INFORMATION TECHNOLOGY MANAGEMENT
Subsidiary Policy & Procedure:

TECHNOLOGY USE

Document Control			
Policy Manager:	Manager, Technology Services	**Date First Approved:**	August 2011
Policy Owner:	Executive Director, Information Technology	**Authorised by:**	Executive Director, Information Technology
Category:	Operational	**Date Last Revised:**	October 2019
High-Level Policy:	Information Technology Management	**Next Review Date:**	September 2022
Relates to NZQA Tertiary Evaluation Indicator(s):		4. Governance & Management 5. Compliance	

1. Purpose & Scope

Wintec provides Information and Communication Technology (ICT) resources to a large and varied group of people, collectively referred to as ICT Users.

Through technology we enable our staff and students greater access to local, national and international sources of information. Staff are able to establish and maintain communication with the wider community and other stakeholders. Faculty and students can facilitate open information sharing and knowledge-building, and enhance their right to academic freedom.

This subsidiary policy applies to all staff, students, contractors, and stakeholders who use or have access to Wintec IT resources. ICT Users must comply with relevant laws, statutes, policies and procedures at all times.

2. Policy Statement

This subsidiary policy defines the responsibilities of all ICT Users, as well as the safeguards in place to protect our ICT resources from unnecessary risks. It promotes the responsible and ethical use of ICT facilities provided by Wintec. It does not conflict with our obligations and commitment to academic freedom, as laid down in s. 161 of the Education Act 1989.

Our environment is one in which students and staff are able to create and collaborate at any of our campuses, and with staff at other institutions, businesses and community groups, without fear that their work will be tampered with, destroyed, stolen or misrepresented.

All ICT Users are required to be aware of and adhere fully to this subsidiary policy.

Towards this end, we:

2.1. Take all reasonable steps to protect stakeholders to the best of our ability

We limit access to systems for staff, students, contractors, consultants, auditors and other third parties to those resources required to perform their role, through the use of secure passwords. Wintec's Information Technology Services (ITS) team work effectively and consistently to manage the prevention and treatment of ICT issues, and ensure the integrity of ICT resources.

2.2. Promote and educate stakeholders on safe ICT use

We actively encourage all ICT Users to be responsible computer and internet users, and provide users with information (and in some instances training) around safe and effective ICT use.

2.3. Recognise safe ICT use as a shared responsibility

All ICT Users must take the appropriate steps to protect their own data and connection to Wintec's network and ensure compliance with this subsidiary policy. In particular, all users must read and agree to the terms and conditions of the Technology Use Subsidiary Policy, prior to being granted access to ICT resources. All users have a responsibility to report suspicious behaviour with regards to ICT use.

2.4. Respect the rights of others with regards to ICT-related privacy and property

All ICT Users respect the rights and privacy of other users. Under no circumstances are ICT Users to harass others, misrepresent themselves or Wintec; access, copy or store inappropriate or objectionable material using ICT resources.

2.5. Take seriously our legal and ethical obligations concerning ICT

No staff, students, contractors, consultants, auditors or other third parties are to engage in any activity that is illegal under New Zealand or International law, nor act in any way that could bring Wintec into disrepute. Wintec ICT systems may be monitored, without notice to ICT Users, to ensure compliance with our policies and relevant legislation. Where violations occur, disciplinary action may be taken in accordance with Wintec's disciplinary procedures. All potential criminal activity in relation to ICT use will be reported to the police.

3. Key Roles & Expectations

This subsidiary policy is managed by the Technology Services Manager, and owned by the Executive Director, Information Technology Services (ITS). While ITS maintain additional guidelines and standards, all stakeholders have an obligation to maintain safe and secure ICT resources for the benefit of all users.

The following roles have key responsibilities:

ICT User

- collectively refers to any staff member, student, contractor, visitor or other user of any Wintec ICT resource.

Students

- read and agree to the terms and conditions of this subsidiary policy
- take all reasonable steps to ensure compliance with this subsidiary policy
- report any suspicious, suspected or actual breaches of this policy to Wintec Security.

All Staff

- read and agree to the terms and conditions of this subsidiary policy. Individual Contractors must complete a "Use of Technology/Photo Consent" form – this is to be completed before a Wintec account will be provided.
- only access ICT systems for which they have been granted the appropriate security clearance, and then only for their intended purpose
- take all reasonable steps to ensure compliance with this subsidiary policy
- report any suspicious, suspected or actual breaches of this policy to their manager, ITS or in the case of physical damage to ICT assets, Wintec Security.

TECHNOLOGY USE

People & Culture	• ensure that all staff have received, understood and agree to abide by the Technology Use Policy and accept it fully, regardless of whether they are permanent, contract or casual staff.
Centre Directors/ Head of School/ Business Managers	• approve additional access to systems and/or services where appropriate • ensure any contract or casual staff that are hired by Wintec have received, understood and agree to abide by the Technology Use Policy and accept it fully.
Network and Systems Administrators	• ensure access to systems is granted only when Managers verify that the relevant Individual Employment Agreement (Acceptance of Offer) or the Master (or Independent) Contractor Agreement has been signed • operate, monitor, maintain and secure ICT resources • treat the contents of all electronic files as private and confidential.
Copyright Officer	• creates awareness of and monitors compliance with the Copyright Act 1994 and subsequent amendments including the Copyright (Infringing File Sharing) Amendment Act 2011, in conjunction with the Executive Director, IT.
Privacy Officer	• creates awareness of and monitors compliance with New Zealand's current privacy law, specifically the Privacy Act 1993, and is aware of the potential implications of the Privacy Bill (proposed law), currently before parliament.
Manager, Technology Services (Policy Manager)	• responsible for the day-to-day management and implementation of this policy • organises the inspection and monitoring of data stored in any ICT resource (including staff and student workstations) when evidence suggests the ICT User may be in breach of this or other relevant policies • reports any potential, suspected or actual ICT related breaches in privacy or copyright to the Executive Director, ITS • promotes awareness of this policy and best practice amongst Wintec staff and students.
Executive Director, ITS (Policy Owner)	• Ensures adequate security is operating/in place to protect Wintec's ICT resources • monitors ICT resource compliance with relevant legislation. For more information, see *9. Related Legislation, Regulations, Policies, Guidelines and Forms* • informs the Chief Executive and Executive Director, Communications, of any potential, suspected or actual ICT related breaches in privacy or copyright • creates and maintains awareness of this policy and related ICT technology use procedures • holds overall responsibility for the implementation of this policy.

4. Measuring Success

The measurements of successful implementation and management of this Information Technology Management policy are:

- All staff, students, contractors, consultants, auditors or other third parties have read and agreed to the terms and conditions of this subsidiary policy and that this is recorded
- All staff, students, contractors, consultants, auditors or other third parties only access ICT systems for which they have been granted the appropriate security clearance, and then only for their intended purpose
- All Incidents of suspicious, suspected or actual breaches of this policy are reported to Management and recorded
- Continue to monitor the use of our various ICT systems, platforms, devices and services to ensure compliance with our policies and applicable legislation.

5. Unacceptable Use of Technology

All ICT Users are expected to act responsibly, ethically and professionally with respect to the use of ICT resources (hardware, software and online services) and with due regard to the rights of others. It is the responsibility of all ICT Users to guard against any misuse that could cause disruption to Wintec's ICT resources. Unacceptable use of ICT resources includes, but is not limited to:

a. using any Wintec facility or ICT resource in a way that violates applicable laws, Wintec policies, agreements or licenses, including, but not limited to this subsidiary policy, the Films, Video and Publications Classification Act 1993, the Copyright Act 1994 (or Copyright (Infringing File Sharing) Amendment Act 2011), the Privacy Act 1993, and the Harmful Digital Communications Act 2015.

b. using ICT resources in a way that misrepresents the identity of any Wintec staff member or student, the institution itself, or any of its subsidiaries, including:

   i. assuming another person's identity or role in an attempt to mislead any other person, or to gain unauthorised access to any Wintec system or information
   ii. attempting to access, monitor or tamper with another ICT user's Wintec identity or files without the explicit agreement of the owner
   iii. reading another ICT User's emails without their permission, or the appropriate authority from ITS
   iv. knowingly allowing another person to use your log-in ID and password for your computer or account
   v. communicating on behalf of Wintec or any other organisation or business unit that the ICT User does not have the authority to represent
   vi. using any ICT resource that hinders Wintec's ability to meet its legal and ethical obligations.

c. knowingly interfering with the normal operations of Wintec's ICT resources (hardware, business systems, networks, etc.) both on and off campus, including:

   i. introducing a software programme, application or software code intended to damage Wintec's or any other ICT Users' technology
   ii. Intentionally using a large amount of resources, such as processing time, disk space, or network bandwidth, resulting in undue or excessive resource requirements being placed on any Wintec system or network, without prior written permission from ITS
   iii. utilising any loophole discovered in a computer's operating system or in any software or application to damage a Wintec system or network

iv. excessive use of Wintec technology in a manner which hinders or prevents Wintec from providing ICT resources to other users
v. accessing, using, destroying, altering, disfiguring, dismantling or removing any Wintec ICT resource without any lawful excuse or the appropriate authority from ITS
vi. knowingly using any Wintec system/information for a purpose other than what it was intended.

d. using any Wintec ICT resources or your Wintec identity to bully, harass or victimise any other person, including:

i. sending harassing, defamatory or potentially libellous emails
ii. accessing, copying/transferring, uploading or storing/archiving any inappropriate, offensive or objectionable material (for example, racist or sexually explicit content) using any Wintec ICT resource
iii. breaching the privacy of individuals without the appropriate authority or other lawful excuse.

e. copying of any licensed or copyrighted software not permitted by law or contract, including:

i. any third-party copyright or patent protections, authorisations or agreements

f. Using Wintec ICT resources for private gain or commercial purposes without prior arrangement.

5.1. Disciplinary action due to unacceptable use of technology

Staff, Student and Contractor use of computers and ICT technology will be monitored, and breaches of this subsidiary policy may result in disciplinary action being undertaken by Wintec, including but not limited to termination of an ICT User's account and access privileges, suspension from modules or their programme, or termination of employment, in accordance with our disciplinary policies and procedures.

Where such a violation is believed to have contravened the Crimes Act 1961 the Harmful Digital Communications Act 2015 or the Films, Videos, and Publications Classification Act 1993, the matter will be referred to the police.

ITS reserve the right to take immediate and appropriate action in the case of possible abuse of computing and other ICT resources. Where ITS takes such action, it is done with due regard for:

- the protection of Wintec's ICT resources and network
- our obligations under law as a public tertiary institution
- the reputational risk to Wintec
- the protection of ICT User's work
- Staff and student disciplinary policies and procedures.

For more information on our policies, refer to Section 9 of this policy: *Related Legislation, Regulations, Policies, Guidelines, and Forms*.

5.2. Monitoring of Wintec ICT Resources

All electronic communication made using any Wintec owned ICT resource or service, or used for the purposes of conducting Wintec activities are considered the property of Wintec. To avoid any doubt when using Wintec's ICT resources, there should be no expectation of complete privacy or confidentiality of any work or communication created in the course of working at Wintec.

The use of our various ICT systems, platforms, devices and services may be monitored, without notice to ICT Users, to ensure compliance with our policies and applicable legislation. We reserve the right to monitor telephone, internet and email use, as well as any other material stored on our computer systems from time to time and at our discretion, including but not limited to:

- checking compliance with all Wintec regulations and policies
- investigating, preventing and/or detecting criminal activities and unauthorised use or access
- investigating complaints
- checking for viruses, malware, or other threats to the performance and stability of any ICT resource
- investigating abnormal system behaviour
- resolving ICT User problems
- monitoring standards of service or training
- maintaining or carrying out Wintec business-as-usual activities.

6. Procedures

There are no set procedures or processes outside of ITS for staff or students in relation to this policy. For staff members, contractors and volunteers at Wintec who wish to raise concerns or make complaints in relation to this Information Technology Management Policy, refer to our Employee Complaint Management Policy.

For students of Wintec, who wish to raise concerns or make complaints in relation this Information Technology Management Policy, refer to our Student Voice Policy.

7. Processes

For relevant processes, please refer to the following policies:

- For issues related to the use of ICT to abuse or harass staff members or students, refer to our Anti-bullying & Harassment Policy
- Staff, contractors and volunteers: Employee Complaint Management Policy
- Students: Student Voice Policy
- See also our Protected Disclosure Policy (for staff)

TECHNOLOGY USE

8. Related Legislation, Regulations, Policies, Guidelines, and Forms

Legislation/Regulations	Policies	Guidelines/Forms
Films, Video and Publications Classification Act 1993 Copyright Act 1994 Copyright (Infringing File Sharing) Amendment Act 2011 Privacy Act 1993 Privacy Bill (for reference, proposed law only) Harmful Digital Communications Act 2015 Films, Videos, and Publications Classification Act 1993 Education Act 1989 (specifically s.161) Human Rights Act 1993 Crimes Act 1961 Employment Relations Act 2000 Public Records Act 2005	Information Technology Security policy Intellectual Property policy Copyright for Educational Purposes policy Contract Management policy Student Voice policy Staff Discipline policy Employee Complaint Management policy Anti-bullying and Harassment policy	Use of Technology/Photo Consent form
Copies of New Zealand Legislation can be found on the New Zealand Legislation Website. You can view Wintec's Policies and Procedures on the Policy Web. This is not an exhaustive list of policies, procedures and legislation.		

9. Key Definitions & Glossary

Academic Freedom	The freedom of academic staff and students, within the law, to question and test prevailing thought, wisdom, and to engage in research and new ideas, and to state controversial or unpopular opinions. For a full definition, see s. 161 of the Education Act 1989.
Harass	Means to disturb or upset in a repetitive way. It is intentional behaviour which is found to be threatening or disturbing. For a full definition, see s. 3 of the Harassment Act 1997 or refer to our policy on Anti-bullying and Harassment.
ICT	Information and Communication Technology.
ICT Resources	Refers to the range of devices, networking components, applications and systems that enable modern computing and/or allow us to interact and communicate with the digital world.
ICT Users	Includes all staff members (whether permanent, temporary or part-time), honorary staff, visiting academic staff, students (whether full or part-time), contractors, sub-contractors, consultants or official visitors or guests of Wintec.

ITS	Information Technology Services. Wintec's IT department.
Objectionable Material	Material is deemed to be objectionable if it describes, depicts, expresses or otherwise deals with matters such as sex, horror, crime, cruelty, racism or violence in such a manner that the availability of the publication is likely to be 'injurious to the public good', as per Part 1 of the Films, Videos, and Publications Classification Act 1993, and/or Part 7 of The Crimes Act 1961.
Stakeholders	Includes alumni, associates, business partners, community groups and other agencies Wintec interacts with.
TUP	Technology Use Policy (this subsidiary policy), and sometimes refers to a form (whether in paper or digital form) that all staff must sign, stating they accept the terms and conditions of technology use at Wintec.

10. Records Management

In with the Public Records Act 2005, Wintec is required to provide an Information and Records Management programme to ensure that authentic, reliable and usable records are created, captured and managed to a standard of best practice, and to meet business and legislative requirements. All records relevant to a specific policy need to be listed in every policy in the following format:

Record	Minimum retention period	Disposal Action	GDA Reference #
This policy document	7 years after date of last action	Destroy	5.1.2 Policies & Decisions (operational)
New Staff Account Request Form	2 years after date of last action	Destroy	15.1.1 Information Management and Systems Administration
Staff/Contractor Employment Contracts	7 years after date of last action	Destroy	10.3.2 Standard Employment Documentation

11. Version History

Version	Date Approved	Details
1	August 2011	First Published.
2	March 2014	Split into two separate parts – policy (part A) and procedure (part B).
3	October 2019	Name changed to Technology Use policy (from Computer Use) and new template used, combining parts A and B into one document. Removed TUP references, differentiated between individual contractors and those from contracted organisations, included links to new and update policies.