POLICY DOCUMENT

Acceptable Use

Policy

Organisation: [Organisation Name]
Version: 1.0
Effective Date: [Date]
Review Date: [Date + 12 months]
Policy Owner: [Name / Role]

Prepared by [IT Provider Name]

1. Purpose

This policy defines the acceptable use of [Organisation Name]'s information technology systems, equipment, networks, and data. It applies to all staff, contractors, volunteers, and any person who accesses the organisation's systems or data in any capacity.

---

2. Scope

This policy applies to all computers, laptops, tablets, and mobile devices owned or managed by the organisation; personal devices used to access organisational systems; cloud services and online platforms used for work; email and internet access; and all data created, stored, or transmitted using organisational systems.

---

3. General Principles

All staff are expected to use organisational technology resources for legitimate work purposes, in compliance with New Zealand law, in a way that does not bring the organisation into disrepute, and with appropriate care for the security and integrity of organisational data.

---

4. Internet and Email

4.1 Internet

Staff may use organisational internet access for work purposes. Incidental personal use is permitted provided it does not interfere with work responsibilities, consume excessive

bandwidth, involve accessing illegal or offensive content, or expose the organisation to legal or security risk.

4.2 Email

- Email accounts are for work use — minimal personal use is permitted
- Do not use organisational email addresses to register for personal services or social media
- Do not send confidential information to personal email addresses
- Do not open attachments or click links in unsolicited or suspicious emails

---

5. Devices and Equipment

5.1 Organisational Devices

- Devices must be kept physically secure and locked when unattended
- Software must not be installed without approval from [IT Manager / IT Provider]
- Devices must not be used by family members or other third parties
- Lost or stolen devices must be reported to [IT Manager / IT Provider] immediately

5.2 Personal Devices (Bring Your Own Device)

- Personal devices used for work must be registered with [IT Manager / IT Provider]
- A device password or PIN of at least six characters must be enabled
- Remote wipe must be enabled and consented to for devices accessing organisational email or data

---

6. Passwords and Access

- Passwords must be at least 14 characters, or use a passphrase of at least four random words
- Passwords must never be shared with anyone — including IT support staff
- A unique password must be used for each system or service
- A password manager approved by [IT Manager / IT Provider] must be used
- Multi-factor authentication must be enabled on all systems that support it
- Suspected compromised passwords must be changed immediately and [IT Manager / IT Provider] notified

PASSWORD MANAGERS

A dedicated password manager generates and stores unique, complex passwords for every system. Reusing passwords across multiple services is one of the most common causes of account compromise. Contact [IT Provider Name] for guidance on approved tools.

---

7. Data Handling and Confidentiality

Staff must handle organisational data in compliance with the Privacy Act 2020:

- Confidential data must only be accessed by staff who require it for their role
- Confidential data must not be stored on personal devices or personal cloud storage without approval
- Client personal information must not be emailed externally in unencrypted form
- Physical documents containing personal information must be disposed of by secure shredding
- Data must not be stored in overseas systems without consideration of Privacy Act 2020 requirements

---

8. Software and Licensing

- Only properly licensed software may be installed on organisational systems
- Pirated or unlicensed software must never be installed
- Browser extensions and plugins must be approved by [IT Manager / IT Provider] before installation

---

9. Social Media

- Do not post content that identifies clients or other third parties without their consent
- Do not post confidential organisational information or financial data on social media
- Make clear when expressing personal views online that those views are your own
- Do not make statements that could constitute defamation, harassment, or discrimination

---

10. Artificial Intelligence Tools

The use of artificial intelligence tools is governed by the organisation's Artificial Intelligence Acceptable Use Policy. Staff must read and comply with that policy before using any AI tool for work purposes. Staff must not submit client personal information, health records, financial data, passwords, or confidential business information to any free or consumer-grade AI tool.

---

11. Monitoring

The organisation reserves the right to monitor the use of its technology systems, including internet access, email, and device activity, to the extent permitted by New Zealand law, including the Employment Relations Act 2000 and the Privacy Act 2020. Staff should have no expectation of privacy when using organisational systems.

---

12. Prohibited Use

The following are strictly prohibited:

- Accessing or distributing illegal content, including material objectionable under the Films, Videos, and Publications Classification Act 1993
- Accessing or distributing material that is sexually explicit, violent, or offensive in a workplace context
- Sending threatening, harassing, or discriminatory communications
- Attempting to gain unauthorised access to any computer system, network, or data
- Installing or distributing malicious software
- Using organisational systems for personal financial gain without approval
- Circumventing security controls, monitoring tools, or access restrictions
- Sharing credentials or allowing unauthorised persons to access organisational systems

---

13. Incident Reporting

Report the following to [IT Manager / IT Provider] immediately:

- Lost or stolen devices containing organisational data
- Suspected phishing, malware, or security attack
- Accidental disclosure of confidential or personal information
- Unusual system behaviour that may indicate compromise

REPORT SECURITY INCIDENTS PROMPTLY

Early reporting significantly reduces the impact of security incidents. Staff will not be penalised for reporting incidents in good faith. Contact [IT Provider Name] on [IT Provider Phone] for urgent incidents.

---

14. Breach of Policy

Breach of this policy may result in disciplinary action up to and including termination of employment. Where a breach results in a notifiable privacy breach under the Privacy Act 2020, the organisation must notify the Office of the Privacy Commissioner and affected individuals.

---

15. Staff Acknowledgement

I confirm that I have read, understood, and agree to comply with this Acceptable Use Policy.

Full Name

Role

Signature

Date

Document Control

Version	Date	Author	Summary of Changes
1.0	[Date]	[IT Provider Name]	Initial version

Prepared by [IT Provider Name] | [IT Provider Website] | [IT Provider Phone]