Digital and Cyber Safety Policy
Te Kaupapa Here mō te Noho Ora ki te Ao Matihiko, ā, ki te Ao Ipurangi hoki

Version 3 | Mahi Tuatoru
Effective Date | Whakamana tahito : November 2025 | Noema 2025
Next Review | ā houanga arotake: November 2026 | Noema 2026
Policy Owner | Rangatira Kaupapa Māhere: Chief Operating Officer
Key Accountabilities | Ngā Takonga Tuatahi: Digital Operations Manager

Introduction | Tīmatanga Kōrero

This policy guides the secure and responsible use of digital tools, technology, and data at Whānau Manaaki Kindergartens. Ensuring technology is used effectively and safely supports our mission to provide high-quality early childhood education and maintain trust with tamariki, whānau, staff, and external stakeholders, including regulatory bodies and partner organisations.

Whānau Manaaki is committed to:

- Protecting all sensitive information, including tamariki, whānau, staff, and external stakeholder data.
- Ensuring digital tools support learning and operational activities.
- Following the Whānau Manaaki Digital Governance Framework (see appendix A for further information).

Whānau Manaaki recognises digital kaitiakitanga as caring for information as taonga and as a shared responsibility across our organisation. This policy supports that commitment and works alongside our Digital Governance Framework. For any activity that involves personal information, the Privacy Policy is authoritative.

Applies To | Ko Wai Whakahāngaitia

This policy applies to all Whānau Manaaki staff, contractors, volunteers, and invited external parties using organisational digital systems, equipment, or data.

Third party access must follow Whānau Manaaki authorisation and approved storage requirements.

General Principles | Mātāpono Whānui

These principles outline the high-level values and guiding philosophies behind this policy. They explain why digital safety and security are essential for Whānau Manaaki and provide the foundation for the specific rules that follow.

1. **Digital Kaitiakitanga (Stewardship)**

- We treat information about tamariki, whānau, staff and partners as taonga that deserves respect and protection.
- We balance usefulness, trust and relationships with technical controls in our daily practice.

***Why this is important**:* It reflects our values and helps ensure the way we collect, store, use and protect information upholds mana and relationships.

2. **Alignment with Digital Governance Framework**:

- Digital practices must align with the Whānau Manaaki Digital Governance Framework to ensure strategic coherence and effective management of risks and resources.

***Why this is important**:* Ensures that digital initiatives support our strategic goals and operational needs.

3. **Protection of Information and Data**:

- Protection of information and data is central to all digital activities. Examples are:
  - Tamariki data (learning records, photos and videos, attendance, health details).
  - Whānau and Community data (contact information, enrolment records).
  - Staff data (employment details, professional development, private records).
  - External stakeholder data (information shared with partner organisations and regulators).

Why this is important**:** Protecting data maintains trust, meets legal requirements (Privacy Act 2020), and upholds ethical standards. This supports Digital Kaitiakitanga and our Privacy Policy obligations.

4. **Continuous Improvement**:

- Regular reviews and improvements of our digital practices help Whānau Manaaki adapt to evolving risks and opportunities.

Why this is important: Keeps our practices current and effective.

Policy Details

Policy details outline specific requirements staff must follow to adhere to these principles.

Definitions: An **incident** is an unplanned interruption or reduction in the quality of a digital service. A **request** is a routine ask such as access or a change that follows an approved process. **Digital kaitiakitanga** is caring for information as taonga and acting as a responsible steward in daily practice.

1. Responsible Use of Technology

- Digital tools and systems must be used responsibly to support tamariki learning and operational activities.
- Limited personal use is permitted if it does not disrupt work, incur additional costs, or pose security risks.
- Only Whānau Manaaki staff may use organisational devices (including work laptops, tablets, and mobile phones). Family members or non-staff must not use these devices.
- All people act as digital kaitiaki. Use systems in ways that protect people and the stories behind our information. If unsure, ask before sharing, storing or forwarding.

Why this is important: Responsible use reduces risks, protects organisational resources, and prevents unauthorised access.

2. Data Protection and Privacy

- All organisational data must be stored in Whānau Manaaki approved platforms (e.g. Teams, SharePoint and OneDrive).
- The use of external storage solutions (e.g., Google Drive, Dropbox) are not permitted unless explicitly approved.
- Use approved tools for sharing sensitive or personal data externally.

These storage and sharing requirements sit under our Privacy Policy which sets the rules for collection, use, sharing, retention and disposal of personal information.

Why this is important: Ensuring secure storage and controlled access reduces the risk and impact of data breaches and compliance failures.

3. Cybersecurity Awareness

- Staff must stay informed on cybersecurity practices through organisational channels like the weekly Kōrero.
- Staff must be familiar with the Digital incident and request process.
- Staff complete required awareness activities when requested.
- Take sensible precautions such as pausing before opening links or attachments and asking if unsure.

Why this is important: Awareness reduces cybersecurity risks and enables swift action to mitigate threats.

4. Account Protection

- Do not share account passwords or credentials.
- Passwords must adhere to Whānau Manaaki password guidelines.
- Follow any additional account protection controls required by the Digital team.

Why this is important: Protecting accounts improves the security of sensitive data and systems, reduces the risk and impact of unauthorised access, and safeguards organisational information.

5. Software and Device Management

- All software installations must follow the Digital Procurement Policy and be authorised by the Digital Team.
- Software covers installed desktop applications, mobile applications, and web based applications and subscriptions.
- Only approved devices are permitted to connect to Whānau Manaaki systems.

Why this is important: Centralised management ensures system security, compatibility, and functionality.

6. Reporting Incidents

- Immediately report cybersecurity breaches, unauthorised access, or malware using the Digital Incident and Request process.
- **If in doubt, report it**. Even minor issues can have serious consequences.

***Why this is important*:** Prompt reporting minimises potential harm and enhances the effectiveness of incident responses.

7. Disposal of Digital Equipment

- Dispose of all ICT equipment following the Digital Procurement Policy procedures to ensure security and environmental responsibility.

***Why this is important*:** Proper disposal prevents data breaches and supports sustainability.

Roles and Responsibilities

The following roles ensure the successful implementation and enforcement of this policy. Each role/group has specific responsibilities that contribute to maintaining a secure, efficient, and compliant digital environment.

- **Digital Operations Manager (DOM):** Oversees compliance, monitors digital security, and manages incident responses. Ensures this policy remains aligned with the Privacy Policy and related privacy statements.
- **Senior Leadership Team (SLT):** Ensures alignment with organisational priorities and resource allocation. Ensures resources and priorities support digital kaitiakitanga and policy compliance.
- **Digital Servicedesk:** Provides support, enforces security, resolves incidents, and offers guidance.
- **All People (staff, volunteers, contractors and invited external collaborators):** Follow policy requirements, use tools responsibly, and report any issues promptly. Act as digital kaitiaki by following approved storage and sharing practices and by protecting accounts and devices.

Relevant Legislation and Regulations | Whaitake Ture me Waituere

The Privacy Act 2020
Licensing Criteria for Early Childhood Education and Care Centres 2008
Whānau Manaaki Digital Governance Framework

Related Procedures or Processes and Documents | Pākanga Tukanga me Pukapuka

Privacy Policy
AI Policy
Digital Procurement Policy
Complaints and Concerns Policy
Digital Incident and Request process

Policy Review Cycle | Kaupapa Arotake Hurihanga

This policy is to be reviewed in six months. Whānau Manaaki may amend or cancel this policy or introduce a new policy, as it considers it necessary within the current cycle of the policy. Any amendments will be considered by the policy Working Group and will need to be approved by the Senior Leadership Team and the Board. The policy will continue on the same review cycle.

Appendices

Appendix A - Digital Governance Frameworks

The Whānau Manaaki Digital and Cyber Safety Policy aligns with the Whānau Manaaki Digital Governance Framework, ensuring that digital security, data protection, and technology use are managed according to international best practices.

This framework integrates **COBIT**, **NIST**, and **ITIL**, which provide governance, cybersecurity, and service management principles to maintain a secure, efficient, and compliant digital environment.

COBIT (Control Objectives for Information and Related Technologies)

- **Purpose**: COBIT provides a governance structure for managing digital risks, ensuring compliance, and aligning technology use with Whānau Manaaki strategic goals.
- **Application in Digital and Cyber Safety:** COBIT ensures that security controls, data access, and risk management are consistently applied across all Whānau Manaaki systems. It also helps define roles and responsibilities in maintaining cybersecurity and digital compliance.

NIST (National Institute of Standards and Technology) Cybersecurity Framework

- **Purpose**: The NIST framework establishes security best practices to protect digital systems and sensitive data from cyber threats. It provides a structured approach to risk management, access control, and incident response.
- **Application in Digital and Cyber Safety**: NIST shapes Whānau Manaaki cybersecurity measures, including password policies, data storage requirements, incident response processes, and ongoing cybersecurity awareness training for staff.

ITIL (Information Technology Infrastructure Library)

- **Purpose**: ITIL ensures that IT services are managed efficiently, supporting availability, reliability, and security in digital operations.
- **Application in Digital and Cyber Safety**: ITIL principles help Whānau Manaaki manage service requests, resolve security incidents efficiently, and standardize processes such as device management and software updates. It ensures that cybersecurity incidents are handled promptly and that all technology use supports educational and operational needs.

Alignment with Whānau Manaaki Digital and Cyber Safety Policy

By integrating COBIT, NIST, and ITIL, Whānau Manaaki ensures that:

- Technology is used responsibly to support tamariki learning and operations.
- Cybersecurity risks are actively managed, with a clear incident response process.
- Staff follow approved digital security measures, including data protection, access control, and software management.
- Digital governance remains adaptable and continuously improves to meet evolving security threats and operational needs.