ACCEPTABLE USE OF TECHNOLOGY POLICY

PURPOSE

The purpose of this policy is to establish acceptable use of Information and Communications Technology (ICT) and to explain the duty of care that is expected of us when dealing with Ministry information. We all have an obligation to ensure that our use of ICT does not compromise the reputation of the Ministry or adversely impact our customers or stakeholders.

The Acceptable Use of Technology Policy is designed to ensure that ICT is always used in a manner that is safe, secure and productive for you and our stakeholders.

SCOPE

The scope of this policy includes all aspects of Ministry ICT and data/information including, but not limited to, desktop computers, laptops, mobile computing devices (including Tablets, iPhones and iPads), SMS messages, virtual machines, telephony, printers, scanners, servers, email, intranets, internet access, WiFi, and core business applications.

This policy applies to all users of Ministry ICT including full-time or part-time employees, volunteers, contractors, vendors and personnel affiliated with third parties. This policy applies at all times, during and outside of business hours.

This policy outlines the expectations required of you, but is not a comprehensive list of what you must and must not do. You are expected to apply good judgement when using Ministry ICT systems and handling Ministry records and information. You must consult your manager if you are unsure what this means.

RESPONSIBILITIES

Employee	• Keep informed of the *Ministry's Acceptable Use of Technology Policy* and seek clarification from your manager if required. • Ensure reasonable and appropriate use of ICT in the Ministry by complying with this policy and any other related policies and procedures.
Manager	• Provide advice and guidance to employees regarding the acceptable use of ICT. • Request investigation where reasonable justification has been identified.
Manager ICT Security	• Provide the monitoring, alerting and reporting of any use of technology that might be in breach of the Code of Conduct, and to educate about acceptable ICT use.

General Manager People Experience	• Assist managers to communicate the *Acceptable Use of Technology Policy* to employees. • Work with employees and their managers to investigate and resolve non-compliance issues.

LIABILITY

You are responsible and accountable for the consequences of your actions including any use of Ministry ICT that is inconsistent with the activities of your job purpose or function. If you have any doubt about what the Ministry would consider 'reasonable' you should consult your manager. Any infringement of the Acceptable Use of Technology Policy may result in disciplinary action up to and including dismissal.

OUR POLICY

Quick links

Personal use of Ministry ICT

Protecting Ministry information

Prohibited use of Ministry ICT

Information Security Controls (includes user accounts and passwords, use of external storage devices, installation and modification of software)

Social Media

Using Cloud services

Mobile devices

Relevant legislation

Related policies and procedures

Limit Your Personal Use

Reasonable and appropriate personal use of Ministry ICT is permitted except where that usage impacts network performance, personal productivity or results in undue costs being incurred. You **must** consult your manager if you are uncertain about what constitutes reasonable and appropriate use.

Excessive personal use of the Ministry's technology can impact network performance and productivity, and cause increased costs for the Ministry.

Heavy usage of network data (such as streaming videos, large file downloads) can impact Ministry ICT services for other employees. Heavy usage is monitored and reported on.

You are not permitted to use your Ministry email to register for services that are not business related or approved by your manager.

The Ministry reserves the right to block access to internet sites and services for operational or security reasons.

Notice of monitoring

All email and internet traffic within Ministry networks is monitored, logged and audited. The content of all storage devices, including desktop computers, laptops, file servers, work related mobiles, cloud services and any device connected to Ministry equipment is periodically scanned for malicious, illicit, illegal and inappropriate content.

Monitoring of personal use of Ministry-supplied ICT services and devices is conducted both on an on-going basis and ad-hoc where specially required, in accordance with the Privacy Act 2020. This includes the monitoring of web browsing, emails, instant messaging and applications used to work mobile devices.

Protect Information

You **must** treat all information as a Ministry asset, and protect it appropriately, unless it is clearly identified otherwise.

Inadequately protected information can adversely impact our customers' privacy and the Ministry's reputation.

When accessing or processing Ministry information, you **must**:

- only access information you are authorised to for legitimate work purposes or as required in the course of your duties and consistent with the access provisions of Court Rules, judicial decisions and/or other policies, procedures and guidelines,
- ensure that information is kept appropriately secure by clearing documents from your desk when absent from your work area and from the output trays of printers, faxes and photocopiers,
- lock your screen if you leave your computer unattended,
- report actual and suspected security incidents or weaknesses to either the Service Desk or your manager,
- assess the risks and consequences of unintended disclosure before transferring information outside of the Ministry, especially to non-government parties. This includes transfer by email and portable devices. Consider the use of encryption where the risk and consequences of unintended disclosure are considered unacceptable. Information classified as SENSITIVE and RESTRICTED must be encrypted before transmission.

Unless done so in line with approved business processes, including ICT approval, you **must not**:

- store Ministry information on IT systems outside of those managed by the Ministry or transport information between such systems except when explicitly permitted to do so,
- transmit or distribute any Ministry information via any internet or web-based service,
- transmit or distribute any Ministry information via portable hard drives,
- intentionally access, modify or delete material that you don't have authorisation to access, modify or delete.

As example, you must not, without authorisation:

- use personal email or an unauthorised portable storage device to transfer Ministry information,

- store Ministry related information on a personal computer or device,
- use an unapproved cloud service to transfer or store Ministry information.

Prohibited Use

You **must not** use Ministry ICT for any purpose that might violate or infringe upon the rights of others or which might be considered offensive or defamatory. Such prohibited use includes, but is not limited to:

Unacceptable actions could damage the Ministry's reputation, cause harm or distress to others, or breach the law.

- distributing or storing unauthorised material in support or operation of any business activity other than that of the Ministry,
- conducting any illegal or unethical activity,
- knowingly destroying the integrity of any information,
- downloading, viewing, storing or distributing material that is vulgar, profane, insulting, of a sexual nature, or in any way likely to be offensive to other people,
- distributing spam or electronic harassment of any kind,
- defamation of any individual or organisation,
- distributing, storing, or accessing material in a manner that might infringe copyright, patent, trade secret or any other intellectual property rights of any person or organisation,
- accessing, promoting or taking part in gambling or gaming.

Information Security Controls

Our ICT systems are protected by a number of information security mechanisms, including use of user accounts and passwords. You are always responsible for the use of your accounts, and must take all reasonable measures to keep your passwords and other security credentials confidential.

Breaches of the Ministry's security controls can lead to unauthorised access to or loss of sensitive information.

You **must**:

- maintain the confidentiality of your account and password details for any system that holds Ministry related information (including external login portals), and not share them with any other person,
- use passwords that meet the complexity requirements of the *Ministry of Justice Password Guidelines* document.

You **must not**:

- access Ministry ICT systems using any other person's account,
- connect non-Ministry provided equipment (including portable hard drives, mobile phones and CDs) to the Ministry's system

- connect networks (including access points and ad-hoc WiFi networks) to the Ministry's systems,
- attempt to install software (including plug-ins, patches, fixes, and games) from any source regardless of whether a current licence is held other than via a Service Desk request,
- perform or attempt any actions which are designed to circumvent information security mechanisms.

Social Media Services

Social media services (e.g. Facebook, LinkedIn, YouTube, and Twitter) provide facilities for online collaboration and social networking.

Unnecessary disclosure of work-related information on Social Media can damage the Ministry's reputation.

Whether you are using these services at home or from within Ministry systems, you are reminded of your obligations to keep Ministry information confidential and to act in accordance with any applicable laws, including the Privacy Act 2020. For example, you should not publish information about Ministry business or comment in a manner that may harm the Ministry's reputation on any public website.

It is important you are aware that information disclosed on the Internet is implicitly or explicitly placed into the public domain. Once placed into the public domain, information may be used, in a variety of ways, without your knowledge or authority. For example, the Ministry, if appropriate, might use such information in a work-related investigation.

You should be careful about the nature of your posts to services like Facebook, Twitter or Instagram or any other information disclosed to social media services.

Social Media Policy

This section of the Acceptable Use of Technology Policy should be read in conjunction with the Ministry's Social Media Policy.

Cloud Computing

Cloud computing is any IT service outside the direct control of the Ministry and outside the Ministry's network boundary, where the Ministry's information is stored or processed.

Using cloud services that have not been evaluated and approved may result in disclosure or loss of sensitive information.

Examples of cloud computing services are Dropbox, Office365, iCloud, Google Drive/Docs, Amazon cloud drive, and Box.

Although convenient, cloud computing introduces risk to the Ministry environment. Factors such as ownership of data, availability, accessibility, and security controls in place must be considered when utilising cloud services.

You **must not** use any cloud services to host Ministry data unless it is a Ministry approved cloud service endorsed by the Chief Executive.

	Court information and Judicial information[1] **must not** be stored or processed on offshore cloud services without the prior agreement of the judiciary.
Ministry Provided Mobile Devices	Ministry tablets and iPhones are assigned for checking emails, calendar appointments, reading documents and being reachable while mobile. **Loss or inappropriate use of mobile devices could lead to unauthorised access to sensitive information.** You **must**: • update your device when notified to from ICT communications, • consult with ICT if you are travelling overseas to a high risk country (as defined by the Privacy and Security team) and comply with their recommendations for Ministry equipment you may take, • report to the service desk if your device is lost or stolen, or you think it has been compromised. You **must not**: • download applications that could adversely affect the Ministry's reputation, • leave mobile devices unattended in places from which theft is a reasonable possibility such as vehicles parked in public spaces, or left luggage depositories while travelling, • tamper with or modify the base settings on the device. This includes attempting to alter the device's Outlook synchronisation settings or jailbreaking your device.
Personal Devices	You must not use personal devices to access Ministry systems and information except when explicitly permitted to do so. Information on approved personal mobile device usage can be found on Jet: https://jet.justice.govt.nz/how-do-i/mobile-devices-and-services/. When permitted to access Ministry data from personal devices, you must agree to be bound by any and all conditions of use specified by the Ministry including the Ministry's right to revoke your access and/or wipe Ministry data. It is your responsibility to ensure that any Ministry information held within a Ministry-provided system approved for use on personal devices is not copied or transferred to any other non-approved location. The Ministry does not pay for, or reimburse, any costs incurred when using a personal device. If your manager approves you as eligible for a Ministry supplied plan, then this can be used in a personally supplied device. Please note that a supplied Ministry phone plan should follow all acceptable use guidelines.

EXCEPTIONS TO THIS POLICY

Employee	If you identify a legitimate business need which requires an exemption from this Policy, you **must** discuss and agree this with your manager before taking any action which breaches the Policy.

[1] Defined in Schedule 2 of the Senior Courts Act 2016 and Schedule 1 of the District Courts Act 2016.

	You **must not** take any action which breaches this Policy until a formal exemption is granted.
Manager	If there is a sound business reason for requesting an exemption from this Policy, you **must** engage with ICT Security who will endeavour to identify safe alternative ways to meet the requirements of the business. In the event that an exemption from any aspect of this Policy is required, ICT Security will grant a time-bound exemption to identified staff or business functions.
ICT Security and Security Assurance	ICT Security **must** gain the approval of the Chief Information Security Officer (CISO) before granting a formal exemption from this Policy. Exemptions **must** be time-bound and limited to identified staff or business functions. A register of exemptions **must** be maintained. Exemptions **must** be reviewed and modified, re-validated or withdrawn as they fall due.

RELEVANT LEGISLATION

Employees must not use Ministry-provided ICT to distribute, publish, reproduce or transmit any information in a manner that may breach the obligations of the Ministry or its employees under the following or any other relevant New Zealand legislation:

- Privacy Act 2020
- Official Information Act 1982
- Copyright Act 1994
- Public Records Act 2005
- Crimes Act 1961
- Electronic Transactions Act 2002
- Harmful Digital Communications Act 2015

RELATED POLICIES AND PROCEDURES

- Ministry of Justice Information Security Framework
  https://jet.justice.govt.nz/our-work/strategy-and-direction/information-security-framework/
- Ministry of Justice password guidelines
  https://jet.justice.govt.nz/how-do-i/create-strong-passwords/
- Security and Usage Guidelines for CMS Users
  https://jet.justice.govt.nz/assets/ICT/How-do-I/0ca396b112/cms_security_and_usage_guidelines_May_20181.pdf
- Code of Conduct
  https://jet.justice.govt.nz/our-work/people/code-of-conduct/

- Ministry of Justice Data and Information Policy
  https://jet.justice.govt.nz/how-do-i/guidelines-for-the-data-and-information-policy/
- Privacy & Information Policy and associated Guidelines
  Privacy | JET — Ministry of Justice Intranet

OWNER	GM Resilience and Assurance Services & Chief Information Security Officer	CONTACT	sean.malthouse@justice.govt.nz
LAST REVIEWED	February 2023 (interim version)	NEXT REVIEW	December 2023
APPROVED	Deputy Chief Executive		