POLICY
ACCEPTABLE USE OF ICT RESOURCES
(03.006)

Order of Precedence:

1. *Kaupapa Here Mana Tāpae ā-Motu / National Delegations Policy*
2. *Education A Rēhita Mana Tāpae / Standing Delegations Register*
3. *Te Kawa Maiorooro / Education Regulatory Framework*
4. *Divisional Policies*

POLICY

Te Pūkenga / New Zealand Institute of Skills and Technology trading as NorthTec (hereafter NorthTec) Information and Communication Technology (ICT) resource users shall properly use and protect all ICT resources in accordance with the ICT User Requirements.

PURPOSE

To protect ICT resources and provide requirements for their use.

APPLICATION AND SCOPE

This policy applies to all NorthTec students, and visitors.

DEFINITIONS

- *User*
  A currently enrolled NorthTec student. Other individuals may also become users (with guest accounts) for NorthTec business purposes, examples include someone providing service to NorthTec and official visitors.
- *ICT Resources*
  Hardware and software including, but not limited to:
  - Data and communication network (LAN, WAN, Internet, and Wireless)
  - Computer and equipment (i.e. servers, computers, printers, multi-function devices, telephones, mobile devices)
  - Data storage media (i.e. backup tape, flash memory, removable hard disk) and data files
  - Business applications and software licences
- *Management of ICT Resources*
  Manager ICT and his / her Line Manager(s)

COMPLIANCE OBLIGATIONS

- *Auditor General*
- *Copyright (Infringing File Sharing) Amendment Act 2011*

Responsibility	Executive Manager with responsibility for ICT
Approval dates	January 2025
Next Review	December 2028

OTHER RELATED DOCUMENTS

Policy: *Computer, Email and Internet Policy – (ICT Resource Security Management (03.008))*

PROCEDURES AND GUIDELINES

1.0 Any non-compliance with this policy or the ICT User Requirements will be dealt with under the procedures contained in Student Disciplinary Regulations (students).

2.0 NorthTec management may authorise the inspection of user data or monitoring of messages (including email) and Internet access when there is reasonable cause to suspect improper use of computing or network resources.

3.0 Access to NorthTec ICT resources may be wholly or partially restricted without prior notice and without consent of the user if:

- Required by law or policy;
- A reasonable suspicion exists that there may have been a violation of law or policy; or
- Required to protect the integrity of NorthTec ICT systems or computing resources.

ICT USER REQUIREMENTS

Users must:

1.0 Respect all NorthTec technology policies and technology services operational procedures including, but not limited to:

- Copyright (Infringing File Sharing) Amendment Act 2011
- *ICT Resource Security Management (03.008)* and relevant procedures; and
- This policy – *Acceptable Use of ICT Resources (03.006).*

2.0 Respect copyrights and licenses to software and legally protected digital information.

2.1 All copyrighted resources (i.e. computer programmes, digital documents) retrieved from computer or network resources must be used in conformance with applicable copyright and other law.All digital information generated by users for the benefits of NorthTec is the property of NorthTec.

2.3 Users must not sell or distribute programs or documentation generated for the benefit of NorthTec to any other party without management approval.

3.0 Respect the integrity of information systems.

Users must <u>not</u>:

3.1 Modify or remove computer, network equipment, or peripherals that are owned by NorthTec from NorthTec premises without explicit permission, except mobile equipment (i.e. laptop, cell phone, camera, data projector) that are assigned for dedicated individual use;

3.2 Connect computer or network devices, to NorthTec computer network without appropriate authorisation from management and ICT services;

3.3 Attach additional network or communication devices (i.e. modems, routers, wireless cards) to personal computers without appropriate authorisation from management and ICT services;

3.4 Access or modify information systems or other information resources for which the user is not authorised;

3.5 Modify, install or upgrade operating systems, applications, or software utilities without appropriate authorisation from Management of ICT services;

3.6 Develop or use programs which disrupt other computer or network users or which access private or restricted information and/or damage software or hardware components of a system;

3.7 Use programs or utilities which interfere with other computer users or which modify normally protected or restricted portions of the system or user accounts; or

3.8 Use software (i.e. peer-to-peer applications) or utilities in a manner that overloads or impairs the network.

4.0 Respect the expense of computer-based resources.

Users must <u>not</u>:

4.1 Print excess copies of documents, files, data, or programmes;

4.2 Use internet bandwidth in an unnecessary manner (e.g. repeated downloads of the same large file, or unnecessary use of internet audio / video, e.g. streaming video or music for personal use); or

4.3 Misuse or mistreat computer hardware in a manner that is likely to cause damage.

5.0 Respect information security management procedures.

Users must <u>not</u>:

5.1 Access computers, computer software, computer data or information, or networks without proper authorisation, or intentionally enable others to do so.

5.2 Share their NorthTec accounts' passwords with others, or allow anyone else to use their accounts. Log-on passwords must be kept confidential. Chosen passwords must conform to the standards established from time to time by ICT Services.

5.3 Undertake any activity, or distribute any information which would compromise the security of NorthTec computer systems, network or data.

5.4 Browse through NorthTec computer systems or networks, or use hardware or software tools to evaluate or to compromise information system security.

5.5 Knowingly transmit viruses or attempt to eradicate viruses without ICT assistance.

Users must:

5.6 Keep their equipment physically secured against theft and damage.

5.7 Report any security alerts, incidents, threads, warnings or breaches to the ICT Services Desk or management.

5.8 Ensure that all sensitive, valuable or critical information is stored on the nominated networked servers (as these servers are backed up daily).

5.9 Exercise caution when handling/sending sensitive information or data.

6.0 Respect the rights of other computer users.

Users must <u>not</u>:

6.1 Access, download, request, transmit or retain material which is illegal, which infringes on the rights of others (e.g. privacy or copyright) or which a reasonable person may consider (by the subject or the intended recipient) to be abusive, discriminatory, defamatory or offensive. This includes, but is not limited to, offensive, fraudulent, harassing, obscene, threatening, racist, pornographic and sexist materials.

6.2 Download, request, transmit or retain material any material which is reasonably likely to be perceived by the intended recipient as harassment, intimidating or an unwarranted invasion of privacy.

6.3 Interfere with or disrupt the reasonable use of the network by any other person including introducing onto the system any material (such as viruses, peer-to-peer applications) that has the potential to destabilise NorthTec's systems.

6.4 Distribute electronic chain letters, hate mail, hoax virus mail or spam messages.

6.5 Send unauthorised emails from another user's email address or misrepresenting, obscuring, suppressing or replacing a user's identity on the Internet or any NorthTec electronic communication system.

6.6 Transmit personal messages with large attachments or broadcast personal emails.

7.0 Use NorthTec ICT resources for business and academic purpose.

Users must <u>not</u>:

7.1 Use NorthTec ICT resources for political or commercial activities, except as permitted under other written policies or with the written approval of management having the authority to give such approval. Personal use of NorthTec ICT resources must be kept to minimum, without negative impact on NorthTec business or academic activities.

7.2 Transmit commercial or personal advertisements, solicitations or promotions. Bulletin boards on the campus portal that have been designated for selling items by members of NorthTec community may be used according to the stated purpose.

7.3 Subscribe to non-business related Internet services where information is downloaded automatically from the Internet (as these services can waste resources).

7.4 Use NorthTec network for gambling.

7.5 Establish or modify Internet websites dealing with NorthTec business without authorisation from the Management of ICT services.

7.6 Use NorthTec network to post any broadcast messages or news group articles on the Internet referencing or commenting about NorthTec without the prior approval of the Regional Executive Director.

7.7 Use NorthTec network to pass off personal views as representing those of NorthTec.

8.0 Attain required computer system training and security awareness programmes.

REVISION HISTORY			
Version	Description of Change	Author	Effective date
1	New – replaced T08/01	QMS Team	January 2009
2	Review – management structure changes	QMS Team	January 2011
3	Review – slight change of title (replace Appropriate)	P Brimacombe	August 2015
4	Triennial review – no changes	S Milner	August 2017
4.1	Add 'Ltd' to Northland Polytechnic Council becomes Board of Directors	QMS Team	May 2020
5	Review – minor changes to wording institutional Titles and responsibilities	QMS Team	January 2025