




**MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT**
HĪKINA WHAKATUTUKI



Information Communications Technology (ICT) Acceptable Use Policy

Released under the
Official Information Act 1982

Purpose

The purpose of this policy is to ensure all MBIE data, information and technology is used in the correct way and for the appropriate reason.

Scope

This policy applies to all staff who use technology, including those in offshore branches (except where it conflicts with local legislative requirements).

Help

For clarification about this policy in a particular situation contact:

ICT Performance, Planning & Assurance

ICTPPA@mbie.govt.nz

Definitions

Technology: For the purposes of this policy, 'technology' refers to any device or system used to produce, access, store or communicate data and information.

Staff: All individuals, directly employed by MBIE, and contractors or employees of organisations supplying services to MBIE, inclusive of individuals who are based offshore.

Appropriate use: Reasonable and responsible use which:

- is predominantly for business purposes
- does not impact on technology performance, speed or availability
- does not involve media streaming unless it is work related
- does not result in unnecessary costs to MBIE
- does not involve excessive storage of personal material
- does not include objectionable or offensive material
- is consistent with MBIEs' values, integrity principles and Code of Conduct.

"Bring Your Own Device (BYOD)": Personally owned devices that are used to access MBIE data, information and systems.

Policy Statements

1. Staff will demonstrate appropriate use of technology by [following instructions for safe and secure technology use](#).
2. Personal use of MBIE technology is permitted as long as it is appropriate and kept to a minimum.

3. MBIE has the right to monitor all use of MBIE technology, systems and information, including BYOD, to ensure usage is appropriate, safe and secure.

Key accountabilities and responsibilities

The **Chief Executive** (CE) is accountable for the ICT Acceptable Use Policy.

The **Senior Leadership Team** (SLT) is responsible for endorsing this Policy as well as promoting and supporting the continuous improvement of the acceptable use of ICT in the Ministry.

The **Deputy Chief Executive** (DCE) of Corporate, Governance and Information (CGI) is responsible for recommending that the ICT Acceptable Use Policy is endorsed by the Senior Leadership Team.

In addition to line management responsibilities, each **Deputy Chief Executive** is responsible for receiving assurance from their general managers that their branch is complying with this Policy and providing the Chief Executive with such assurance as necessary

General Managers (GMs) are responsible for ensuring their managers and staff are made aware of and comply with the ICT Acceptable Use Policy.

The **Chief Information Officer** (CIO) is responsible for the ICT Acceptable Use Policy, including ensuring it meets the minimum requirements for development and implementation, it is signed off at the appropriate level, compliance can be monitored and breaches are investigated.

The **Information Communication Technology Branch** (ICT) will support the CIO to:

- review the policy periodically to ensure it meets MBIE's requirements
- ensure the ICT Acceptable Use Policy is published on The Link
- provide reporting on MBIE's use of Information and Communication Technology to measure compliance and investigate breaches
- ensure that the ICT Acceptable Use Policy meets the requirements of the Government CIO and NZ Information Security Manual (NZISM).

All **managers of staff** are responsible for:

- ensuring their staff are aware of this policy, procedures, and Instructions for Safe and Secure Use; including reminding staff of their obligations under the ICT Acceptable Use Policy
- discussing use of technology with their staff to ensure use is appropriate, necessary, and not putting MBIE at risk
- reinforcing MBIE's commitment to maximising the value realised from our investment in technology
- ensuring the timely return of any MBIE technology and information
- reviewing reports provided by ICT to ensure that their staff have the appropriate technology allocated, are using technology appropriately, and actioning any issues

- ensuring staff receive appropriate training on how to use technology safely and securely
- the reporting of breaches of this policy to the GM and DCE in their reporting line.

All staff accessing MBIE data, information and systems are personally responsible for:

- using technology appropriately and in accordance with all established policies, procedures, instructions, and guidelines
- limiting personal use of MBIE technology to ensure that personal use does not unduly impact productivity, threaten the security of MBIE's ICT environment, or negatively impact system performance and cost
- registering BYOD devices
- using only authorised technology to access MBIE data, information and systems
- managing user accounts and passwords by following instructions for safe and secure use
- not storing MBIE data and information in locations that have not been approved by MBIE
- safely using devices which are accessing MBIE information, data and systems by maintaining an awareness of risk, in particular when using devices in public places or on public Wi-Fi systems
- labelling, sending and using messaging and documents appropriately, as per the Rules for Document Classification
- immediately reporting lost or stolen devices, including BYODs, to the ICT service desk so that procedures can be applied to protect MBIE data, information and systems
- not recording images, audio or video unless approved by all participants and classified and stored appropriately.

HR Recruitment are responsible for:

- ensuring the ICT Acceptable Use Policy is sent to successful candidates (both permanent and fixed term roles) along with their contract of employment and offer letter and then filing the signed returned policy in employees files in MAKO

Mandatory guidelines and processes

- [Instructions for Safe and Secure Technology Use](#)
- [Approved ICT Devices](#)
- [Rules for Document Classification](#)

Related MBIE policies

- [MBIE Code of Conduct](#)
- [Sensitive Expenditure Policy](#)
- [Travel Policy](#)
- [Protective Security Policy](#)

- [Privacy Policy](#)
- [Records Management Policy](#)

Relevant legislation and regulations

- Privacy Act 1993
- Official Information Act 1982
- Copyright Act 1994
- Public Records Act 2005
- State Services Code of Conduct
- New Zealand Information Security Manual (NZISM)
- State Sector Standards of Integrity and Conduct
- Controlling sensitive expenditure: Guidelines for public entities

Measures of the success of the Policy

The success of this policy will be measured through the monitoring and analysis of staff use to ensure usage is appropriate.

Consultation processes in developing or reviewing this Policy

Key stakeholders were consulted in the development and consequential reviews of the ICT Acceptable Use Policy. These include:

- ICT Information and Data
- ICT Strategy, Architecture and Security
- ICT Security and Risk
- Director of Security
- Business Manager & Client Relationships
- Risk and Assurance
- Human Resources
- Legal
- a sample of end users in each business group.

Compliance Management

Managers are responsible for use of technology by their staff. They will receive reporting from ICT to ensure that the appropriate technology is allocated, use of technology is appropriate and costs incurred are correct.

The following compliance management tools and processes will be used to minimise the risk of breaches of this policy before they occur, allow visibility of compliance against this policy and identify trends or risks so they can be appropriately managed:

- blocking access to websites, whitelisting applications, forcing document classification and compliance to password rules, and removing access to or applications from devices, which result in a breach of the policy
- tools such as checklists or online modules to help inform staff and managers of their obligations
- reviews of performance in relation to required processes, procedures or guidelines, set out in the mandatory procedures listed above, on a regular basis to ensure continued improvement
- breaches will be recorded in a central register.

Compliance information regarding the performance of this policy will be provided to Risk and Assurance on a quarterly basis.

Communication and Training

The ICT Acceptable Use Policy is communicated to staff through its inclusion in the induction process and is available on The Link as part of MBIE's internal policies. An online module on the Learn@MBIE site provides an overview of security, including technology and cyber security and is compulsory for all staff members to complete. There are also optional 'tech sessions' provided by ICT through Learn@MBIE for staff who want training on how to use ICT in a secure and acceptable way.