Wellington City Council

# ICT Policy Handbook

Absolutely Positively
**Wellington** City Council

Me Heke Ki Pōneke

# Contents

# ICT Policy Handbook

## Introduction

This handbook gives you an overview of how Business Information & Technology (BIT) can support you with your ICT needs and explains the policies to apply in order to protect you and the Council.

## Users

The ICT policy handbook is for all users of Council ICT systems including:

- Council employees (including full-time, part-time or casual)
- consultants
- contractors
- councillors
- vendors
- volunteers
- Other third-parties who are responsible for managing, administering, supporting, protecting and accessing Council data, applications or systems.

## Overview

This handbook covers four policies:

- General Information Technology Policy
- IT Security Policy
- Information Management Policy
- Mobile Device Policy

The relevant systems, data and applications are outlined at the beginning of each policy.

The policies aim to manage risks that could impact the confidentiality, integrity, and availability of Council information systems. BIT is the business group within the Council, responsible for the implementation and management of these policies.

These policies will be reviewed on an annual (or as required) basis to make sure information meets any changing circumstances that are significant enough to warrant a change to the policy.

**Note:** There are some clauses in these policies that are intended for IT professionals and need to be included to meet our audit requirements. These are entitled 'For IT professionals'.

## Questions or issues

If you have any questions about these policies, you can contact the BIT Helpdesk (servicedesk@wcc.govt.nz, x3333).

In particular, if you find any component of these policies impacts your ability to do your job, contact the BIT Service Desk so they can try to address this for you.

If you are unhappy with any decision, you will have the option of raising the issue with the Council's Policy Sub Committee.

# General Information Technology Policy

# Equipment and systems

The General Information Technology Policy applies to all Council IT equipment and related components that are used to create, access, process, exchange and store data / information, including but not limited to the following technology:

- Desk phones
- Desktop computers
- Email
- Fax
- Information systems
- Internet
- Mobile devices
- Network hardware
- Photocopies
- Printer / multifunction devices
- Private and public websites
- Social media
- Software
- Storage media and peripheral devices such as flash drives, USB sticks and external hard drives, and any Cloud-based / hosted applications
- Tracking devices

## Policy statement

**1. Eligibility / allocation**

1.1. BIT will issue you with the Council IT equipment you need to do your job.

**2. Procurement**

2.1. BIT will purchase your IT equipment on your behalf to ensure the effective management of Council IT equipment and data purchasing and service requirements. In the absence of a 'Bring Your Own Device' (BYOD) Policy, contact the BIT Service Desk to discuss your business needs if you identify a need to bring a device to work that is not Council owned.

2.2. If you need to make any changes of ownership to IT equipment, data plans and contracts, contact the BIT Service Desk to work through this process with you.

**3. Financial / spending**

3.1. Except in approved cases, your business group will manage all costs associated with IT equipment, including - but not limited to - purchase, maintenance, licensing cost, and call usage.

**4. Property**

4.1. Only use your Council ICT equipment for business purposes, and do not sell or lend it to anyone without agreement.

4.2. Remember, all data / information (including email) you create while using Council systems and applications is considered 'official data' and is the property of the Council.

**5. Management requirements**

5.1. If you'd like to register, record and manage any new requirements for IT equipment, data plans, connectivity, and software applications (including 'Cloud' hosted applications), contact the BIT Service Desk to organise this for you.

5.2. To keep Council data and information secure, make sure you and your team back up or archive data / information before it is deleted. This excludes your personal information.

5.3. If your IT equipment is no longer needed for your role, notify the BIT Service Desk so we can securely dispose of it.

**6. Access to the internet**

6.1. You can access personal email, social media forums and websites, as agreed with direct line managers.

6.2. Any websites that contain inappropriate material will be blocked - including - but not limited to - pornographic, dating, gambling, and gaming websites. If in doubt, check with the BIT Service Desk.

**7. Security of devices, data and information**

7.1. Do your best to securely store confidential data / information and IT equipment. Do not leave these in the care of anyone who has no obligation to this policy and other related Council policies.

7.2. Keep the security information for your Council IT equipment safe.

7.3. If your Council IT equipment is lost, stolen or breached, inform the BIT Service Desk, your direct manager and/or report this to the police as soon as possible.

**8. Monitoring rights**

8.1. In exceptional circumstances, the Council reserves the right to inspect, move, copy or delete information contained in / associated with any Council IT equipment.

8.2. BIT monitors internet traffic on a monthly basis to check internet usage is not excessive. These usage reports are available to Cost Centre Managers and/or Human Resources.

**9. Inappropriate use**

9.1. You can only make physical modifications or reconfigurations to hardware, software and applications on Council IT equipment with BIT approval.

9.2. Avoid electronic “chain letters”, “spam” or advertisements unless they relate to legitimate business activities.

# Associated policies

Read the following documents in conjunction with this policy:

- Information Management Policy
- Mobile Device Policy
- IT Security Policy
- Procurement Policy
- Code of Conduct
- Delegated Financial Authority

**End of Policy**

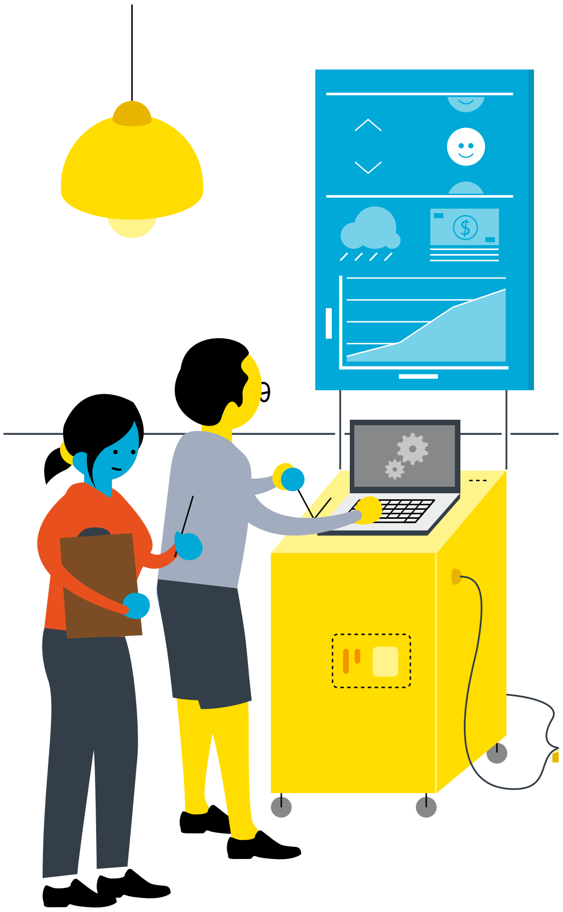
# IT Security Policy

# IT Security

## Electronic information assets

The IT Security policy applies to all Council electronic information assets such as systems / resources, including technology hardware and software, whether owned, leased, or licenced.

This includes - but is not limited to - hardware and software used to process, store, display, and transmit electronic representations of data, voice and video content.



## Policy statement

1. **Security management**

   1.1. Remember to securely control, manage and maintain all IT equipment and software applications you use in your job, whether these are hosted internally or in the cloud.

2. **Access rights and user accounts**

   2.1. Your access rights for applications or systems are assigned based on your role and responsibilities, making sure you have the right tools to do your job effectively. If new rights or changes to current access rights are needed, such as when a role changes or at the end of a contract, people leaders should let the BIT Service Desk know so this can be addressed.

   2.2. Your user account is only to be used by you. If needed, BIT can create group user accounts and passwords.

   2.3. Your user account is unique, and will be disabled when you no longer need it for your work at the Council.

   2.4. The Council will retain access to your user account and email account and manage as required.

   2.5. If you need system administrative rights for a specific business purpose, BIT can set these up for you. These will be removed when you no longer need them for your role.

   2.6. BIT maintains a catalogue of IT user accounts to manage user access. We also maintain a log of invalid log-on attempts for investigation and reporting purposes, if required.

3. **Passwords**

   3.1. BIT will give you a secure password for all the Council's IT systems and devices you use in your role at the Council.

   3.2. Keep your passwords and user IDs secure and do not share them.

4. **Remote access**

   4.1. If you need to work remotely, BIT can set up remote access for you. The system will be made secure by including at least two basic security questions.

5. **Physical access**

   5.1. Remember to keep Council IT equipment secure at all times, whether on site, or off site with third party vendors. Business owners and contract owners are responsible for maintaining this security.

6. **Cybercrime and security incidents**

   6.1. BIT maintains a process for managing and reporting security incidents. If there is a security breach, we will support you through this process to manage the breach.

   6.2. BIT implements detective and preventative controls such as Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS) and corrective processes to keep the Council IT systems safe.

   6.3. If you suspect a security incident, encounter a problem, or receive an alert, contact the BIT Service Desk as soon as possible.

   6.4. BIT is required to commission an IT Security audit by an accredited security auditor on IT equipment and resources owned and managed by the Council, as required. We may ask for input from the wider business for this annual audit.

7. **Viruses**

   7.1. BIT installs, maintains and operates anti-virus software with the most current list of virus definitions on all servers, workstations and devices in the Council's IT environment.

   7.2. If you suspect a virus on any Council system, inform the BIT Service Desk as soon as possible.

   7.3. BIT will make sure that files or software tagged by anti-virus software are removed and recorded in the anti-virus system and the security incident log.

## For IT professionals

8. **Cryptography**

   8.1. BIT uses encryption to protect the confidentiality of all sensitive data / information from an unauthorised access.

   8.2. BIT will securely manage the Cryptographic Equipment and Cryptographic key material so that you can recover data if the encryption key is lost, damages or fails.

9. **Firewall management**

   9.1. BIT installs and manages a network firewall within Council to mitigate the risks identified by risk assessments.

   9.2. BIT is responsible for installing, configuring and managing all firewalls in the Council IT environment.

# Associated policies

Read the following documents in conjunction with this policy:

- Information Management Policy
- General IT Policy
- Mobile Device Policy
- Code of Conduct

**End of Policy**

# Information Management Policy

# Records and information

The Information Management Policy applies to records and information. By records and information, we mean all information created and received as a result of business activities performed by, or on behalf of, the Council.

This includes all written and recorded spoken transactions (eg meeting minutes, Contact Centre voice records) - whether paper or electronic - which result from Council business activities.

## Policy statement

1. **Legislation**

   1.1. All Council records are defined as Local Authority Records under the Public Records Act 2005, and must be kept in accordance with statutory and industry standards or guidelines. This means we need to create and manage full and accurate records that support the day-to-day functions and business activities of our work at the Council, as well as have the ability to authorise disposal of them.

   1.2. The Council is committed to the following information management principles:

   - We will treat information as a corporate asset because it has a quantifiable value and without it we cannot do our business.
   - Employees will be aware of their responsibilities in relation to Information Management to ensure Council information is managed securely.
   - We will safeguard the integrity of information so we can trust that the information we create and manage has not been adversely tampered with, altered or damaged through system error.
   - We will facilitate access to information so that knowledge is shared within the Council.
   - We will openly and proactively share information with the public.
   - We will adhere to the principles of the Privacy Act 1993.

2. **Transition to a digital workplace**

   2.1. The Council is migrating from paper-based records and recordkeeping systems to electronic records and digital recordkeeping. Digital records will be kept for as long as specified in the Public Records Act.

   2.2. The Council will digitise information to meet accessibility and business-process efficiency drivers. The primary focus is to make sure current, or historic physical records that are being scanned for business purposes all meet a defined set of standards.

2.3. The council will adhere to any associated digitisation guidelines to make sure the digital version of the record becomes the official record, enabling the disposal of the physical records.

**3. Security of information**

3.1. It's important that you store, administer, transfer and manage all information in a way that provides reasonable safeguards against loss, unauthorised access, and misuse.

3.2. When communicating both internally and externally, make sure you create and manage information carefully and responsibly.

3.3. To guide us all, the Council have adopted the Association of Local Government Information Management (ALGIM) Information Security Classification Guidelines, Appendix A.

3.4. Make sure you hold confidential physical information securely, with restricted access, eg in suitable lockable filing cabinets. We will not leave such information unattended on desks during the day.

3.5. Make sure you securely file confidential physical information away at the end of the day, adhering to the 'clear desk' rule, where no such information is left on desks when we leave work. This protects the Council against unauthorised access to our information and the risk of data loss in a disaster.

# Associated policies

Read the following documents in conjunction with this policy:

- General IT Policy
- IT Security Policy
- Mobile Device Policy
- Code of Conduct

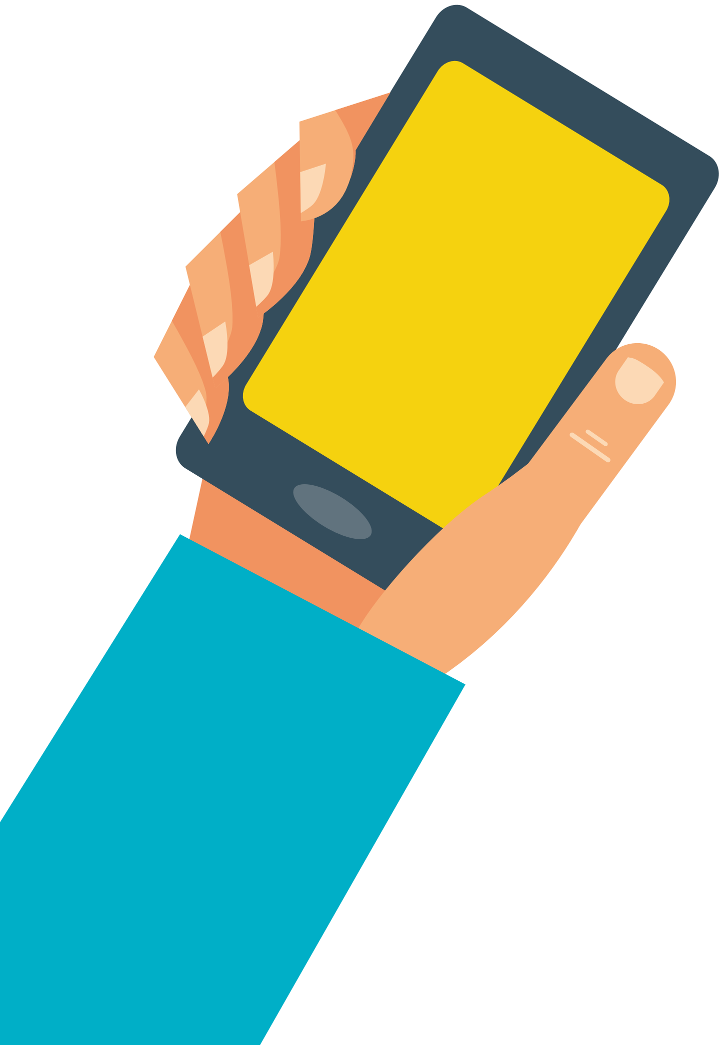
**End of Policy**

# Mobile Device Policy

# Mobile devices and related components

This policy applies to all mobile devices and related components that are used for capturing, storing, accessing, relocating, and backing up Council data / information, including - but not limited to - all devices and accompanying media that fit the following classifications:

- Mobile / cellular phones (Feature Phones)
- Smart phones (all makes and models)
- Laptops / Notebooks
- Personal digital assistants (PDAs)
- Tablet computers such as iPads
- Any mobile device capable of storing data and connecting to a managed or unmanaged network, such as portable disk, USB flash drive or stick, mobile data card and/or mobile broadband device.



## Policy statement

**1. Eligibility / allocation**

1.1. If you need a Council mobile device for your role, contact the BIT Service Desk and we can issue you one.

**2. Management requirements**

2.1. BIT will register, record and manage your mobile device. This allows us to keep an account of all mobile devices, associated equipment and data plans used in the Council's IT environment.

2.2. In the absence of a 'Bring Your Own Device' (BYOD) Policy, contact the BIT Service Desk to discuss your business needs if you identify a need to bring a mobile device to work that is not Council owned.

**3. Procurement**

3.1. The BIT Service Desk will arrange all associated equipment and data plans for your Council mobile device.

3.2. The BIT Service Desk will manage any changes of ownership on your Council mobile device, associated equipment, data plans and contracts.

3.3. To keep Council data and information safe, make sure you and all other users in your team back up or archive data / information before it is deleted. This excludes personal information

3.4. BIT will publish a list of Council-allocated mobile devices in Council directories and make these available on StaffNet.

**4. Financial / spending**

4.1. Except in approved cases, your business group will fund and manage all costs associated with mobile devices, including - but not limited to - purchase, monthly plan, calls, texts, data and overseas usage.

4.2. If you choose to use your Council mobile device for personal use, you may be required to reimburse the Council for personal use up to a maximum amount of $10 per month. This will be managed by your direct line manager.

4.3. BIT monitors mobile device usage and, if usage is thought to be excessive, we send the usage reports to Cost Centre managers and/or Human Resources to review.

**5. Property**

5.1. Only use your Council mobile equipment for business purposes, and do not sell or lend it to anyone without agreement.

5.2. If you leave the Council, return all mobile devices and associated equipment to the BIT Service Desk.

**6. Security of devices, data and information**

6.1. Do your best to securely store your mobile device and confidential data / information. Do not leave your mobile device in the care of anyone who has no obligation to this policy and other related Council policies.

6.2. Be careful not to disclose the security information on your mobile device.

6.3. If you lose your mobile device, or it is stolen or the security is breached, inform the BIT Service Desk, your direct manager and/or report to the police as soon as possible.

6.4. In exceptional circumstances, the Council reserves the right to inspect and access information contained in or associated with any mobile device.

**7. Access rights**

7.1. To make sure the Council's mobile data / information remains secure, BIT reserves the right to restrict, decline or disconnect mobile devices if there is reason to believe Council information and systems are at risk.

# Associated policies

Read the following documents in conjunction with this policy:

- Information Management Policy
- General Information Technology Policy
- IT Security Policy
- Procurement Policy
- Code of Conduct
- Delegated Financial Authority.

**End of Policy**

# Appendix A: ALGIM Information Security Classifications

Security classifications take into account the requirements of New Zealand legislation, international standards and industry best-practice. They are based, in particular, on the Department of the Prime Minister & Cabinet Cab Guide to ensure consistency in terminology across public sector entities. Those guidelines include classifications to cover national security which have been omitted from these classifications as they are not relevant.

In addition the definition for use has been amended slightly to better reflect a Council environment.

| CLASSIFICATION | USE |
|---|---|
| **Unclassified**<br>Open access | - Default value |
| **In Confidence**<br>Prejudice law and order, impede Council business, affect privacy of the public | - Prejudice maintenance of the law.<br>- Adversely affect privacy of a natural person.<br>- Prejudice member of the public's commercial information.<br>- Adversely affect obligations of confidence.<br>- Prejudice measures that protect the health or safety of the public.<br>- Adversely affect the economic interests of the Council.<br>- Prejudice measures that prevent or mitigate loss to the public.<br>- Impede the effective conduct of public affairs.<br>- Breach legal professional privilege.<br>- Impede Council commercial activities.<br>- Disclosure or use of information for improper gain or advantage |
| **Sensitive** | - Damage Council interests, endanger the public<br>- Endanger the safety of any person.<br>- Seriously damage the economic interests of the Council.<br>- Impede Council negotiations. |

## Endorsements

In conjunction with classifications, endorsements can be used to identify protected information. They may also be used on unclassified material and could indicate:

- the specific nature of the information
- temporary sensitivities
- limitations of availability
- how information should be handled or disclosed.

| ENDORSEMENT | USE |
|---|---|
| Council | Material which will be presented to, and/or require decisions by Council or Council Committee. |
| Commercial | Sensitive commercial processes and/or negotiations. |
| Evaluative | Material relating to competitive evaluation such as interview records and tender documents. |
| Staff | Personal information about named or identifiable staff. Also for use by staff in entrusting personal confidences to management. |
| Policy | Proposals for new policy or changes to Council policy before publication. |
| [Department(s)] use only | For use only within the specified department(s). |
| Embargoed for release | Material restricted to internal use prior to a designated time. |
| To be reviewed on | A designated time at which the classification of the information is to be reviewed. |
| Legally privileged | Legal advice or legal proceedings |

Absolutely Positively
**Wellington** City Council

Me Heke Ki Pōneke