Technology Use Procedures

Policy Document number: OP-11/02B

1. Pūtake | Purpose

1.1. These procedures operationalise and should be read in conjunction with the Technology Use Policy and Wintec Use of Artificial Intelligence Standard. The policy details the principles and policy statements underpinning these procedures, the audience and scope to whom the procedures apply, responsibilities and definitions applicable to these procedures, and links to other policies, documents, and relevant legislation.

2. Ngā Hātepe | Procedures

2.1. Photos and videos

ICT (Information and Communication Technology systems and tools) users may only take photos or videos in the workplace for lawful and work-related purposes. If an ICT user does wish to take photos or videos in the workplace for use on social media, they must get permission from any individuals captured in the photos or videos first. Refer to Wintec's Social Media Policy for acceptable use of social media.

2.2. Software

All software or services procured will undergo a security assessment before approval. No software can be purchased or installed without this assessment and approval from the Digital Technology Services unit (Digital). All software solutions must be requested through the technology requests assessment process.

2.3. Network Access & Internet

1. The right to access and use Wintec networks can be withdrawn at any point if deemed necessary by Digital to protect Wintec.
2. Accessing unauthorised, illicit, or objectional materials is strictly prohibited.
3. Network use is monitored.
4. Kaimahi: Network access and internet for Wintec managed devices is available at all Wintec sites. Access will be restricted to those devices in which kaimahi require access; where **Wintec Secure** is available, kaimahi should use this network.
5. Ākonga: Internet is provided for use on BYO devices; where **Wintec Secure** is available, ākonga should use this network.

2.4. Email

1. Kaimahi use Wintec work email account(s), they must comply with this Policy and:
   a. Only use email accounts they have permission to use.
   b. Forwarding or redirection rules to external mailboxes are not acceptable.
   c. Handle confidential information with care including personal information.
   d. Meet New Zealand's anti-spam rules in accordance with the Unsolicited Electronic Messages Act 2007 when sending emails to numerous addresses, for example, marketing messages to customer lists.
2. ICT users can use work email for work or personal use as long as it is at a reasonable level.

3. Ākonga email accounts are provided for the purpose of learning. They can also be used personally provided that the use complies with this policy.

2.5. **Files**

Under no circumstances will internal Wintec information or work product, excluding teaching files given to ākonga, be transmitted or downloaded and stored in systems not owned and managed by Wintec. For example, sending Wintec work to a personal email or private file storage, e.g., Google Drive, Dropbox, personal OneDrive etc. Refer to Wintec's Information and Records Management Policy for management of Wintec information.

2.6. **Security**

1. All ICT users must:
   a. Take all reasonable care to minimise the amount of Wintec data stored locally on their device, to protect that data in the event the device is lost or stolen. If an ICT user is accessing Wintec data resources from a personal or Bring Your Own Device (BYOD), they are required to work in online only mode or access via Shortcut to OneDrive and not download or store files locally (this includes syncing to your hard drive[1]).
   b. If ICT users are connecting BYOD or personal devices to corporate applications, they must consent to the policies and software controls of Wintec to protect our data and our customers data in order to access these apps. Failure to consent will mean these applications will be unavailable on their device.
   c. When ICT users cease employment, study, or contracted mahi at, with, or on behalf of Wintec, they must remove all Wintec data from their devices. ICT users must also remove any Wintec specific software (applications) that were required and/or licensed under Wintec. This includes any software applications such as Microsoft Office 365. Digital reserves the right to inspect ICT users' devices to ensure this is done. If ICT users need assistance with this, please contact the Digital Service Desk.
2. Kaimahi will not be granted administrative access to computer systems, unless required by work function and at the approval of Digital Management.
3. Only software and apps can be downloaded on Wintec devices as approved by Digital. Installation of unapproved applications is prohibited.
4. A mobile phone or computer hardware device can store a significant amount of corporate data, some of which could be of a sensitive nature. For security reasons, ICT users must always enable a device lock when they are not using the device. ICT users' personal devices are subject to this procedure if they contain Wintec contained data. i.e. OneDrive, Teams or Outlook etc.
5. All Wintec devices capable of encryption will have encryption configured to secure information at rest.
6. Digital will push patches and software updates to devices as part of our system maintenance. ICT users must restart their computer, tablet or mobile phone as requested by these automatic processes to ensure the patches apply in a timely manner.
7. Any errors reported by an ICT user's computer system must be logged with the Digital Service Desk.
8. ICT users must not install or attempt to circumvent any security controls in place or attempt to bypass restrictions.

2.7. **System Access**

[1] For the latest guidance see Digital Workplace page.

1. Only authorised ICT users are permitted to access and use Wintec private corporate systems. All individual accounts are unique and created, deleted, and managed by Digital under the direction of People and Culture or in line with the following criteria:
    a. Annual auditing of accounts to verify account status.
    b. Disablement of kaimahi accounts at termination date, unless requested sooner.
    c. Or when kaimahi accounts are to be retained as active, with approval from the Digital Director.
    d. Deletion of kaimahi accounts in alignment to the data retention schedule post People and Culture notified termination date.
    e. Ensuring that no account user IDs are to be used again unless for a returning kaimahi or ākonga.
2. Contractor accounts created and managed by Digital will all have account expiry set on creation. Only kaimahi responsible for the contractor can request enablement of disabled and expired accounts. Contractor accounts without activity for 45 days are disabled.
3. All contractor accounts will be for a specific person, no company shared accounts will be created.
4. Key systems will have an access review every 6 months. This includes the following systems:
    a. Learner Management systems.
    b. Health systems.
    c. Organisational Finance systems.
    d. Payroll systems.
    e. Physical access security systems.
5. Logins can be disabled for protection of the organisation at any time.
6. Accounts with no activity for 180 days will be disabled.

2.8. Privacy

1. ICT users of Wintec digital facilities have a right to a reasonable expectation of privacy; however, system failures or design faults may compromise this. ICT users should also recognise that authorised Wintec kaimahi may have access to personal data and software stored on digital facilities while performing routine operations or pursuing system problems.
2. As specified in the relevant administrative policies at Wintec, authorised Wintec personnel are obligated to take reasonable and appropriate steps to ensure the integrity of the digital facilities and to ensure the Technology Use Policy, Wintec Use of Artificial Intelligence Standard, and these procedures are complied with.

2.9. Password Standards

1. Access to Wintec systems and devices is controlled through individual accounts and passwords. ICT users must:
    a. Not reuse passwords on accounts either work or personal.
    b. Ensure all access codes, account numbers, passwords, or other authorisation that have been assigned to them are kept confidential and never shared with others.
    c. Not log on to a device with their authentication details for someone other than the ICT user to use. This specifically includes multiple logins of a kaimahi ID to facilitate ākonga access in a learning space as well as sharing user access with any other person.
    d. Not write passwords down. Digital Service Desk or our self-service password services can reset passwords if forgotten.

e. If they believe their account has been accessed by someone other than themselves, they will change the password immediately and contact the Digital Service Desk to report and for further remediation steps.

2.10. **Incident Response**

1. Wintec has an incident response program for efficient remediation of information security incidents. ICT users are expected to comply with the following requirements to ensure effective and efficient incident remediation:
   a. ICT users must report any suspected security incident to the Digital Service Desk immediately, including but not limited to lost/stolen equipment, suspected malware infection, compromised credentials, and any other possible compromises of Wintec systems and/or data.
   b. ICT users must cooperate with incident response processes, such as forfeiting their equipment to the Digital Service Desk for investigation if it is potentially compromised, or as requested by the incident response team.

2.11. **Security Awareness Training**

1. Human error and negligence are common sources of security issues. Wintec takes a proactive approach by requiring security awareness and training:
   a. During onboarding, ICT users will be required to undergo information security awareness and training. Upon completion, users will be required to sign a declaration that they have completed the training, understand the requirements and specific procedures taught, and intend to abide by the policies and procedures provided.
   b. ICT users must complete ongoing security awareness and training as scheduled. Through this, ICT users will be kept aware of how to keep themselves and the organisation safe and what to do if they encounter a security issue.
2. Digital will conduct phishing training exercises which will help make us all safer at home and at work. ICT users are expected to participate in these exercises which may result in further training requirements.

2.12. **Information Security**

Maintaining the confidentiality, integrity, and availability of organisational data is paramount to the security and success of the organisation. The following requirements are defined to keep data secure and handled appropriately.

2.13. **Information Access and Authority**

1. ICT users may have access to more information than generally needed for their roles. However, access to information does not create authority to use the information. Authority is implied when a business purpose requires use of the information. When no business process requires use of the information, authority to use is removed.
2. ICT users may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to Wintec or another individual without authorised permission of the information owner. Destruction of information must be in alignment with the Wintec Information and Records Management Policy.
3. ICT users will only access data provided to them for duties in connection with their employment or engagement and in accordance with their terms and conditions of employment or equivalent. Access to some applications and information sources will be routinely recorded and/or monitored for this purpose.

4. Extraction, manipulation, and reporting of Wintec data must be done for business purposes only.
5. Personal use of organisational data, including derived data, in any format and at any location, is prohibited and may result in disciplinary action.
6. ICT users will follow all Wintec sanctioned data removal procedures to permanently erase data from devices once its use is no longer required.
7. ICT users upon discovery they can access files or applications that are not required for their role, will contact the Digital Service Desk and advise immediately.

2.14. **Information Classification**

All organisational data is owned by Wintec and, as such, all ICT users are responsible for appropriately respecting and protecting all data assets. This includes but is not limited to calling out and stopping others from inappropriate use of Wintec organisational data. ICT users must keep all data secure by taking sensible precautions and following requirements defined in this policy.

2.15. **Artificial Intelligence**

1. For the purposes of this policy, the term 'Artificial intelligence' or 'AI' refers to all generative AI, AI, and machine learning, even if it is not derived from a large language model. Wintec has a Standard covering the use of AI (Wintec Use of Artificial Intelligence Standard) which should be consulted before knowingly entering any data into AI systems during the duties of work.
2. Acceptable use of AI - ICT users can generally use an AI tool provided that the use is not in breach of the Technology Use Policy or Wintec Use of Artificial Intelligence Standard and the following criteria:
    a. Ensure consultation with Digital Service Desk before using any AI service and take care when sharing personal data on these services.
    b. Examples of acceptable use are: Testing own ideas or thoughts, developing document headings and structure, developing text responses to refine thinking provided none of the information is confidential.
    c. AI in research and rangahau activity, including where Māori, Pacific, and/or indigenous knowledge is involved, is allowed provided the relevant Wintec units or subject matter experts have been consulted and given consent, and ethics approval has been sought and approved in accordance with Wintec's research and rangahau policies.
    d. Read and use AI services in alignment with the Wintec Use of Artificial Intelligence Standard.
3. Unacceptable use of AI - ICT users will:
    a. Not input any information classified as INTERNAL, SENSITIVE, or RESTRICTED, or any information without classification that would satisfy the requirements to be classified as INTERNAL, SENSITIVE, or RESTRICTED.[2]
    b. Not input any Wintec commercially owned[3] or culturally significant information such as intellectual property, mātauranga Māori, Pacific, indigenous, or sensitive data into AI systems unless explicit consent has been obtained from the appropriate data owners and the use complies with the Wintec Use of Artificial Intelligence Standard.
    c. Not allow ingestion of data from parties that have not directly agreed to the AI tool terms of service, e.g. group use where not all participants have agreed to the terms.

[2] Refer to the Sensitivity Labels page in the Digital Workplace as well as Wintec Information and Records Management Policy and Information Classification Standard for further guidance on sensitivity labels.
[3] Refers to the commercial arm of Wintec e.g., LearningWorks, Soda.

3. Ngā Haepapa | Responsibilities

3.1. Refer to the Technology Use Policy for information on responsibilities relating to these procedures.

4. Ngā Whakamāramatanga | Definitions

4.1. Refer to the Technology Use Policy for information on definitions relating to these procedures.

5. Mokamoka whakaaetanga | Approval details

Title	Technology Use Procedures
Policy Document Number	11-02/B
Governing Policy	Technology Use Policy 11-02/A
Category	Operational
Subcategory	OP: Information and Systems Management
Approval Date	December 2025
Effective Date	January 2026
Review Date	October 2027
Policy Sponsor	Chief Financial and Operations Officer
Policy Manager	Manager Technology Platforms
Approving Authority	Chief Executive
Amendment History	Refer to Technology Use Policy for amendment history.