Principles and Procedures

Part B: Technology Use
Number: OP11-02

Policy Manager:	IT Director	**Date Approved:**	August 2011
Category:	Information Technology	**Date Last Revised:**	March 2014
Authorised by	Chief Executive	**Next Review Date:**	May 2017

1. Definitions

Technology	Includes computer hardware, audio/visual equipment, software, electronics, internet, telecom equipment, e-commerce and computer services.
System	Used to refer to the information and communication technology (ICT) that our organization uses to process (capture, transmit, store, retrieve, manipulate and display) information.
Software	Also known as computer programs, is the non-tangible component of computers. Computer software includes all computer programs that upon execution, instructs hardware to perform the tasks for which it is designed.
Objectionable material	Material is deemed to be objectionable if it describes, depicts, expresses, or otherwise deals with matters such as sex, horror, crime, cruelty, or violence in such a manner that the availability of the publication is likely to be injurious to the public good.
Harass	To disturb or upset, and it is characteristically repetitive. In the legal sense, it is intentional behaviour which is found threatening or disturbing.
Network	Allows computers to exchange data and share use of applications, storage, servers, printers, email and messaging applications.

2. Expectations

2.1. No staff, students, contractors, consultants, auditors, evaluators or temporaries affiliated with third parties (all users) of Wintec technology will engage in any activity that is illegal in New Zealand or international law.

2.2. Use of Wintec systems may be monitored, without notice to you, to ensure compliance with Wintec policies and applicable legislation. Wintec reserves the right to monitor telephone use, Internet use, access email and other material on its computer systems from time to time for various reasons, including but not limited to:

a) Checking compliance with all Wintec regulations and policies;
b) Preventing or detecting criminal activities;
c) Investigating or detecting unauthorised use;
d) Investigating complaints;
e) Checking for viruses or other threats to the performance of the system;
f) Investigating abnormal system behaviour;
g) Resolving a user problem;
h) Monitoring standards of service or training;
i) Maintaining or carrying out Wintec business.

2.3. All electronic communication made using Wintec services, or in the purposes of conducting Wintec activities are considered the property of Wintec. For the avoidance of doubt there should be no expectation of privacy or confidentiality within Wintec's electronic services.

2.4. Unacceptable use of technology (hardware, software and online services) includes but is not limited to:

a) Using an identity that is not your own or allowing anyone to use your identity for the purpose of gaining access to Wintec resources.

b) Attempting to gain unauthorised access to Wintec systems/information or intentionally using a system/information for a purpose for which it was not intended.

c) Knowingly interfering with the normal operations of Wintec technology systems (hardware, business systems, networks etc).

d) Knowingly introducing a software programme or software code intended to damage or place excessive load on Wintec technology systems.

e) Using Wintec resources or your Wintec identity to harass others.

f) Intentionally accessing or archiving objectionable material.

g) Commercial use of Wintec technology/resources for private gain. Refer to the Intellectual Property Policy EXG-1/00.

h) Attempting to access, monitor or tamper with another user's Wintec identity or files without the explicit agreement of the owner.

i) Excessive use of Wintec technology resources in a manner which may hinder or prevent Wintec from providing Wintec technology resources to others.

2.5. Before accessing the Wintec network, students must have read, understood and agreed to the terms and conditions of this policy (parts A and B) and the Copyright and Photocopying Policy.

2.6. When students first log on to a Wintec account after enrolment or first log on in a new calendar year, they must confirm that they accept the conditions of this policy (parts A and B) and the Copyright and Photocopying Policy.

2.7. By signing Employment Agreements, employees agree to follow all Wintec policies and procedures.

3. Roles and Responsibilities

IT Director	• Ensures adequate security to protect the Wintec's systems and technology; • Monitors compliance with the Copyright Act (1994) and amendments including the Copyright (Infringing File Sharing) Amendment Act (2011) in conjunction with the Copyright Policy owner; • Informs the Chief Executive and Director Communications of any potential copyright breaches; • Organises the inspection and monitoring of data stored on the

	network and staff or student workstations when evidence suggests breaches of this policy. Any inspection of electronic files, and any action based upon such inspection, will be governed by all applicable New Zealand legislation; and • Creates and maintains staff awareness of this policy.
Network and Systems Administrators	• Ensure access to systems is only granted once conditions are accepted by all new users; • Maintain, operate, monitor, access and secure computing resources, systems and technology; and • Treat the contents of electronic files as private and confidential.
Learning Hub Manager (Copyright Policy owner)	• Creates awareness around and monitors compliance with the Copyright Act (1994) and amendments including the Copyright (Infringing File Sharing) Amendment Act (2011) in conjunction with the IT Director.
Heads of School/Centre Directors and Managers	• Approve additional access to systems and/or or services where appropriate

4. Measurements of success

- There are no breaches of this policy and evidence of compliance can be demonstrated.
- Processes are in place to ensure all users are aware of Technology Use policy.

5. Records Management

In line with the Public Records Act 2005, Wintec is required to provide a 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 #
Employment Agreement/Contract	7 years after date of last action	Destroy	9.1.1