|  |
| --- |
| Acceptable use of technology policy  (example) |

## Policy purpose

This policy outlines the acceptable use of technology at [ORGANISATION NAME]. Inappropriate use can expose your organisation to risks including data loss, cyber attacks, compromise of network systems and services, loss of productivity and legal action.

**Scope**

This policy applies to the use of all [ORGANISATION NAME] technology and any personal devices connecting to and/or using [ORGANISATION NAME] systems or services.

**Definitions**

Staff: everyone provided with a [ORGANISATION NAME] account. This includes all employees and contractors. This may also include consultants and third-party vendors.

Personal devices: any form of technology not provided by the organisation that staff use to do their work.

[ORGANISATION NAME] technology: information and communications technology (ICT) systems, services and devices that are used and managed by the organisation. This includes:

ICT hardware, eg, computers, removable devices, mobile devices, telephone systems and printers.

software and systems, whether locally installed, networked or cloud based, eg, Microsoft M365, Intranet, software applications or tools, databases and email.

systems and devices supplied, maintained or administered by third-party suppliers.

**Policy requirements**

All staff must:

* Be aware of and adhere to this policy (staff are required to complete an [Agreement to comply with conditions of technology use form](https://objweb.tec.govt.nz:8443/id:A1063658) [add link])
* take reasonable steps to mitigate any identified risks
* report on these risks and/or policy breaches to the appropriate person or group in the organisation.
* All third-party vendors must adhere to [ORGANISATION NAME]’s ICT policies. Staff must ensure vendors are aware of this obligation and must call out if a vendor is unable to.

**Policy principles**

* [ORGANISATION NAME] technology is the property of [ORGANISATION NAME], whether supplied, maintained or administered internally or by third-party suppliers.
* Technology must be used for business purposes. However, limited and reasonable personal use of company technology is allowed.
* Use of [ORGANISATION NAME] technology requires having multi-factor authentication (MFA) enabled on your mobile devices, ie, mobile phone.
* [ORGANISATION NAME] proprietary information stored on [ORGANISATION NAME] technology, whether owned or leased by [ORGANISATION NAME], the employee or a third party, remains the sole property of [ORGANISATION NAME].
* All uses of [ORGANISATION NAME] technology must comply with all [ORGANISATION NAME] policies, standards, procedures and guidelines, as well as any applicable license agreements and local laws and regulations.

**Acceptable use**

* The acceptable use of [ORGANISATION NAME] technology encompasses the following responsibilities for all staff:
* Comply with the [ORGANISATION NAME] Code of Conduct when using [ORGANISATION NAME] technology.
* Exercise good judgment regarding the reasonableness of personal use.
* Understand your security responsibilities and comply with legislation and related policies and guidelines when carrying out [ORGANISATION NAME] activities.
* Protect [ORGANISATION NAME] information, resources and sensitive information from unauthorised use or disclosure.
* Notify the ICT Service Desk about any:
* unauthorised access or disclosure of [ORGANISATION NAME] information
* misuse, damage, loss or theft of any [ORGANISATION NAME] technology
* infection with a virus or malware of any [ORGANISATION NAME] technology.

**Unacceptable use**

* The following activities are prohibited for all staff, with no exceptions:
* Conducting fraudulent or illegal activities.
* Violation of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.
* Performing any act that may bring discredit to [ORGANISATION NAME], its staff or business partners.
* Stealing or copying electronic information or data without permission.
* Distributing, transmitting, posting or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, racist, defamatory, discriminatory, sexist or illegal.
* Providing unauthorised third parties with access to [ORGANISATION NAME]’s information, resources or facilities.
* Installing, downloading or using (online) software and products for undertaking [ORGANISATION NAME] work that are not approved for use at [ORGANISATION NAME].
* Use of someone else’s [ORGANISATION NAME] logon ID and password.
* Browsing the private files or accounts of others, except as provided by appropriate authority.
* Storing any [ORGANISATION NAME] information or data on a non-[ORGANISATION NAME]-issued device or on a third-party file storage service.
* Introduction of malicious code or programs that would affect the performance of or access to any [ORGANISATION NAME] technology or information/data.
* Intentionally creating a security breach or a disruption of [ORGANISATION NAME] technology.
* Tampering with or circumventing [ORGANISATION NAME] user authentication or security controls.
* Disclosing any information about [ORGANISATION NAME] or its staff that is not otherwise public, to unauthorised parties outside [ORGANISATION NAME].

**Using [ORGANISATION NAME]-supplied devices**

* Usage of all [ORGANISATION NAME]-supplied devices must comply with this policy when used within [ORGANISATION NAME] or outside the organisation (eg, in a home office). Staff members must comply with relevant policies when using a company-supplied mobile device.
* [ORGANISATION NAME] has the right to remote wipe the device if required.
* All [ORGANISATION NAME]-supplied devices must:
* be kept secure
* have applied the latest security and device updates
* use a password, Passcode/PIN or biometric protection
* follow [ORGANISATION NAME]’s password guidelines when creating a password.
* All staff are prohibited from:
* leaving the device unsecured or unattended in public areas
* allowing the device to be used by any other party
* connecting to unsecured Wi-Fi networks
* displaying sensitive information when using the device in public places.

**Using a personal device at [ORGANISATION NAME] to connect to [ORGANISATION NAME]**

* Use of personal devices to access [ORGANISATION NAME] networks and information (eg, email) is permitted, provided such use complies with this policy.
* If you choose to use a personal device to connect to [ORGANISATION NAME], you are responsible for:
* all related costs of use
* maintenance and repair of the device
* ensuring the device is current with security updates, eg, anti-virus
* ensuring the device is password protected
* ensuring the device is locked when not in use.
* [ORGANISATION NAME] may prevent, limit and/or revoke the use of personal devices for work purposes at any time.
* Staff leaving [ORGANISATION NAME] must ensure that all [ORGANISATION NAME] information and/or data has been removed from personal devices.
* Any support requested for personal devices will be limited and only provided when work-related. Some information related to personal devices may be retained within [ORGANISATION NAME] systems as part of this support work.

**Using email**

* The [ORGANISATION NAME] email system is intended for business purposes only. [ORGANISATION NAME] monitors email messages for compliance with our policies and to help manage the system.
* Before sending an email, users must remember they represent [ORGANISATION NAME] and not bring the organisation into disrepute using email.
* Staff must use extreme caution when opening email attachments received from unknown senders, which may contain malware. (If in doubt do not open and contact the ICT Service Desk for support.)
* Unacceptable use of email:
* Using a [ORGANISATION NAME] email address for personal activities.
* Using a personal email account to conduct [ORGANISATION NAME] business.
* Sending any [ORGANISATION NAME] information or data to or from personal email accounts (eg, Gmail, Hotmail).
* Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

**Using internet and cloud services**

* When accessing the internet from a [ORGANISATION NAME] device it must be used:
* primarily for business purposes
* in a secure, ethical and lawful manner
* for activities that are appropriate and responsible
* [ORGANISATION NAME] monitors websites visited and blocks web content that it considers inappropriate for the workplace or that may pose a risk to the reputation or security of [ORGANISATION NAME].
* Staff must not use any free versions of cloud services. (Contact the [ICT Service Desk or equivalent] if a cloud service is required.)
* Staff must comply with the relevant policy [add link] when using social media.

**Authorised monitoring**

* Authorised individuals within [ORGANISATION NAME] may monitor [ORGANISATION NAME] technology and network traffic (which may include user traffic) at any time for security and network maintenance purposes.
* [ORGANISATION NAME] reserves the right to audit user activity, networks and systems for security and network maintenance purposes and to ensure compliance with this policy. [ORGANISATION NAME] may obtain and use any data or information generated or accessed through it and report this accordingly to management.
* [ORGANISATION NAME] may without notice delete any non-work-related content or impose restrictions on technology not serving legitimate business purposes.

## Responsibilities and accountabilities

|  |  |
| --- | --- |
| Position | Responsibilities |
| [ROLE TITLE] (Chief Information Security Officer) | Is accountable for this policy in the organisation.  Ensures that this policy and subsequent standards and procedures comply with legal, regulatory requirements, New Zealand Government security requirements and standards; and are understood, implemented, and complied with at all levels of the organisation.  Approves exceptions to this policy in conjunction where relevant with Finance and/or Human Resources. |
| [ROLE TITLE] (IT Security Manager) | Is responsible for the operational implementation of this policy and related standards and procedures.  Ensures adequate skilled resources are available to implement, enforce and monitor effectiveness of this policy and subsequent standards and procedures.  Reviews and advises on this policy and subsequent standards and procedures.  Develops, maintains and improves operational processes to support this policy and related standards and procedures.  Engages with the organisation to ensure their work processes, systems and practices adhere to this policy and related standards and procedures.  Where appropriate develops organisational training and education to enhance organisational awareness of this policy. |
| Managers | Ensures compliance with this policy and related standards and procedures within their business area or area of responsibility in the organisation.  Informs the **[ROLE TITLE]** (IT Security Manager) of any security issues raised to them by staff. |
| All staff | Complies with this policy and related standards and procedures and reports security breaches to their reporting manager and/or **[ROLE TITLE]** (IT Security Manager).  Compliance with this policy is a condition of employment. Non-compliance with this Policy may result in disciplinary action. The severity of the breach will determine the action taken. |

**Related policies and guidance**

* This policy is related to the following policies and guidance on [relevant platform]:
* [relevant policies]
* [relevant procedures]

**Further assistance**

If you have any questions in relations to this policy and any related standards or guidelines, please contact [ROLE TITLE].

Sponsor: Role Title (Chief Information Security Officer)

Owner: [ROLE TITLE] (IT Security Manager)

Approved by: Appropriate authority

Last approval date: MMM YYYY

Last review date: MMM YYYY

Next review date: MMM YYYY