Information Technology and Services Acceptable Use Policy

On this page

Last reviewed: October 2019
Next review: October 2021
Owner: Manager Customer Services, FPT

Purpose

The purpose of this policy is to ensure all Department of Corrections' data, information, systems and technology, is obtained, purchased and used in the correct way and for the appropriate reason. This Policy merges, and replaces, both the former IT Acceptable Use Policy and the Mobile Phone Policy.

This policy aligns with the Department's values and guiding principles of:

- Rangatira – Leadership; Manaaki – Respect; Wairua – Spirituality; Kaitiaki – Guardianship; and Whānāu – Relationships
- Complying with the law and legislation
- Ensuring a healthy, safe and secure environment
- Being a good employer, and
- Acting in the Spirit of Service.

Scope

This policy applies to all users of Information Technology Services at Corrections.

This policy applies to all Information Technology Services irrespective of whether they are free or paid for. Information Technology Services include:

- Software
- Hardware

- Software as a Service
- Websites
- Hosting Services

Key Principles

1. All Staff must use information technology services assigned or allocated to them for work related activities following the Department's Employment Code of Conduct at all times.

2. Department of Corrections information technology services are available to approved users only. Some Department of Corrections' information technology services are licence-based and may only be available in limited numbers or at an extra cost. All users must gain approval from their direct manager before requesting or use of any information technology services. Requests for provisioning of technology should be directed to the IT Service Desk clearly stating the work needs.

3. All information technology services, websites, all hosting services including all cloud as-a-service technology must be purchased via IT to ensure;

    a. Appropriate approval,

    b. The technology meets both Government Chief Digital Officer and Corrections policy

    c. The information technology service   is maintained and supported adequately.

4. Storing of Departmental information on external websites, all hosting services and cloud as-a-service technology is not allowed without the Department's Chief Digital Officer's approval.

5. Use of non-Department managed devices or unauthorised software (including cloud services) for storing Department information is not allowed without the Department's Chief Digital Officer's approval.

6. Specialist staff may be granted permission to utilise specialised software (including cloud services) and gain access to social media and social networking sites for their specialist job roles using a secure and approved technical environment. These people should be formally granted permission in writing and adhere to the specific software operational guidelines at all times.

7. All staff are permitted to access approved cloud services. Accessing publicly a services for work purposes should be done only from a Department managed for that purpose. A list of IT Security approved software and directions for use can be found at IT Security Guidelines on Tātou.

8. Staff are given the system access required to do their jobs when operating Department provided equipment. Administrator rights are granted only to authorised support personnel. Users should seek IT assistance for installing new applications following the standard approval process.

9. All staff are responsible for user accounts assigned to them. Staff must use only their own unique ID and password to access the Department provided technology. Staff must never share their login details with others.

10. Only authorised IT technology is permitted to be connected to the Department's network(s) and systems.

11. All departmental data, irrespective of type or format remains the property of the Department and as such will be available for scrutiny at any time. In addition, Department data is subject to this and other departmental policies, regardless of the ownership of the device. Departmental data should be protected at all times. All staff should take reasonable measures both collectively and individually to make sure adequate controls to maintain confidentiality are in place and all breaches are reported.

12. Corrections business systems or business related information the Department owns or has access to e.g. IOMS, COBRA, and SAP may only be accessed for appropriate business purposes that relates to a user's role. Accessing information or systems without good reason is prohibited.

13. Reasonable personal access to non-Corrections systems (e.g. Internet browsing and email) using a Corrections network or a Corrections device is permitted. However, it should be kept to a minimum and must not impact the Department's normal business operations, incur any extra cost to the Department, put any Departmental data at risk of unauthorised access, or damage organisational reputation. The Department reserves the right to recover any mobility costs from staff who have incurred costs of a personal nature that are considered excessive, (more than incidental to business use), refer to Sensitive Expenditure Policy.

14. Departmental equipment or services must never be used to threaten or harass other users, conduct unsolicited mass e-mail promotional campaigns (spam) for commercial or profit-making, or viewing objectionable or illegal material as mandated by the Department of Internal Affairs guidelines

15. Staff must avoid unauthorised modifications to technology (such as installing software or changing critical settings) that would potentially compromise the security of data or bring the Department into disrepute. Network scans, attacks and d compromises of Department systems and information are strictly prohibited.

16. Department managed devices may require IT to wipe the device to ensure the security of Department information. Limited storing of personal information is allowed on non-critical devices (such as desktops, laptops and mobile phones)

however staff may lose their personal data when a Corrections device is wiped or replaced as part of a Corrections management of that device.

17. Technology issued to individuals by the Department remains the property of the Department and must be returned when requested. All technology should be brought on site for relocation or secure disposal when no longer required.

18. IT equipment is generally assigned to a staff member or contractor while working with the Department. It is the prime user's responsibility to ensure that the device is connected regularly (at least monthly) to the Department's networks to allow for regular software and firmware updates.

19. Only approved personnel are authorised to publish Department information in online communication channels (such as social media sites and blogs). No Departmental information should be published online from any device without written authorisation. Departmental staff should not respond to, or become involved in social media exchanges with people in our care or their friends and associates without approval and the use of appropriate equipment.

20. All staff who remotely access Department information from outside their work place must take reasonable steps to protect the information including checking the environment and using up-to-date systems. Viewing or working with information on Corrections systems, outside Corrections sites (e.g., using mobile device on a train or in a café) carries risks of that information being viewed by non-corrections staff. Take reasonable steps to keep that information safe. This could include placing yourself to avoid someone looking over your shoulder, and ensuring your assigned devices is kept up to date.

21. All parties operating mobile devices with Department data must take all reasonable steps to prevent theft or unauthorised access to the equipment. Lost or stolen devices should be reported immediately to the IT Service Desk.

22. All users must report activities that violate this policy immediately to the IT Service Desk

Related Departmental Policies and Procedures

Policy / Procedure	Relevance
Code of	Describes the principles we operate by – the principles that enable us

Conduct	to make a positive difference.
IT Security Policy	Defines the IT security requirements that will allow us to prevent, to the best of our ability, threats to the security of our IT assets from being realised, and mitigate as many risks and areas of vulnerability as possible and practicable
Information Security Policy	Captures the high level information security requirements that will allow us to protect our information assets and capture the responsibilities of the different roles involved in information security
Certification & Accreditation Policy	Defines the security risk management requirements that will allow us to effectively certify and accredit the initial use of IT systems and services, and periodically reassess these IT systems and services to ensure they continue to meet the Department's standards and Government's expectations
Social Media Policy	Provides guidance for, and sets out the obligations of, users using social media both as a representative of the organisation and in a personal capacity.
Creating Good Passwords & Passphrases	Provides guidance to ensure security access to technology is by authorised users only
Safe Driving and Use of Departmental Vehicles Policy	Provides guidance for the use of mobile devices in vehicles
IT Mobile	Provides information and costs for approved technology

Outside of Scope ████████████████████████████

Plans and Price List	
Mobile International Travel Bundles Guide PDF, 545.7 KB	Provides guidance, and options for staff to enable, on mobile devices before travelling overseas on business.
Sensitive Expenditure Policy	Provides guidance on departmental expenditure that may be for personal use that may be considered more than incidental to business use.

Key Accountabilities and Responsibilities

Person / Party	Responsibilities
Users	• Ensure they receive and complete training as required on how to use technology safely and securely • Carry out requests from the Departmental IT team. This may include but is not limited to, stopping streaming audio or video, downloading of data or logging off the network • Take care to protect the Department's technology systems and devices from misuse, loss, theft, other security breach or damage. • Immediately report any breach of this Policy to your Manager such as, inappropriate use of technology systems, misuse of Department's information or inappropriate material found or seen. • Accept that use of the department's devices may incur usage (e.g. Mobile Devices); these costs are the responsibility of the Centre Manager. However usage and resulting costs considered excessive may be recovered from the staff member.

Person / Party	Responsibilities
Managers of Users	Promote compliant use of technology, • Accountable for devices allocated to users – this includes being able to locate devices. • Ensure timely return of any Department technology from users where the device is no longer required. • Ensure staff are provided appropriate training and support as required on how to use technology safely and securely • Cost Centre managers review usage costs and where excessive take appropriate action. • ensure appropriate disciplinary action for reported breaches
Manager IT Security & Assurance	Accountable for: • Setting technology security standards to reduce exposing the Department to any unauthorised access, data loss and/or disclosure of technology • Reviewing and ensuring new and current Technology meets security standards

Monitoring and Assurance

This policy will be monitored by the Chief Digital Officer for effectiveness and for compliance.

Measures of Success

Measure of success will be measured by the number connections where

1. inappropriate or unacceptable content has been accessed, or,

2. Individual usage is higher than normal without reasonable justification.

Compliance Management

The following compliance management tools and processes will be used to help ensure compliance with this policy and related procedures, minimise the risk of breaches and identify trends and risks so that they can be managed appropriately:

- Managers are responsible for the appropriate use of technology by their staff and will receive reports from IT to help ensure that appropriate technology is allocated, use of technology is appropriate and costs incurred are correct

- Blocking access to websites, whitelisting applications, forcing document classification and compliance to password rules, and removing access to, or applications on, devices which result in a breach of this policy

- Providing information and reminders to staff about this policy, and their obligations, in order to deter inappropriate use of IT exposing security risks or compromising the Department's data and systems

- Tools such as checklists or online modules to help inform staff and managers of their obligations

Reporting

Reporting is provided on the following basis:

- A standard (existing) report of usage is sent to cost centre managers.

- Exceptional report of atypical use is sent on a case by case basis.

Related Legislation and Regulations

The following legislation creates or contains legal obligations applying to the Department, relating to using, retaining and disposing of information lawfully and appropriately.

- Privacy Act 1993

- Official Information Act 1982

- Copyright Act 1994

- Public Records Act 2005

- Health Practitioners Assurance Act – (regulations re the security of clinical information within the Department)

- Department of Corrections Code of Conduct

Definitions

Staff	All individuals granted access to Department of Corrections technology, including, but not limited to, employees (permanent, fixed-term and casual), secondees, consultants, contractors, service providers and volunteers
Technology	For the purposes of this policy 'technology' refers to any device, software application or system, which includes departmental networks, wireless, cellular and cloud services, used to produce, access, process, store or communicate data and information. This includes mobile phones and other devices such as tablets.
Information	All Department owned information that is stored on Department of Corrections' or privately owned hardware, including mobile devices, software and systems regardless of ownership.
ICT	Information, Communications and Technology
Information Technology Service	Information Technology Services include, but may not be limited to: - Software - Hardware, mobile and fixed - Software as a Service - Websites - Hosting Services
Appropriate Use	Any use for a business purpose. Non business use (private use has to be reasonable and responsib which;

	• Is consistent with the Department's values, integrity principles and Code of Conduct • Does not impact on technology performance, speed or availability of systems and data • Does not involve media streaming unless it is work related • Does not result in unnecessary costs to the Department • Does not involve excessive storage of personal material • Does not include objectionable or offensive material.
In appropriate material	Inappropriate material is strictly prohibited. Examples of inappropriate material (unsuitable or improper) personal material include but are not limited to: • Comments that are pejorative, knowingly inaccurate, unsubstantiated, discriminatory or defamatory. • Copyright breaches • Material that is sexually explicit, racist, offensive or abusive

Last Published: 18.10.2019 | By: ███ 9(2)(a) ████