, but not limited to sending or receiving:

- Objectionable materials in terms of the Films, Video and Publications Classification Act 1993.
- Defamatory or illegal material.
- unauthorised confidential or commercially sensitive material.
- Offensive, harassing or discriminatory material under the meaning of the Human Rights Act 1993 or the Harassment Act 1997;
- Material that breaches others' right to privacy and confidentiality. Personal information in emails must be treated in accordance with the Privacy Act 1993 and Unitec's Privacy of Information Policy;
- Material that can be considered harmful to Unitec or members of the Unitec community;
- Material that create or distributes unsolicited emails (Spam) that are sent to students; people external to Unitec or external organisations that contravenes the *Unsolicited Electronic Messages Act, 2007* or subsequent legislation

2.6.3 Unacceptable User Conduct

Use of Unitec's electronic devices and systems *must* not be used to:

- Attempt to subvert or actually subvert network security.
- Intentionally introduce, distribute, propagate or create viruses.
- Take part in any activity involving plagiarism or cheating.
- Take part in any commercial or personal profit activities without direct authorisation by the appropriate Head of Department or other manager.

- Directly or indirectly, compromise Unitec's information technology service.
- Misrepresent personal views as being the views of Unitec.
- Cause costs to be incurred by any person or organisation (including Unitec) without the consent of that person or organization.
- Gamble online.
- Access pornography, sexist, racist or offensive content.

Additionally users *must* not:

- Intentionally damage Unitec equipment
- Without authority, read, delete, copy, modify or send an email from within another users' email account
- With dishonest intent, modify any email with a view to disguising its origin, including date and authorship, or the original message;

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 either:
  - The Student Disciplinary Statute (for students), or
  - The Disciplinary Policy (for staff), and
  - 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), Student Disciplinary Statute (for students), 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), and the Student Disciplinary Statute (for students).
- 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 means...
Users	Students, staff, contractors, sub-contractors of Unitec or any other person authorised to use Unitec's electronic devices and systems.
Electronic devices and systems	Email, internet, mobile devices and any other information technology software or hardware controlled or owned by Unitec, including Unitec's networks and the services provided via these facilities.
Private devices	Mobile devices and any other information technology software or hardware, owned by students and authorised by Unitec through Information Management Services (IMS) to use Unitec's electronic devices and systems.
Email	Transmission of messages over communications networks, including internal and external emails. For the purposes of this policy, the word 'email' includes 'text messaging' and any other electronic message.
Internet	Global network connecting computers for the exchange of data, information, news and opinions.
Reasonable use	Use that does not impact negatively on: • Ability of the staff member to fulfil their employment duties; or • Ability of the student to carry out their work and/or studies effectively and efficiently; or • Other users.
User account	Security software enabling users to access Unitec's electronic devices and systems. This software provides users with unique (and in certain limited instances, generic (i.e. group- based) identifiers. **Note:** Different access rights are accorded the User Account, depending on the role of the user.

5. Reference Documents

5.1 Compliance with legislation

The Electronic Devices and Systems Policy adheres to the following legislation:

- Public Records Act 2005
- Privacy Act 1993
- Official Information Act 1982

5.2 Compliance with international agreements

5.2.1 Compliance with government policies and guidelines

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

5.2.2 Compliance with Unitec corporate policies

Unitec's Electronic Devices and Systems policy, processes and activities will be conducted in accordance with Unitec's corporate policies as well as with standards of behavior specified and/or implied by Unitec's:

- Code of Conduct
- Guidelines for the Use of Email
- Mobile Devices Policy
- Intellectual Property Policy
- Records Management Policy
- Privacy of Information Policy & Procedures

6. Document Management and Control Details

6.1 Document Details

Version:	1.2	**Issue Date this Version:**	16 October 2014
This Version Approved by:	Leadership Team	**Date of Approval:**	15 October 2014
Policy Owner:	IMS Operations General Manager	**Policy Sponsor:**	Executive Director, Organisational Development
Date of Next Review:	15 October 2016		
Date first version issued:	6 May 2009	**Original Approval Body:**	Leadership Team

6.2 Amendment History

Version	Issue Date	Reason for Revision	Approved by
1.2	16 October 2014	Restructure, reformat and minor review of document content	General Manager, Information Management Services
1.1	17 August 2012	Changed policy owner to reflect change in position titles resulting from recent IT Restructure; changed reference to ITSC to IMS (new name for IT).	Leadership Team
1	6 May 2009	This policy supersedes the Communications Systems Policy Amendments (date and substance)	