Peke Waihanga
Artificial Limb Service

Orthotic Service

Information Protection Policy

Function: Operations National
Approved on: 20 January 2023

Business Activity: Privacy & informed consent
Version No: 1.0

Table of Contents

1. Background 2
2. Purpose 2
3. Scope 2
4. Definitions 2
5. Key documents related to information security 3
6. Key Policy Statements 4
7. Staff IT access, training and support 5
8. Physical security systems 7
9. IT security systems 7
10. Safeguarding patient information 10
11. Safeguarding employee information 12
12. Safeguarding financial information 13
13. Managing Data Breaches 14
14. Specific Responsibilities 14
15. Legal Compliance 15
16. Key Related Documents 16
17. References 16

Appendix A: Key websites, applications and platforms 17

1. Background

1.1. Peke Waihanga holds personal information relating to employees, patients, suppliers, and other organisations it needs to successfully provide its health services. It is required by law to have reasonable security mechanisms in place to ensure this information is secure against misuse including loss, access, use, modification, or disclosure except for lawful purpose.

1.2. Peke Waihanga has a duty to safeguard the confidential, business/commercial and proprietary information it holds where misuse of that information may harm the organisation, its staff or patients.

1.3. Peke Waihanga is seriously committed to the protection of the privacy and confidentiality of its employees, patients, volunteers, suppliers and others with whom it comes into contact. It understands they need to be assured that their data will not be used for any improper purpose or fall into the hands of a third party that has no right or authority to that information.

1.4. It is vital that all electronic devices connecting to the Peke Waihanga network are secure and that Peke Waihanga information remains protected.

2. Purpose

The purpose of this document is to describe Peke Waihanga policy in safeguarding the information it holds against unauthorised access, use, modification, disclosure or loss or other misuse.

3. Scope

3.1. This policy applies to all Peke Waihanga employees, volunteers, independent contractors (who hold Peke Waihanga information), and board members.

3.2. This policy covers the protection of both soft copy (digitalised) information and hard copy (physical) information held by Peke Waihanga

4. Definitions

General definitions

Data - information (especially facts or numbers) that is collected to be categorised, analysed, and/or used to help decision-making. Computer Data is data which can be processed by a computer.

Data / Information breach – A data or privacy breach is the result of unauthorised access to or collection, use or disclosure of information – particularly personal and health information.

Data / Information security - the practice of protecting information from unauthorised access, modification, use, or disclosure, loss or other misuse during its entire lifecycle.

Electronic device - a device which is used for audio, video, or text communication or any other type of computer or computer-like instrument including: a smart (mobile) phone, a laptop and a tablet.

Information Technology (IT) –Peke Waihanga's information technology and communication system includes all computing, audio visual, data network, telecommunication and other communications systems, their storage media and peripheral devices. The system includes use of internet, intranet (Whiria), email, telephone and voicemail systems.

Logical access controls - also called technical controls, these use software and data to monitor and control access to information and computing systems. Examples of logical controls are passwords, network firewalls, access control lists and data encryption.

Multifactor authentication (MFA) - a security process used to confirm users should be given access to Peke Waihanga apps, networks and data and which uses authentication methods beyond just entering a password. At Peke Waihanga, one log in at the start of the day also allows access to apps such as Teams, email, network drives, Whiria, Sharepoint resource library, etc.

Information definitions

Business/Commercial Information - means all information relating to Peke Waihanga business matters, including but not limited to:

- contracts, confidential operations, policies, processes or dealings, including any confidential incident reviews or other reports
- any information concerning the organisation, business, finances, transactions or Peke Waihanga affairs of services or Centres; and
- any data that has been deemed commercial in confidence by the Chief Executive Officer.

Confidential Information - information which any party with ownership or knowledge of that information wants to keep secret. This can include business, health, and personal information.

Health Information - in the Health Information Privacy Code defined to mean:

- information about the health of an individual, including his or her medical history; or
- information about any disabilities an individual has, or has had; or
- information about any health services or disability services that are being provided, or have been provided, to an individual; or
- information provided by an individual in connection with the donation, by that individual, of any body part or any bodily substance of that individual or derived from the testing or examination of any body part, or any bodily substance of that individual; or
- information about an individual which is collected before or in the course of, and incidental to, the provision of any health service or disability service to that individual.

Official information - means any information held by Peke Waihanga in any format.

Personal information - any information about an identifiable individual.

5. Key documents related to information security

5.1. Peke Waihanga has a suite of policies and procedures which support the implementation of this Information Security Policy. These key documents and their content are (see also Section 16 for list of all Key Related Documents):

- Privacy Policy – how Peke Waihanga and its employees meet the requirements of the Privacy Act 2020 in relation to storing, managing, using and disclosing identifiable patient and employee personal and health information. Includes managing a privacy breach or complaint.
- Information Request Policy – the proper information processes to be followed when a request for information is received to ensure the organisation meets the information disclosure requirements of the Privacy Act 2020 and Official Information Act 1982.

- Clinical Record Procedure – procedures for managing patient records (both digitalised on Manaaki) and hard, physical copies.
- Information Technology (IT) Users' Procedure – responsibilities and the procedures Peke Waihanga system users should follow when they are accessing and using IT to safeguard the information Peke Waihanga holds. This includes when users are:
    - Online (using the internet, Whiria and Teams)
    - Using social media
    - Emailing
    - Using Peke Waihanga devices (including laptops and desktop computers, tablets, smartphones (mobile phones) and any other devices) in the course of their work for Peke Waihanga
- Record Management Policy – describes how Peke Waihanga manages information efficiently and systematically.
- Staff Access to IT Procedure – describes the processes followed to reduce the risk from unauthorised access to Peke Waihanga data by regulating staff access to Peke Waihanga information technology systems.
- Telehealth Clinical Consultations Procedure – includes how to ensure patient information is protected during telehealth consultations.
- ICT Disaster Recovery Plan – includes Peke Waihanga procedures for protecting against loss of digitalised information during local and national civil emergencies/disasters.

6. Key Policy Statements

6.1. Peke Waihanga will implement reasonable security safeguards to protect against unauthorised access, use, modification or disclosure, loss or other misuse of information held by Peke Waihanga.

6.2. All information stored on electronic devices operated by Peke Waihanga, or on its behalf, is the property of Peke Waihanga. This includes material stored on desktop computers or portable devices supplied by Peke Waihanga and any material which may have been created for personal use by employees but has been stored on a Peke Waihanga system and/or device.

6.3. Information protection is always the responsibility of all employees and Board members. (See Section 10 Specific Responsibilities for responsibilities for different roles).

6.4. Personal and health information records (both patient and employee) may only be accessed by authorised employees and only for the purposes of providing Peke Waihanga services to patients. (See Privacy Policy for more information)

6.5. IT componentry, devices and other equipment are to be used only by approved personnel for approved Peke Waihanga work.

6.6. Peke Waihanga will only disclose personal or health information, or information that is commercially sensitive, if permitted or required under the Privacy Act, Health Information Privacy Code, Health Act or any other law. This includes to third parties and under Peke Waihanga agreements with funders. The Privacy and Complaints Officer must be notified of any request for information from government agencies or the police.

6.7. Information which does not identify any individual may be used in a general way by Peke Waihanga to provide statistical data. All requests for data not already published on the Peke Waihanga website needs to be approved for use by the Privacy and Complaints Officer or Chief Executive Officer.

6.8. All requests for statistical data are to be directed to the Privacy and Complaints Officer or Chief Executive. (See Privacy Policy for full details)

6.9. Peke Waihanga employees must not disclose confidential or proprietary information, or personally identifying information of any Peke Waihanga staff, volunteers, or patients, in online postings or publications. Employees who wish to post any social media site content relevant to Peke Waihanga may only do so in consultation with the Chief Executive Officer. (See Information Technology (IT) Users' Procedure for details on how to safeguard information and privacy when publishing online (e.g., on social media.))

6.10. Employees do not discuss any aspect of their work with people outside of Peke Waihanga to prevent individuals being identified, the unauthorised disclosure of their information or their privacy being breached.

6.11. Peke Waihanga will provide information and training to staff (both at induction and during ongoing professional development) and to other users of its IT systems to ensure they are data security aware, and that their online behaviour and electronic device use does not result in misuse of Peke Waihanga information. (See Section 7.8 - **Error! Reference source not found.**)

6.12. Any data or privacy breach is considered a serious matter. Peke Waihanga has a Privacy and Complaints Officer who is responsible for managing the response to data or privacy breaches. All breaches (actual and potential) must be reported to the Privacy and Complaints Officer without delay. (See Privacy Policy for full details)

6.13. It is considered serious misconduct for employees, contractors, board members or volunteers to breach Peke Waihanga procedures that apply in respect of safeguarding the information it holds. Violations may be deemed to be in breach of an employee's agreement and lead to disciplinary action. (See Discipline and Misconduct Policy)

6.14. Peke Waihanga uses physical access controls (e.g., keys and alarms) and security processes to protect against unauthorised access to its premises and so prevent the theft or opportunistic sighting of both digitalised and hard copies of the information it holds.

6.15. Peke Waihanga has backup procedures for all information held electronically to protect against the loss of its data. Employees involved in any element of back up data must comply with the backup procedures in a timely manner. (See Section 9.5 - 9.15 for back-up processes)

7. Staff IT access, training and support

Staff access to IT systems

7.1. Staff access to Peke Waihanga IT systems is provided and managed by National Office following requests for access from managers of new staff.

7.2. The processes described in the Staff Access to IT Procedure are followed when onboarding new staff and giving them access to Peke Waihanga IT systems, changing any access during their employment and when offboarding departing staff.

7.3. Multifactor Authentication is used as a security process to confirm users should be given access to Peke Waihanga apps, networks and data.

7.4. During onboarding all new Peke Waihanga staff are added to the staff directory, issued any electronic devices required for their work and given access to the following Peke Waihanga IT systems:

- Telephone system
- Microsoft Teams
- Outlook email and calendar system

- Pūmanawa
- Whiria
- Appropriate Peke Waihanga Sharepoint Libraries depending on their role
- Appropriate centre shared drives and folders depending on the Centre they are working from
- Appropriate national drives and folders depending on their role

7.5. Depending on each staff member's role, they may also be given access to any of the following if requested by their managers:

- Manaaki
- Exonet
- Third-party applications – My ACC Portal; DHB Patient Management Systems

7.6. Departing staff access to Peke Waihanga IT systems is disabled by National Office following the request of their managers.

7.7. Managers ensure that departing staff return all devices, key and swipe cards previously held by them to Peke Waihanga.

Staff IT systems training

7.8. During onboarding new staff receive training from their manager/supervisor to ensure staff competency when using the following:

- Telephone system – phone numbers, making outside calls
- Passwords and security
- Microsoft Teams
- Outlook – email and calendar system
- Whiria – communications via Whiria, links to health and safety, links to Resource Library and Learning hub
- Procedures to follow when staff are accessing and using the Peke Waihanga IT system including:
    - When they are online (using the internet, Whiria and Teams)
    - Emailing
    - Using Peke Waihanga devices (including laptops and desktop computers, tablets, smartphones (mobile phones) and any other devices) in the course of their work for Peke Waihanga

7.9. During onboarding new staff who have been given access to Manaaki (Peke Waihanga patient information management system) are given training to use Manaaki in a way that safeguards information from misuse. (See Employee Induction Follow-up Checklist for learning outcomes for Manaaki training.)

7.10. During onboarding new staff are expected to read Peke Waihanga Policy Summaries for New Staff (which includes expectations regarding safeguarding Peke Waihanga information) and to read the Privacy Policy and the Information Technology (IT) Users' Procedure. Assignment and completion of these tasks is tracked through Pūmanawa.

7.11. New staff are not given access to Peke Waihanga IT systems unless they have signed their employment agreement which states they accept Peke Waihanga policies and procedures (this means they are agreeing to requirements covering their use of Peke Waihanga information systems).

7.12. Staff access to Peke Waihanga IT systems can be revoked at any time.

Staff IT support

7.13. Staff are provided with IT support from National Office through the itsupport@nzals.co.nz email and also from its external IT systems and service provider Redstripe.

Staff personal use of internet and email

7.14. Peke Waihanga allows some personal use of the internet and email as long as use is reasonable and does not endanger Peke Waihanga information security. See Information Technology (IT) Users' Procedure for what constitutes reasonable and unacceptable use of internet and email.

8. Physical security systems

8.1. Each centre has one or more of the following physical security controls:

- A monitored alarm system which covers entrances and internal spaces within the buildings and should be activated whenever the building is unoccupied.
- A security patrol to monitor the premises on a regular basis through regular inspections outside of business hours.
- External lighting to sufficiently illuminate the building and the surrounding area at night.

8.2. To assist securing Peke Waihanga' assets and information:

- The premises, filing cabinets and stores are locked and all windows closed at the end of working hours with only authorised personnel as key holders.
- Key holders are registered with the alarm monitoring firm or security personnel.
- Componentry, equipment and information are not left out unattended in public areas
- Authorised personnel only have access to National Office computers, central files and physical records.

9. IT security systems[1]

9.1. The following security safeguards are in place for the websites, applications and platforms used at Peke Waihanga (see Appendix A for a list of these):

- Malware protection: Office 365 malware filtering; up-to-date anti malware (ESET) software on terminal service and all devices
- Terminal server can only be modified by IT support provider
- IT users' policy which cautions users against opening certain higher risk websites
- An Intellium (Broadband provider) firewall
- Logical access controls at all levels (e.g., network, server driver, folders, file, applications) to monitor and control access to information and computing systems.

[1] Peke Waihanga has two Servers – one located in Wellington and one in Auckland - which support its IT needs. These two Physical Hyper-V Servers are running 5 Virtual Machines. The first Hyper-VServer (ALSHV02) runs a Virtual Machine which supports Active Directory (AD), GPO, DNS, DHCP, Print Services and a File Server. There is a Second Virtual Server running SQL for Manaaki and Exonet and a final Virtual Machine running the VOIP PBX. The Second Hyper-V Host (ALSHV01) runs Two Virtual RDS along with a separate RDS gateway Broker.

9.2. Employees must not open any email that looks like it is spam, and if unsure must check with IT support.

9.3. If an employee is using the internet and believes that a file has been inadvertently downloaded, they must report this to the IT support team.

9.4. All Peke Waihanga computers run operating system and antivirus updates. Employees must allow the operating system and antivirus system updates to run on their computer or devices.

Data loss prevention and backup processes

Backup processes

9.5. The Auckland Server runs a Virtual Machine that replicates Live AD and DNS along with a backup copy of the business files. In addition to this, all of the Wellington Virtual Machines are replicated in a stood down state to the Auckland Server, excluding the PBX.

9.6. If the primary server's is unavailable (due to disruption), the AD and DNS roles are automatically switched to the Auckland centre. A replicated virtual server is stood up and the required network changes made to allow them to be available to Peke Waihanga Staff either remotely or from other centres

9.7. Peke Waihanga utilises Voice Over Internet Protocol (VOIP) in all centres and National Office as the primary means of telecommunication. If the Wellington Server is unavailable, then VOIP is temporarily disrupted. As the VOIP Trunks are cloud based, Trunks can be redirected to other centres if required.

9.8. Every 24 hours - the Wellington servers are replicated to Auckland in real time as changes occur this happens 24/7. This is managed by Peke Waihanga' external IT systems provider.

9.9. Every 24 hours, incremental file backups are done every 180 minutes Monday through to Friday. On Sunday a full backup is completed. These backups are stored on the Auckland Hyper-V Host. They are encrypted in transit and at rest. Four full Image sets are retained at any one time.

9.10. Weekly a full file backup is completed to a NAS located in the Wellington National Office. This backup is encrypted in transit and at rest as well. Ten full Image sets are retained at any one time.

9.11. Manaaki and Exonet databases are backed up daily with two copies retained, this is alongside the full replication of the Server to Auckland

9.12. Peke Waihanga Smartsheets are backed up weekly. The backup file is emailed to a Smartsheet administrator and they download them into G:\Backup- Smartsheets.

9.13. The agreed backup strategy chosen is for a fully mirrored recovery site at all Peke Waihanga facilities. This strategy entails the maintenance of a fully mirrored duplicate site which will enable instantaneous switching between the live site (headquarters) and the backup site.

9.14. When data is backed up, a new file is created, which holds a copy of the data. The backups must be regularly tested to ensure they are effective. Backups must be tested on a regular basis, by:

- Restoring the system from a backup to test the entire backup, or
- Restoring the data from a single database to test part of the backup, or
- Recovery to independent hardware to prove the Peke Waihanga can be recovered to disparate hardware if required, or
- Annual offsite recovery test to prove critical services can be recovered to an offsite location.

9.15. Nightly backups of Peke Waihanga routers' configuration are taken and collected in a Data Centre (DC) server. Respective of Intellium's Data Centres, the Christchurch DC provider is backup to the central Auckland DC provider(s). The Auckland connections are two-fold. One peering with two

peers provides internal backup. Other peering with a single peer is primary internet. Service Level Agreements (SLAs) for return to service exist with primary Internet upstream provider. Routing failover to Christchurch will occur if Auckland fails. Failover is tested annually. In the event of a primary connection failing, the cutover to secondary is automatic. All but Tauranga have a primary and secondary connection.

Electronic device security

9.16. Peke Waihanga will take all reasonable precautions to ensure all devices connected to its network are secure and that the information it holds remains protected.

9.17. All hardware has an asset number and is registered under the employee's name as the user and employee responsible for it while they are employed with Peke Waihanga.

9.18. All Peke Waihanga devices must be pin protected or protected with a complex password (i.e., with a minimum of 10 characters made up of at least six letters (one capital, and either four numbers or symbols)).

9.19. Employees must not disclose their password to anybody except for shared user accounts (with those internal users who share these accounts).

9.20. Passwords must be changed every 90 days. The centre IT delegate is responsible for changing user account passwords.

9.21. There is a requirement for staff to lock computer access and an automatic lock of computers is activated when not in use (after 15 minutes).

9.22. Users of Peke Waihanga devices connected to the Peke Waihanga network will allow for any use to be monitored and recorded on their device.

9.23. Personal devices are only permitted to access the Peke Waihanga servers via VPN and to access Peke Waihanga webmail.

9.24. Under no circumstances may hardware provided to an employee by Peke Waihanga be used by other people.

9.25. When the hardware becomes 'end of life' employees must return it to the IT support team so that it can be cleaned/erased. If an employee wishes to purchase the equipment, this can only happen after the hardware has been wiped and has gone through the established open bid process.

9.26. If necessary, a laptop will be provided to the employee in preference to the employee undertaking Peke Waihanga work on a home machine.

See Information Technology (IT) Users' Procedure for full information about user responsibilities for keeping electronic devices secure.

Safeguarding information when working from home

9.27. When working from home, staff must understand and following the organisation's policies and procedures to safeguard information. See Information Technology (IT) Users' Procedure and Telehealth Clinical Consultations Procedure for full details on users' responsibilities.

9.28. Employees using home computers must protect unauthorised access to Peke Waihanga information by other users of the computer.

9.29. Employees must not allow their computer system to remember their password.

9.30. All home wireless units must be secured with encryption enabled and passwords to authenticate users.

9.31. If an employee is unable to provide antivirus software for their home device, they must advise the IT support team who will provide them with a licence (for as long as they are employed by Peke Waihanga).

10. Safeguarding patient information

10.1. Staff must follow the procedures in the Information Technology (IT) Users' Procedure to safeguard patient privacy and information.

10.2. All information about patients collected and held by Peke Waihanga while providing services to the patient, including, information required for prescriptions, manufacture, fitting and rehabilitation services, is health information under the Health Information Privacy Code.

10.3. A patient's health information may only be accessed by employees while providing services to the patient.

10.4. Consent must be obtained from the patient prior to any patient photography.

See Privacy Policy for full policy details on disclosing patient information.

Management of patient records

10.5. Patient records must be established and managed as per the Clinical Record Procedure and Record Management Policy. Main points relating to patient information protection are:

- A patient's record is established on Manaaki when a patient is first referred to Peke Waihanga and does not already have an existing record.
- Each patient only has one record.
- Only approved Peke Waihanga forms recording patient care are used.
- Entries to patient records may only be made by persons with authorised access to record.
- Every consultation or episode of care must be recorded within 24 hours after it has occurred, by the attending clinician and include all relevant information.
- Every record must be legible, dated and signed (or electronic authorship established).
- Records must not be erased but may be amended if made in error.
- Records and any supplementary paper records are stored in places that are clean, secure, readily accessible to authorised users but inaccessible to unauthorised people.

10.6. Peke Waihanga also has obligations in relation to the retention of all records held by Peke Waihanga (including patient records) under the Public Records Act. See Record Management Policy.

10.7. Before any patients' health information or clinical records are destroyed, transferred to another provider, or removed from Peke Waihanga by any means the Privacy Officer must be informed. If a patient's record is transferred to another provider, this should be done via registered mail or other secure means (not ordinary post). A copy of the record must be retained by Peke Waihanga for subsequent reference.

10.8. Health information held by Peke Waihanga continues to be covered by Rule 11 of the Health Information Privacy Code for 20 years following the death of a patient See Record Management Policy for procedure for managing deceased and inactive patients.

10.9. All digitalised patient documentation is held under the patient's name in Manaaki document manager.

10.10. All hard copies of identifiable patient data are safeguarded from misuse and not left lying around unattended, this includes never leaving information unattended in vehicles. When not in use patient data in the workplace is stored in locked filing cabinets with access to keys limited to those employees who require them for their work. Access to keys is overseen by regional managers.

10.11. Staff log out of Manaaki and do not leave digitilised patient information open on unattended electronic devices.

10.12. Any identifiable patient information held on any mobile device must be removed from that device as soon as it is no longer required to be held on that device. **No identifiable patient data is stored on any personal mobile or home devices nor are they ever used to obtain identifiable patient information.**

10.13. Where Peke Waihanga mobile devices are used they should be connected to Peke Waihanga services where the information used on the device will be held. **No personal mobile devices are connected to the Peke Waihanga It network.**

10.14. In general, patient information should not be kept on a USB key or portable hard drive unless it has been encrypted, or as otherwise agreed by the Privacy and Complaints Officer. **No personal or online shared drives or USB keys are used to store patient files.**

10.15. Where patient information (for instance an X-ray) is brought into a clinic on a USB or other portable device by a patient or health practitioner for viewing at a Peke Waihanga Centre, the USB or other portable device may only be viewed on a Smart TV.

See Clinical Record Procedure for more details about managing patient records.

Safe handling and transfer of patient information

10.16. Peke Waihanga has clear procedures regarding the transfer (both digitalised and physical copies) of patient information and files and ensures staff understand these procedures and the consequences for not following them.

10.17. The Information Technology (IT) Users' Procedure details procedures for emailing or transferring patient files or data. Main points are:

- Sending documents by email or courier are the only accepted methods for transferring or sharing identifiable patient's health information with service providers and funders. Faxing is not acceptable.
- When sending health information by email to funders and other health services, a new email is started where practical, and the relevant information inserted into it.
- No personal or online shared drives (such as Dropbox and Skydrive) or USB keys are used to transfer patient files.
- If for any reason any employee needs to take any printed material containing personal or health information home, the employee must ensure this is registered with the Privacy and Complaints Officer and advise when it will be returned. Where possible, in preference to taking printed personal or health information home, any material should be scanned and accessed remotely.

Safeguarding patient information during telehealth consultations

10.18. Transmissions through software platforms for telehealth consultations are encrypted. Microsoft Teams is provided by Peke Waihanga as the preferred platform for telehealth consultations. Zoom can also be used for telehealth consultations. Microsoft Teams uses several privacy and security controls including data encryption. Zoom meetings are encrypted during transmission and the overall risk of interception is considered to be very low by the New Zealand Telehealth Resource Centre.

10.19. Clinicians take the following precautions to maximise the privacy of patients and safeguard their information:

- Telehealth sessions are delivered from a private space

- Clinicians wear headphones
- Clinicians confirm the identity of the patient using three identifiers and confirm that they are currently in New Zealand
- Clinicians inform the patient the telehealth consultation will not be recorded unless both parties' consent. File sharing features cannot be used in the session.

10.20. Patients have a right to record their own telehealth consultations but if they do want to record, staff should explain they can only use the information for their own purposes and for referral purposes later, they cannot share the recording on social media or put in the public domain. See Section 6.10 – 6.14 of the Privacy Policy.

See Telehealth Clinical Consultations Procedure for full details.

11. Safeguarding employee information

11.1. Employee information is mostly digitalised and kept on Peke Waihanga's main server. If hard copies of employee information are received, it is scanned, and the hard copy destroyed as soon as possible.

11.2. Access to employee data is protected and is limited to specified employees.

11.3. All spreadsheets and files with employee information are held in folders which restrict access and files are password protected. Folders with the information are only accessible by persons with either administration access to the servicers or to administration personnel authorised to access company personnel records.

11.4. The payroll system is password protected and the CEO, CFO, Accountant, HR Manager and Finance & Payroll Administrator have a unique password to access the system.

11.5. Employee data is kept for as long as the person is employed by Peke Waihanga then is archived for at least seven years from their last date of employment (reference Archives NZ General Disposal Authority 7: Facilitative, transitory and/or short-term value records (2013) - section 3.0.0 Human Resources Management). After this it is then deleted/securely destroyed in line with Peke Waihanga' obligations under the Privacy Act 2020 and the Public Records Act 2005.

11.6. Employee data will not be given to any third parties without written permission from the employee unless the information sharing is:

- Expressly permitted or required by legislation
- Permitted by an exception in the Privacy Act (see s6 principles 10 and 11)
- Permitted by an 'Approved Information Sharing Agreement' under Part 9A of the Privacy Act.

11.7. Personal information about employees is collected and held by Peke Waihanga to maintain proper employment records in order to comply with legislative requirements and for Peke Waihanga' own lawful use. This includes information required for salary records, leave entitlements and to pay employees, tax purposes, health and safety purposes, and to meet other legal obligations relating to the employee's employment.

11.8. Peke Waihanga requires the following information to be held on an employee's personnel file. The list is not exhaustive, and other information may also be held:

- Letter of appointment, job description, employment agreement, personal details including emergency contact, bank details and driver's licence details if role requires it
- Completed induction forms
- Salary related documents addressed to employee (salary review, IRD PAYE, Kiwi Saver, Superannuation, deductions for PSA or other)

- Employment amendments/variations including change in working hours, salary reviews, updated employment agreements
- Terms and conditions of employment, including signed declarations agreeing to abide by Peke Waihanga policies and procedures (including Code of Conduct Policy and IT Users procedures)
- Completed induction checklists
- CV and cover letter
- Personal development documentation
- Performance management notes and/or warnings including misconduct warnings
- Leave documentation
- Immigration documentation - copies of work permits, residency permits, and if granted citizenship certificate
- Workplace health and safety relate, i.e., ACC forms
- Specific correspondence from employee with appropriate responses from Peke Waihanga

11.9. Examples of information that should not normally be placed in the employee's personnel file include:

- General day-to-day email correspondence about the employee, i.e., between Regional Manager and CEO or CFO. Exceptions will apply e.g., management of extended absences due to injury or sickness
- Feedback from other employees
- Documentation to National Office about employee, e.g., for salary increase request or in reports
- Investigation documentation into allegations of misconduct after investigation completed. This information is kept in National Office files only
- Employee documentation that includes other employees' information, e.g., emails to payroll re employees' changes to pay or leave
- Other employees' documentation.

11.10. Employees may ask to review or update the personal information that Peke Waihanga holds about them at any time. If the request relates to pay, leave, or other day-to-day employment matters the request should be forwarded to the Finance and Payroll Administrator. Any other request, or a request to correct information held about the employee should be treated as a request under Principle 6 or 7 of the Privacy Act and all such requests must be forwarded to the Privacy and Complaints Officer. See the Privacy Policy for full details

11.11. See Recruitment and Selection Policy, Section 8 for details about protecting the privacy and information of job applications.

12. Safeguarding financial information

12.1. Financial and credit card information is used to obtain payment for goods and services ordered from Peke Waihanga. Peke Waihanga does not use the information obtained for payment for goods and services for any other purpose unless legally permitted or required to do so. Peke Waihanga only holds this information for as long as it is required to process a payment or to meet any other legal requirements, including under the Public Records Act 2005.

Safeguarding supplier information

12.2. Peke Waihanga does not use the information obtained for payment for goods and services it is purchasing for any other purpose unless legally permitted or required to do so. Peke Waihanga only holds this information for as long as it is required to process a payment or to meet any other legal requirements, including under the Public Records Act 2005.

12.3. Peke Waihanga will protect supplier's confidential or commercially sensitive information. This includes information that could compromise fair competition between suppliers. A supplier's confidential or commercially sensitive information will only be disclosed if:

- The supplier has already agreed to the disclosure in writing (email is fine); or
- The disclosure is permitted or required by law (e.g., under the Official Information Act, or any other Act or Regulation); or
- It is a limited disclosure expressly notified in a Notice of Procurement which suppliers have consented to by participating in the process

See Information Technology (IT) Users' Procedure employee's responsibilities for safeguarding supplier information.

13. Managing Data Breaches

13.1. The Privacy and Complaints Officer is responsible for managing the response to all data or privacy breaches. Any data or privacy breach is considered a serious matter. Refer to Section 16 of the Privacy Policy for details on managing data or privacy breaches.

14. Specific Responsibilities

Party	Responsibilities
All Employees	• Ensures a knowledge and understanding of their obligations under this policy and related information security policies and procedures including regarding use of the internet, email and electronic devices. • Reports lost or stolen Peke Waihanga devices in their possession • Immediately notifies IT that their device is compromised with a virus
Regional Manager/ Team Leader	Ensures: • appropriate security of physical records containing personal or health information • disposal of records, in conjunction with the Privacy and Complaints Officer, in compliance with the Public Records Act when no longer required to be held by Peke Waihanga. • employees are trained in and aware of their obligations under this Policy.
Privacy Officer	• Authorises release of statistical data, extraction of data for specific purposes. • Grants permission for transfer of data to USB or portable hard drive.

Party	Responsibilities
	• Maintains register for physical files removed from premises for working from home. • Coordinates response to requests for disclosure of personal or health information, or commercially sensitive information. • Coordinates Peke Waihanga' response to any data breach.
IT Delegates	Maintain passwords for shared user accounts.
IT Support team	Supports users including for password resets, responding to reports of suspicious content, wiping of hardware devices at end of life.
CEO	• Ensures Peke Waihanga complies with its legal obligations in relation to data security, has a fit for purpose Information Protection Policy, and employees are aware of their obligations under the Policy. • Reports any data or privacy breaches to the Board and determines whether the Office of the Privacy Commissioner should be notified. • Authorises the release of statistical data approved by the Privacy and Complaints Officer
Board Members	• Endorses this policy • Under s57 of the Crown Entities Act a Peke Waihanga Board member who has information in his or her capacity as a member that would not otherwise be available to him or her must not disclose that information to any person, or make use of, or act on, that information, 'except' a) When performing a function for Peke Waihanga; or b) As required or permitted by law; or c) In accordance with paragraph below: or d) In complying with the requirements for members to disclose interests. • A member may disclose, make use of, or act on information if: a) The member is first authorised to do so by the Board; and b) The disclosure, use, or act in question will not, or will be unlikely to, prejudice Peke Waihanga.

15. Legal Compliance

- Crown Entities Act 2004
- Health Information Privacy Code 2020
- Health Act 1956
- Health (Retention of Health Information) Regulations 1996
- Health and Disability Commissioner Act 1994
- Health and Disability Services Consumers' Rights 1996 (Code)
- Official Information Act 1982
- Privacy Act 2020

- Public Records Act 2005
- State Services Commission Code of Practice

16. Key Related Documents

- Clinical Record Procedure
- Code of Conduct Policy
- Communications Policy
- Discipline and Misconduct Policy
- Informed Consent Policy
- Employee Induction Checklist
- Employee Induction Follow-up Checklist
- ICT Disaster Recovery Plan
- Information Request Policy
- Information Technology (IT) Users' Procedure
- Multifactor Authentication (MFA) Guide
- Onboard or change to Staff Access to Information Technology Form
- Offboarding Staff Access to Information Technology Form
- Policy Summaries for New Staff
- Privacy and Informed Consent Conversation Procedures
- Privacy Policy
- Privacy Request Checklist.pdf
- Privacy Request Procedure.pdf
- Record Management Policy
- Recruitment and Selection Policy
- Recruitment and Onboarding Checklist
- Staff Access to IT Procedure
- Telehealth Clinical Consultations Procedure

17. References

- Archives NZ General Disposal Authority 6: Common corporate service public records (May 2013)
- Archives NZ General Disposal Authority 7: Facilitative, transitory and/or short-term value records (2013)
- New Zealand Telehealth Forum and Resource Centre

Appendix A: Key websites, applications and platforms

The following table outlines the key websites, applications and platforms used at Peke Waihanga:

Website/Application/Platform/ Service	Use/Comments
Microsoft Office 365 suite of products	Allows the use of Emails and Teams to be hosted in the Cloud
Mobile phones	Limited number of mobile phones predominantly used by Managers. Contracted with 2 Degrees
Centre toll free number, SIM cards for Safelife SOS Pendant Alarm	Managed by Vodafone. Safelife SOS Pendant Alarms are used by lone workers
Intellium	Broadband provider.
Manaaki	Patient management database. Managed by Very Impressive Software.
Peke Waihanga, Peer Support Service and Orthotic Services Waikato websites	Support for patients. Websites managed by Pikselin
Infoodle website	Manage peer support volunteer and recipient visits and information
Pūmanawa (ELMO recruitment software)	Recruitment, onboarding and HR management of employees. This is managed by ELMO
Cemplicity	Surveying satisfaction of patients accessing our services
IMS	Payroll and leave management
Exonet (MYOB Exo)	Account management including CRM, inventory management, job costing, fixed assets, analytics and reporting
VI Assets	Tracking assets and depreciation. Managed by Very Impressive Software.
Smartsheets	Recording and tracking example e.g., H&S, complaints, OIA, building works
Stellar Library	Board reporting
Orbit Travel	Online booking travel and accommodation
Physio Tools	Physiotherapy tools
Facebook, Twitter, Instagram and LinkedIn	Social media
EAP website	View number of people accessing EAP services
BowTieXP software	Create BowTie risk assessments

For Use by National Office Only

Document development and approval			
Review period	3 years	Next review date	January 2026
Legal review required?	✓	Board approval required?	✓
Interconnected processes and documents affected by this document?	Information Technology Users' Procedures Privacy Policy Clinical Records Procedure Record Management Policy		

Version history		
Version No.	Version Date	Description of Change
1.0	20 January 2023	Amalgamation of documents below into this new Information Protection Policy
Data Protection Policy		
3.4	July 2017	Amendments from Data Controller to Privacy and Complaints Officer, add CFO & Regional Manager. Updates to use of Fax and retention period for archiving employee data
3.3	April 2016	Changes to handling of health information
3.2	February 2016	Email exception for regional clinic
3.1	December 2015	Incorporation of feedback from Claro and updated branding
2.2	June 2015	Addition of a personal copy of the acknowledgment page

Authors and reviewers	
Content owner name and role	Claire Rumble, Policy and Quality Advisor
Content author(s)	Claire Rumble, Policy and Quality Advisor
Was there a review committee?	
Internal peer reviewer names and roles	Kate Livesey (Service Development Manager), Jeremy Speight (CF), Bari Chin (Cloud Solutions Specialist)
External reviewer names, organisations, and roles	
Tikanga consultant	

Implementation history	
✓ Internal communication ✓ Manager in-team training ☐ National roll-out via group workshops ☐ Self-learning: ☐ Other (describe)	**Roles affected:** All roles
Procurement, IT, or other budgetary considerations	
When updated, these people need to be notified	