Te Whatu Ora
Health New Zealand

Privacy Policy

Mā te kimi ka kite, Mā te kite ka mōhio, Mā te mōhio ka mārama.
Seek and discover. Discover and know. Know and become enlightened.

Purpose

1. This policy describes how Te Whatu Ora-Health New Zealand will collect, store, use, disclose, retain, and protect personal information, ensuring we meet the requirements of the Privacy Act 2020 and the Health Information Privacy Code (HIPC) 2020, and the spirit of the Data Protection and Use Policy (DPUP).

Context

2. Te Whatu Ora is entrusted with significant amounts of personal information (including health information). Personal information is a valuable asset that must be handled with care. Mishandling of personal information, or lack of transparency with how it is handled, can cause significant harm to individuals, and may result in widespread media interest and a loss of trust and confidence in the agency.

3. The Privacy Act 2020 sets out 13 Information Privacy Principles (IPPs) which cover the collection, storage, use and disclosure of personal information, and give people the right to access and correct their information. The HIPC 2020 is a code of practice that sets specific rules for agencies in health sector. These rules replace the IPPs for the health sector.

4. The DPUP is a Cabinet-endorsed policy which recommends good practice above and beyond the minimum legal requirements of the Privacy Act 2020. The policy comprises five principles, which articulate the values and behaviours that underpin the respectful and transparent use of data across the social sector.

Application

5. This policy applies to everyone in Te Whatu Ora National Office, including permanent, seconded, and temporary employees and contractors (referred to as our people).

6. For other parts of Te Whatu Ora, the corresponding policies that were in place before 1 July 2022 continue to apply until changed by the Board of Te Whatu Ora or its delegate.

Te Whatu Ora
Health New Zealand

Definitions

7. The following definitions are used for the purposes of this policy:

Health Information	"Health information" is a subset of personal information, where the information is about an identifiable individual's health. This includes information about their health or disabilities, their medical history, health or disability services provided to them, and information collected while providing health and disability services, such as addresses for billing purposes or information relevant to funding. Examples of health information are: clinical notes, genetic information, test results, diagnostic images, verbal discussion and records of conversations. This includes information about living individuals and can include information about deceased individuals.
Personal Information	"Personal information" means information about a living identifiable individual. This information can be in any form, including paper and electronic documents and files, emails, personnel records and patient records, and can include images such as photos, an image of a pathology report or a diagnostic image. It can also include video recordings and audio recordings. Examples of personal information include an individual's name, telephone number, address (email and postal), date of birth, ethnic origin, tax number and Health Information. Even if an individual's name does not appear in information, but there is a reasonable chance that an individual could be identified from the information (including where information can be combined with other information to identify a person), it can still be personal information for the purposes of the Privacy Act.

Privacy Breach	A "privacy breach" occurs when personal information held by Te Whatu Ora is accessed, disclosed, altered, lost or destroyed without authorisation or by accident, or when requests for access or correction to personal information are not processed in a timely manner. This includes internal misuse of information, such as browsing of personal information or inappropriate sharing of personal information with colleagues who have no work-related purpose to access it. A privacy breach may also be something that prevents Te Whatu Ora from accessing the information on a temporary or permanent basis.
Privacy Incident	A "privacy incident" is any incident that may be, or that could have led to, a privacy breach. This includes near misses. Examples include that personal would have been disclosed by accident but for security measures (e.g., password protection).
Te Whatu Ora National Office	a) Staff who are working in roles that would **not** have been District Health Board, Te Hiringa Hauora/Health Promotion Agency or Shared Services Agency roles under the previous health system (including all staff employed/engaged by Te Whatu Ora on or after 1 July 2022); and b) For operational policies other than employment policies, staff who have transferred from the Ministry of Health (MoH) under the Pae Ora (Healthy Futures) Act 2022 (Pae Ora Act)

Policy

8. Te Whatu Ora will only collect personal information where it is necessary for lawful purposes connected with its functions and activities under the Pae Ora Act.

Key Principles

Collection of personal/health information

9. Personal information must be collected from the individual who the information is about, or from another source with that individual's authority. Te Whatu Ora may collect information from a third party if permitted by law, for example, by one of the exceptions in the Privacy Act or HIPC (see IPP2 and rule 2 of the HIPC).

10. When collecting personal information, Te Whatu Ora commits to being transparent with the individual involved about why the information is being collected, who will receive it, whether collecting it is voluntary and what will happen if it is not collected, as well as informing them of their rights of access and correction.

11. Te Whatu Ora will only collect personal information in a way that is lawful, fair, open and transparent. This is particularly important when collecting information about a child, young person or vulnerable adult.

Storage and security of personal/health information

12. Te Whatu Ora is committed to taking all reasonable steps to ensure that personal information held about an individual is protected against loss, unauthorised access, misuse, modification or disclosure. This applies to information held in Te Whatu Ora's electronic systems and all personal information held in hard copy.

13. Appropriate security measures will depend on the sensitivity of information involved and potential consequences if it is not kept secure. Security steps may include having appropriate access controls and auditing processes, confirming the identify of an individual before releasing information to them, checking addresses (email or physical) before sending, use of password protection.

14. Electronic personal information must only be stored in approved Te Whatu Ora systems of record that have undergone appropriate information security testing and privacy risk assessment.

Access to and correction of personal information

15. Everyone has the right to access information about themselves. Te Whatu Ora will provide people with access to their personal information, in a timely manner, except in limited circumstances where a withholding ground applies.

16. Everyone has the right to request that information held about them is corrected. Te Whatu Ora will make such corrections by amending, deleting or adding information, if the request is reasonable and necessary to ensure accuracy. If Te Whatu Ora does not believe the information needs correcting, or is unable to make the requested changes, Te Whatu Ora will take reasonable steps to attach a statement of correction to ensure that the individual's views are read alongside the disputed information.

17. Te Whatu Ora will give reasonable assistance to the individual who wishes to access or correct their information, working with them to refine the scope of the request and resolve any concerns. Te Whatu Ora must not charge any individual for access to, or correction of, their personal information.

18. Te Whatu Ora will take reasonable steps to ensure that the person requesting access to or correction of information is that person or their approved representative. This verification may include viewing identification and/or answering security questions.

Retention of personal information

19. Te Whatu Ora will only keep personal information for as long as it is necessary for the purpose it was collected, or as long as is allowed or required by legislation (for example the Public Records Act 2005 and the Health (Retention of Health Information) Regulations 1996).

Use and disclosure of personal information

20. Te Whatu Ora will only use or disclose personal information for the same purposes for which it was collected, unless the individual has authorised a different use or disclosure, if permitted by law, for example by one of the exceptions in the Privacy Act or HIPC (see IPP10 and 11 and rules 10 and 11 of the HIPC), or another law requires disclosure.

21. Te Whatu Ora will take reasonable steps to check personal information before use or disclosure to ensure that it is accurate, up to date, complete, relevant, and not misleading. Where appropriate, this may include contacting the individual to confirm their address or other details.

22. Where using or disclosing personal information, Te Whatu Ora will take care to ensure that only the information necessary to fulfil the requirement is used/disclosed.

23. Te Whatu Ora will only disclose information overseas if the overseas recipient (a foreign person or entity) is subject to the Privacy Act 2020 or comparable privacy laws/safeguards, or if the individual involved authorises the disclosure after being expressly informed that the overseas recipient organisation may not be required to protect the information in a way that provides comparable safeguards to the Privacy Act 2020.

Unique Identifiers

24. Te Whatu Ora will only use unique identifiers where necessary, and in the context that they are created. Unique identifiers must not be used or shared for other reasons.

Staff information

25. Te Whatu Ora will ensure that the personal information of our people is treated with the utmost care and respect, in accordance with legislative requirements and this policy.

Information held by Te Whatu Ora as an agent

26. The Privacy Act provides that, if an agency holds information as an agent or to process the information for another agency, and does not disclose the information for its own purposes the information is deemed to be held by the agency on whose behalf the information is held. Te Whatu Ora must take that into account in relation to information that it holds on behalf of another agency. If, for example, Te Whatu Ora receives a request for such information, Te Whatu Ora will need to engage that agency on whose behalf Te Whatu Ora holds the information.

Privacy breaches

27. Te Whatu Ora has a clear process for reporting, managing and escalating privacy incidents, including privacy breaches and possible breaches.

28. Internal misuse of personal information by staff will be considered a privacy breach. This includes browsing or accessing information that they do not need to access, or sharing information with others who have no purpose to receive it.

29. Suspected or actual privacy incidents must be responded to immediately to minimise the harm to affected individuals. Being transparent, clear and open with the impacted individuals is critical to maintaining their trust.

30. Full reporting of all incidents provides Te Whatu Ora with an opportunity to improve processes or systems to avoid future breaches.

31. All breaches that have or are likely to cause 'serious harm' will be notified to the Office of the Privacy Commissioner and the affected individual as soon as practicable (unless one of the exceptions to the requirement to notify affected individuals in the Privacy Act applies). The notifications will include the information required by the Privacy Act.

32. When assessing whether a breach is likely to cause serious harm, Te Whatu Ora will consider actions taken by Te Whatu Ora to reduce the risk of harm, whether the information is sensitive, the nature of the harm that may be caused to affected individuals, who has or may have obtained information as a result of the breach, whether the information was protected by a security measure (e.g., a password), and any other relevant matters. In some case, it may be necessary to give public notice of a breach.

Privacy complaints

33. Te Whatu Ora has a clear process for escalating complaints about privacy or complaints alleging a breach of the Privacy Act 2020 or HIPC 2020 to the Te Whatu Ora Privacy Team. Te Whatu Ora will aim to work with individuals to resolve their concerns.

Privacy Impact Assessments

34. Te Whatu Ora has a clear process to assess privacy risk where a proposed project, policy, service change or facility design or build may affect the collection, storage, security, access, retention, use or disclosure of personal or health information.

35. Te Whatu Ora aims to embed privacy throughout the product or service lifecycle from design to disposal. Privacy risks and enhancements must be considered from the start of the project and the privacy assessment completed prior to implementation.

Privacy culture and training

36. Te Whatu Ora is committed to providing appropriate privacy training and support to all Te Whatu Ora staff. This includes a privacy learning module as part of all staff's mandatory learning, and availability of privacy advice from a dedicated privacy team

37. Privacy training will be regularly reviewed to ensure it is fit for purpose. Additional targeted training will be provided, as required, based on identified risks and trends.

Roles and Responsibilities

Te Whatu Ora Board	• Accountable to the Privacy Commissioner for Te Whatu Ora's performance in respect of the Privacy Act 2020 and this policy • Responsible for promoting a culture of openness and transparency, by championing positive engagement with privacy legislation and best practice
Chief Executive	• Responsible for promoting a culture of openness and transparency, by championing positive engagement with privacy legislation and best practice. Make clear regular statements to staff and stakeholders in support of the appropriate management of personal information and reminding staff of their obligations
Chief Information Officer	• Responsible for implementing security functions to ensure electronic personal information is adequately secured against loss and protected against unlawful access, misuse and disclosure
Privacy Officer	• Responsible for the Privacy Policy, strategy, and programme of work • Protects and promotes privacy by encouraging compliance with the Privacy Act 2020, HIPC and DPUP • Oversees external and internal communication and information sharing in the event of a privacy breach or incident • Manages external relationships with the Government Chief Privacy Officer and the Office of the Privacy Commissioner
Senior Leaders	• Responsible for promoting a culture of openness and transparency, by championing positive engagement with privacy legislation and best practice. Make clear regular statements to staff and stakeholders in support of the appropriate management of personal information and reminding staff of their obligations

Managers	• Responsible for promoting a culture of openness and transparency, by championing positive engagement with privacy legislation and best practice. Make clear regular statements to staff and stakeholders in support of the appropriate management of personal information and reminding staff of their obligations • Demonstrate clear knowledge and support for the Privacy Act and internal processes for managing personal information • Ensure staff complete internal training modules on privacy, and have access to internal guidance and tools • Ensure staff report all breaches or other privacy incidents through the privacy incident reporting process. Oversee and support staff's investigation into the cause of the breach and provide recommendations for remediation
Our people	• Understand and comply this policy, and related policies and procedures, when handling personal information • Manage personal information safely and with integrity, respecting others' information and being mindful when discussing personal information that this is appropriate and in the correct forum • Responsible for the identification, escalation and initial response to privacy breaches • Report all breaches or near misses through the privacy incident reporting process, as soon as they become aware of it. Where allocated, investigate the cause of the breach and provide recommendations for remediation

Non-compliance with policy

38. Failure by staff to fully comply with this policy may result in Te Whatu Ora taking disciplinary action in accordance with the Code of Conduct.

39. An individual is entitled to complain to the Office of the Privacy Commissioner if they consider that an action of Te Whatu Ora is an interference with their privacy. For an action to be an interference with privacy, there must have been a breach of one or more of the IPPS (or of an information sharing or matching agreement), or a failure to give notice of a privacy breach. The action must also have caused loss, detriment, damage, on injury to the individual, adversely affected (or may adversely affect) their rights, benefits, obligations, or interests, or resulted in (or may result in) significant humiliation, significant loss of dignity, or significant injury to the individual's feelings. The Privacy Commissioner may investigate

such complaints, may try to settle the complaint, and may refer complaints to the Director of Proceedings.

40. Failure to comply with the Privacy Act 2020 may result in Te Whatu Ora receiving a fine or compliance notice from the Office of the Privacy Commissioner.

Related Policies and Procedures

- Code of Conduct
- Information Management Policy
- Information Security and Acceptable Use of IT Policy
- Official Information Act Policy
- Use of Social Media Policy

Related Legislation

Privacy Act 2020

Health Information Privacy Code 2020

Official Information Act 1982

Public Records Act 2005

Public Service Act 2020

Health Act 1956

Health (Retention of Health Information) Regulations 1996

Family Violence Act 2018

Oranga Tamariki Act 1989

Related Guidance

Data Protection and Use Policy

HISO 10064:2017 Health Information Governance Guidelines

OWNER:	Governance, Partnerships and Risk
CONTACT:	Deborah Roche
ENDORSED:	July 2022
TO BE REVIEWED:	June 2023

Guidance for using this National Policy document

This policy offers a nationally consistent approach to comply with the Privacy Act 2020 and Health Information Privacy Code 2020.

This is not a legal instrument. District Health Boards may adopt this policy with or without alteration to fit their specific and local needs. All red text provides guidance on content to be captured within this document to support local application – this must be deleted prior to finalising this policy. Each district health board is responsible to ensure that local document approval processes are obtained for the review and approval of this policy.

This policy is approved by the majority of privacy, legal and quality advisors from all District Health Boards nationally, with input provided by the Office of the Privacy Commissioner, Government Chief Privacy Officer, Social Wellbeing Agency (Data Protection and Use Policy) and Ministry of Health.

KEY:

Guidelines to support local application of this policy are provided in red – delete once local content is provided

Examples are provided in blue text – these can be retained within the final document

Data Protection and Use Policy considerations are provided in green text

Hyperlinks to relevant websites, link to sections within this document and templates are highlighted in orange. Hyperlinks to the templates, saved on your local drive, need to be updated with the local network address.

Document Control

Version Control

Name	Date	Reason for Change	Version

Document Approvers/Sign offs

This may be email or physical signature, and represents acceptance of the content of this document. The follow key stakeholders have approved this document:

Title	Name	Signature	Date

Document References

This section contains a list of documents referenced to, or related to this document:

No	Title	Author	Version	Location

Contents

1. Introduction

1.1 Purpose

The purpose of this policy is to:

- Provide guidance and confirm our DHB's expectations about the management of personal and health information, including the collection, storage, use of, retention and destruction.
- Outline our requirements to comply with the Information Privacy Principles and Health Information Privacy Rules under the Privacy Act 2020 and Health Information Privacy Code 2020.
- Support DHB personnel in dealing with complaints and potential breaches of privacy.

1.2 Guiding Values

The following guiding values support this policy:

- Privacy is about managing and protecting personal and health information about an ***individual***. We are mindful of the trust relationship and respectful of our obligations as kaitiaki[1] and guardians of information we hold about individuals.
- Privacy is everyone's responsibility.
- When dealing with personal and health information it should be treated with the same care and respect as if it were our own.
- We have a transparent and open approach to managing personal and health information.
- We build privacy into the design and implementation of our facilities, services, processes and systems.
- We know, promote and comply with our legal, ethical and individual professional obligations.
- We acknowledge and incorporate the Data Protection and Use Policy values of *He tāngata; Manaakitanga; Mana whakahaere; Kaitiakitanga;* and *Mahitahitanga* into all privacy practices.

1.3 Scope

This policy applies to all DHB personnel handling personal and health information. DHB personnel must:

- Observe the legal requirements that govern the collection, security, access, retention, use and disclosure of personal and health information.
- Familiarise themselves with this policy, the associated procedures, the Privacy Act 2020, the Health Information Privacy Code 2020, privacy/confidentiality obligations in their employment/contractor agreements and policy by their professional registration body appropriate to their role.
- Read this policy alongside the associated procedures to support informed and good decision making.

1.4 Data Protection and Use Policy

This policy includes considerations from the Data Protection and Use Policy (DPUP). Take care that DPUP recommends good practice above and beyond the minimum legal requirements of the Privacy Act 2020. DHBs are not legally bound by DPUP but are encouraged to consider it when collecting, using and sharing information.

[1] (noun) trustee, minder, guard, custodian, guardian, caregiver, keeper, steward.

DPUP consists of five Principles[2]:

- ***He tāngata***- Focus on improving people's lives — individuals, children and young people, whānau, iwi, and communities
- ***Manaakitanga*** - Respect and uphold the mana and dignity of the people, whānau, communities or groups who share their data and information.
- ***Mana whakahaere*** - Empower people by giving them choice and enabling their access to, and use of, their data and information.
- ***Kaitiakitanga*** - Act as a steward in a way that is understood and trusted by New Zealanders.
- ***Mahitahitanga*** - Work as equals to create and share valuable knowledge.

DPUP has a collectively developed Toolkit containing more information for implementing DPUP available on their website.

2. Definitions

The table below sets out an agreed definition for terms in this policy and associated procedures.

Term	Definition
Data Protection and Use Policy	The Data Protection and Use Policy articulates what 'doing the right thing' looks like across the social sector in its collection and use of people's data and information. What personal data and information people share, who they share it with and how they share it matters. Building and maintaining trust is key. The policy comprises five principles, which articulate the values and behaviours that underpin the respectful and transparent use of data across the social sector. DPUP was developed by the social sector, for the social sector, after extensive and inclusive engagement with agencies, iwi and communities. For further information see the Social Wellbeing Agency's website here.
DHB personnel	"DHB personnel" means a person who carries out work for a district health board, including work as an employee, board member, contractor, subcontractor, employee of a contractor or subcontractor, an employee of a recruitment company who is assigned to work at a DHB, a trainee or student, a person gaining work experience or undertaking a work trial or a volunteer.
Health information	"Health information" means information about an identifiable individual's health. This includes information about their health or disabilities, their medical history, health or disability services provided to them, information about donating organs or blood and information collected while providing health and disability services, such as addresses for billing purposes or information relevant to funding. Examples of health information are: clinical notes, genetic information, test results, diagnostic images, verbal discussion and records of conversations. This includes information about both a living individual and a deceased individual.
Individual	An "individual" means a natural person, such as DHB personnel, a patient or a visitor.
Interference with privacy	An "interference with privacy" is an action that breaches an information privacy principle under the Privacy Act 2020 **and** harms or may harm an individual. The legislative definition is here.
Patient	"Patient" or "service user" means a person receiving health and disability services.
Personal information	"Personal information" means information about a living identifiable individual. This information can be in any form, including paper and electronic documents and files, emails, personnel records and patient records, and can include images such as photos, an image of a pathology report or a diagnostic image. It can also include video recordings, audio recordings. Examples of personal information include an individual's name, telephone number, address (email and postal), date of birth, ethnic origin, tax file number and Health Information.

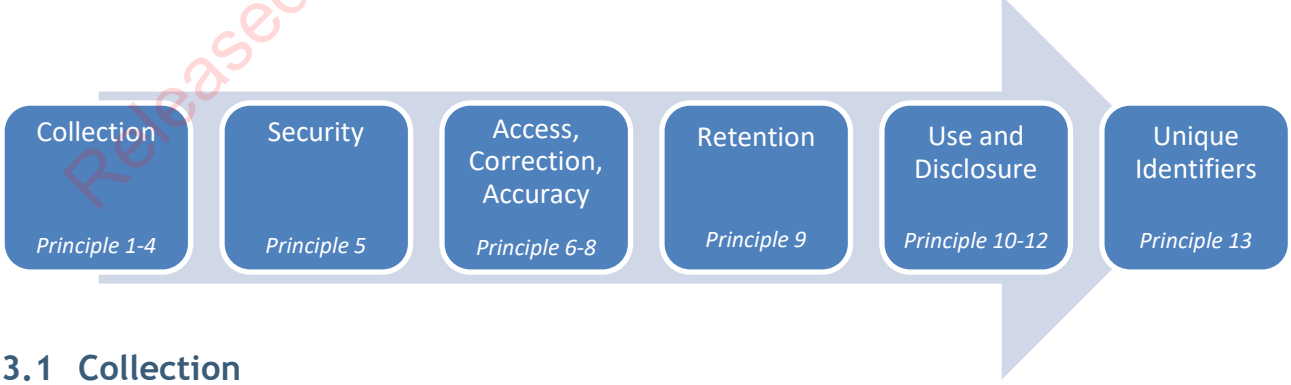
[2] Built upon, but separate to the Information Privacy Principles in the Privacy Act 2020

Term	Definition
	Even if an individual's name does not appear, but there is a reasonable chance that an individual could be identified from the information (including where information can be combined with other information to identify a person), it can still be personal information for the purposes of the Privacy Act.
Privacy breach	A "privacy breach" occurs when the DHB does not comply with one or more of the Information Privacy Principles set out in Part 3 of the Privacy Act 2020 or rules as defined within the Health Information Privacy Code 2020. Examples include instances where personal information held by the DHB is accessed, disclosed, altered, lost or destroyed without authorisation or by accident or when requests for access to personal information are not processed in a timely manner. A privacy breach may also be something that prevents the DHB from accessing the information on a temporary or permanent basis.
Privacy by Design	"Privacy by Design" is an approach taken when creating new technologies and systems. It is when privacy is incorporated into tech and systems, **by default.** It means your product is designed with privacy as a priority, along with whatever other purposes the system serves. The seven principles of Privacy by Design are explained here.
Research	Research is any social science; kaupapa Māori methodology; or biomedical, behavioural or epidemiological activity that involves systematically collecting or analysing data to generate new knowledge, in which a human being is exposed to manipulation, intervention, observation or other interaction with researchers either directly or by changing their environment, or that involves collecting, preparing or using biological material or medical or other data to generate new knowledge about health and disability.
Third Party (includes other agencies)	"Third Party" or "Third Parties" means a person or group external to a particular DHB. A Third Party could be a healthcare provider (such as a primary health organisation or another DHB), a government agency (such as Police, Oranga Tamariki), or other individuals (such as whanau or family of a patient).

3. Privacy Act 2020 and Health Information Privacy Code 2020

The Privacy Act 2020 sets out 13 information privacy principles to govern the collection, security, access, retention, use and disclosure of personal information. The Health Information Privacy Code 2020 is a code of practice under the Privacy Act 2020 to govern health information. The 13 rules of the Health Information Privacy Code 2020 complement the 13 information privacy principles of the Privacy Act 2020.

The 13 information privacy principles from the Privacy Act 2020 and rules from the Health Information Privacy Code 2020 are summarised in the following section of this policy, as shown in the diagram below. To see the rules and principles in full please refer to the Office of the Privacy Commissioner's website.



3.1 Collection

Expected values and behaviours

He tāngata
Focus on improving New Zealanders' lives — individuals, children and young people, whānau, iwi, and communities.

- Strive to create positive outcomes from any collection, sharing or use of data and information
- Use appropriate checks and balances and ensure that information is suitable and reasonably necessary for the intended outcome

Manaakitanga

Respect and uphold the mana and dignity of the people, whānau, communities or groups who share their data and information.

- Recognise and incorporate diverse cultural interests, worldviews, perspectives and needs
- Include and involve service users whenever possible
- Incorporate the needs and priorities of people with a specific or particular interest in what is done with their data and information

Only collect personal and health information if you really need it – [Principle 1/ Rule 1]

Information must only be collected if it is necessary for purposes connected with the DHB's functions. Patient health information may be collected to provide care and treatment, administration, training and education and monitoring quality of care. Personal information relating to DHB personnel may be collected for purposes including determining job suitability, work performance, workplace health, safety and security of DHB assets, workforce planning and administration.

Collect only the information required to fulfil your objectives; this can include questions you ask of patients, but also software settings for equipment you use.

*Consider DPUP value '**He tāngata**': Are the purposes of collection clearly focused on positive outcomes and is the information to be collected necessary to achieve those outcomes? Purpose will **always** be relevant. Assessing and articulating it properly is vital to both legal compliance and guarding against indiscriminate or excessive collection of people's information.*

Get it straight from the individual concerned – [Principle 2/ Rule 2]

Information should be collected from the individual who the information is about. If you want information about an individual, just ask them.

*Consider DPUP value '**Manaakitanga**': Complete forms, assessments or records together with patients or relevant individuals.*

In some situations, information can be collected from other people such as next of kin or who have the individual's consent or authority to act on their behalf.

Tell the individual what you will do with their information – [Principle 3/ Rule 3]

When you collect information, let the individual know why it is being collected, who will receive it, whether collecting it is voluntary and what will happen if it is not collected. An explanation is not necessary if doing so is impractical, against the individual's interests or prejudices the purpose of collection.

***Guideline**: This explanation could be a privacy statement on a form, a wall poster, patient information brochure, statement on DHB website or discussed in conversation. DHB specific content to be detailed in this section.*

*Consider DPUP value '**kaitiakitanga**': As kaitiaki or stewards of individual's personal information, can the purposes of collecting be easily explained to individuals and in a way that fosters understanding and trust in what is being done with their information?*

Be considerate when you collect the information – [Principle 4/ Rule 4]

Collect information in a way that is lawful, fair, open and transparent. Information cannot be collected by unlawful, unfair or intrusive methods. This is particularly important when collecting information from a child, young person or vulnerable adult– take extra care.

Some examples:

Collection is unlawful if it is in breach of another law. Collection is unfair if it is done in a threatening or misleading way. Collection is unreasonably intrusive if you collect information without respecting cultural needs or the individual's preferences.

3.2 Security

Expected values and behaviours

Kaitiakitanga

Act as a steward in a way that is understood and trusted by New Zealanders.

- Recognise you are a kaitiaki, rather than an owner of data and information
- Be open and transparent; support people's interest or need to understand
- Keep data and information safe and secure and respect its value

Take care of it once you have got it – [Principle 5/ Rule 5]

Take reasonable steps to ensure that all information collected about an individual is protected against loss, unauthorised access, misuse, modification or disclosure. Consider kaitiakitanga: keep information safe and secure and respect its value.

***Guideline**: Reference local DHB Security/ IT Policies/ User Audit process etc.*

Some examples:

Auditing is useful way to pick up a common misuse: unauthorised browsing by DHB personnel. A Privacy Impact Assessment provides assurance that appropriate privacy risks have been considered to support security and data governance.

*Consider DPUP value '**kaitiakitanga**': Understand that as a steward of the data-, we must keep data and information safe and secure and respect its value:*

- *Use data management practices that are safe and secure, bearing in mind the nature of the information and data, and how it is being collected, used, shared, analysed and reported.*
- *Treat data as a valuable asset. Store and maintain it so that it is accessible and reliable.*
- *Those who hold people's information are in a position to grow its value. They may do this by creating and sharing insights, or by returning collective, non-personal data back to the people and community it came from for their use. In all cases they must take care to comply with the law, protect people's privacy and maintain people's trust and confidence.*

3.3 Access, Correction and Accuracy

Expected values and behaviours

Mana whakahaere

Empower people by giving them choice and enabling their access to, and use of, their data and information.

- Where possible, give people choices and respect the choices they make
- Give people easy access to and oversight of their information wherever possible

Access and correction requests must be dealt with in accordance with the *local DHB procedure/ policy to be referenced here*. Requests for access or correction of personal and health information can be made verbally or in writing, and should be directed to *local DHB specific team name/ individual to be included here.*

***Guideline**: Each DHB to provide escalation process/ contact details should staff member need technical expertise could be Legal Team/ Privacy Officer.*

An individual can see their personal and health information if they want to – [Principle 6/ Rule 6]

Everyone has the right to access information about themselves. However, a DHB may refuse access to the information if there are good reasons. This principle is about access to information, and not ownership of information. You must take care that the person who is requesting the information is that person or their approved representative. Please note that it is an individual's ***legal right*** to make a request to a DHB to confirm if the DHB holds any personal information about them, and to have access to that information.

*Consider DPUP value '**mana whakahaere**': Consider the following:*

- *Give people easy access to and oversight of their information wherever possible*
- *Encouraging people to see what is recorded about them is a way of empowering them and acknowledging that their data and information is part of their story and experiences.*
- *Making it easy for people to see their data and information can mean many things — from showing them what is written on a computer screen, to including them on email referrals to another agency (taking care to double-check email addresses), to providing information in accessible formats for people with a sight disability or limited literacy. The important thing is that people shouldn't have to rely on Privacy Act requests to access information held about them.*
- *Whenever possible, help people check, add, or correct their information.*
- *Help people access their information so that they can share it with others and avoid retelling their story if that is what they want.*

Some examples:

An individual's access to information can be declined if allowing access to the information would pose a serious threat to life, health or safety, or lead to serious harassment. A complete list of reasons to refuse access is set out in sections 49-53 of the Privacy Act 2020.

The Office of the Privacy Commissioner may direct a DHB to provide an individual access to their personal and health information if the DHB refuses access without a proper basis. See Section: 2.10 Compliance, offences and fines.

An individual can ask to correct their information if they think it is wrong – [Principle 7/ Rule 7]

Everyone has the right to request a DHB to correct the information held about them. Correction may involve amending, deleting or adding information, if the request is reasonable and necessary to ensure accuracy.

A DHB must give reasonable assistance to the individual who wishes to make a correction and may have to transfer the request to another DHB if necessary. If a DHB does not believe the information needs correcting, it must take reasonable steps to attach a statement of the correction sought by the individual. You must tell the individual what you have corrected; if you are not going to correct the information, you must tell them what steps you have taken for their request for correction to be added to their records and files.

For further guidance refer to your Privacy Officer [insert specific DHB Privacy Officer contact details here] for support.

Check the accuracy of information before using it – [Principle 8/ Rule 8]

Ensure the personal and health information is accurate, up to date, complete, relevant and not misleading before you use or disclose it.

3.4 Retention

Get rid of the information once you are done with it – [Principle 9/ Rule 9]

Personal and health information should only be kept for as long as it is necessary for the purpose it was collected. Health information must be retained under certain legislation, and this overrides the Health Information Privacy Code 2020 and the Privacy Act 2020, to the extent that they are inconsistent.

Some examples:

- *Health (Retention of Health Information) Regulations 1996 require all health information to be retained for ten years from the last encounter with the patient, unless transferred to another doctor or to the patient.*
- *The Public Records Act 2005 also requires retention. The DHB General Disposal Authority lists how long each type of clinical record must be kept for and what must be done afterwards.*

Once the obligatory retention periods have passed, personal information should be disposed of, securely, unless there is a lawful purpose to retain it.

Sometimes health and personal information may need to be kept longer for special reasons.

Example:

DHBs must currently hold some information indefinitely due to the Royal Commission of harm while in State Care.

***Guideline**: Reference own retention procedure here.*

3.5 Use and Disclosure

Expected values and behaviours

He tāngata
Focus on improving New Zealanders' lives — individuals, children and young people, whānau, iwi, and communities.

- Strive to create positive outcomes from any collection, sharing or use of data and information

Mahitahitanga
Work as equals to create and share valuable knowledge.

- Work with others across the sector to create and share value together
- Confidentially share relevant information between professionals so people get the support they want and need
- Make sure there is a two-way street of sharing (de-identified) data, analysis, results and research findings to grow collective knowledge and improve services

Use it for the purpose you got it – [Principle 10/ Rule 10]

Personal and health information should generally be used for the same purposes it was collected. Consider the purposes for which information is being collected at the time of collection (see Principle 1 / Rule 1 above). Principle 10 / Rule 10 permit a DHB to use the information for those legitimate purposes connected with the DHB's functions.

A new use of information is allowed in certain situations.

Only disclose the information if there is a good reason – [Principle 11/ Rule 11]

Disclosure is permitted if the individual consents or disclosure is one of the purposes for which the information was collected. Information must be disclosed if another law requires it. Information can also be disclosed in certain situations if it is not appropriate to obtain the individual's consent. Only disclose the information required to fulfil the requirement and try to avoid excessive sharing.

There are several situations where a DHB is permitted to disclose information under rule 11. This policy does not describe all those situations. However, DHBs most frequently disclose information in the following situations:

- Disclosure is authorised by the individual or their representative
- Disclosure was one of the purposes for which the DHB got the information, e.g. sharing the hospital discharge notes with the patient's GP
- Disclosure is necessary to prevent a serious threat to an individual's life or safety
- Disclosure is necessary for court proceedings or to maintain the law
- Disclosure is for statistical / research purposes

Information must be disclosed if it is required by a compulsory legal authority that overrides the Privacy Act 2020, such as:

- a production order or search warrant by New Zealand Police
- a request for information about child care and protection under section 66 of the Oranga Tamariki Act 1989 by police or Oranga Tamariki
- a request for health information, requested by any person providing health services to the individual under section 22F of the Health Act 1956

Information can be disclosed in certain situations if it is not appropriate to obtain the individual's consent, such as:

- Information may be disclosed if necessary to prevent a serious threat to any individual's life or safety, or to avoid prejudice to the maintenance of the law or for statistical/research purposes, under information privacy principle 11;
- Health information may be disclosed, on request, to New Zealand Police, Oranga Tamariki or a probation officer under section 22C of the Health Act 1956
- Information may be disclosed via a report of concern to Oranga Tamariki if a child is at risk, under section 15 of the Oranga Tamariki Act 1989
- Information may be proactively shared with specified agencies and persons for the well-being or safety of a child and / or to respond to family violence

*Consider DPUP value '**Mahitahitanga**': Confidentially share relevant information between professionals so people get the support they want and need.*

- *Recognise the diverse and complex nature of the sector and use it as an opportunity. In many situations, no single professional or agency will have the whole picture.*
- *Enable other professionals to support service users by making sure they have the information they need to do their work, within what the law permits.*

Make sure there is a two-way street of sharing (de-identified) data, analysis, results and research findings to grow collective knowledge and improve services.

- *Enable organisations/groups with a clear and legitimate interest to safely and easily access and use government held data sets in a de-identified form, for locally led development.*
- *Share expertise and help others understand and use data accurately and safely, for example, ensuring it is not re-identified.*

- *Advocate for, and support 'by/for' research, like Kaupapa Māori, so communities or groups better understand their own goals and priorities and the needs of their people.*
- *Create feedback loops with people and organisations who contribute data and information. Tell them the outcomes of any use and the value it created.*

Only disclose information overseas if it is safe to do so for the individual – [Principle 12/ Rule 12]

Information may only be disclosed overseas if the overseas recipient (a foreign person or entity):

- Is subject to the Privacy Act 2020 because they do business in New Zealand;
- Is subject to privacy laws that provide comparable safeguards to the Privacy Act 2020;
- agrees to protect the information in a way that provides comparable safeguards to the Privacy Act 2020, e.g. contractual clauses between the parties provide for privacy obligations; and/or
- is covered by a binding scheme or is a country prescribed by the New Zealand government.

If the overseas recipient does not meet one of the above requirements, then seek authorisation from the individual. The individual must be expressly informed that the overseas recipient organisation may not be required to protect the information in a way that provides comparable safeguards to the Privacy Act 2020. If the individual does not provide authorisation, then do not disclose the information overseas. Talk to the Privacy Officer and/or Legal Services to explore other options.

Take care to note that these obligations do not apply if the information is urgently required overseas to maintain the law or to prevent or lessen a serious threat to public health, safety, or an individual's life or health (both for the individual concerned, and also for another individual whose life or health is under serious threat as the case may be).

Sending information to an overseas cloud storage service to hold information on the DHB's behalf is not considered to be an overseas disclosure of information, as the storage service is holding the information on behalf of the DHB for safe custody under section 11 of the Privacy Act 2020.

The Privacy Act 2020 has extraterritoriality effect; this means it applies to overseas agencies in relation to actions taken by them while carrying on business in New Zealand. Therefore if you are sending information to a foreign entity (for the purposes of IPP 12) who is also an overseas agency (for the purposes of section 4), they will be subject to the Privacy Act in respect of the personal information that they hold in the course of carrying on business in New Zealand, and this gives you a basis to disclose information overseas.

In short, when sharing information to a foreign person, authority or country, an individual's privacy should be protected the same if not better than if it was shared in New Zealand.

3.6 Unique Identifiers

Only use unique identifiers where necessary – [Principle 13/ Rule 13]

National Health Index numbers are assigned and used to identify patients, instead of using their names. Unique identifiers are also assigned to DHB personnel to support the identification of the individual. Unique identifiers are used to support patient care and DHB personnel management only – they must not be used or shared for other reasons.

Unique identifiers should only be used in the context they are created; if it is not necessary to use a unique identifier like an NHI number and you can use a patient's name, you can avoid using the NHI number. For instance when sending a letter addressed to the patient, consider if it is necessary to include a unique identifier when the patient's name will do.

4. Privacy Breaches/ Interference with Privacy

4.1 Managing a Privacy Breach

If DHB personnel suspect or are aware that there has been a possible privacy breach or near-miss, they must immediately activate the *[local DHB process and escalation path/ National Procedure: Privacy Breach Response Procedure reference to be included here]*

It is important to respond to a suspected or actual privacy breach as quickly as possible so that the DHB can deal with it immediately and minimise the harm to the affected individuals. Being transparent, clear and open with the impacted individuals is critical to maintaining their trust. Full reporting of all incidents provides the DHB with an opportunity to improve processes or systems to avoid future breaches. Under the notifiable privacy breach framework, a DHB is required to notify the Office of the Privacy Commissioner and the affected individual if the breach caused 'serious harm' to the individual.

IMPORTANT: See the National Privacy Response Procedure [include the link to the document here] which details the roles and responsibilities for investigating, assessment and reporting through to the Office of the Privacy Commissioner for breaches that meet the 'serious harm' threshold.

Key steps in managing a breach:

- Contain the breach and make a first assessment (Use the Office of the Privacy Commissioner's Notify Us Tool)
- Evaluate the breach
- Notify affected people if necessary
- Prevent the breach from happening again

The DHB Privacy Officer will confirm whether there has been a notifiable privacy breach that triggers notification to the Office of the Privacy Commissioner and the affected individual/s. Failure to notify the Office of the Privacy Commissioner of a notifiable privacy breach is an offence and can result in a fine up to $10,000.

Further guidance can be found in the Procedure: Privacy Breach Response

4.2 Interference with Privacy

An interference with privacy is caused when the DHB breaches one of the privacy principles of the Privacy Act and harms an individual. Not all privacy breaches are interferences with privacy. A breach without harm is not an interference with privacy.

If the DHB breaches an individual's right to access their information, this is also considered an interference with privacy - without the individual needing to show that they've been harmed as a result of the breach.

4.3 Lodging a complaint

DHBs should seek to redress privacy complaints with the individual as much as possible, and that while the Office of the Privacy Commissioner is always available to the individual, this should not be their first port of call to redress their complaint with the DHB.

However, any individual who thinks they have suffered a breach of the Privacy Principles or some other interference with their privacy can:

1. Lodge a complaint through *[insert local process here]*

2. Contact our Privacy Officer *[insert local contact details for DHB Privacy Officer]*
3. Complain to the Office of the Privacy Commissioner, see details.

5. Compliance, offences and fines

Failing to comply with this policy might be considered *local DHB HR serious misconduct specific DHB definition to be inserted here* and might be escalated to the *(local DHB Human Resources Department term to be used)* for investigation and possible disciplinary procedures.

***Guideline**: Confirm HR policies re: serious misconduct. Escalation of non-compliance - confirm DHB process for investigation.*

The Privacy Act 2020 gives the Privacy Commissioner greater powers to ensure businesses and organisations comply with their obligations. The following table provides the potential fines and actions that can be taken by the Privacy Commissioner for non-compliance:

Compliance and enforcement	Potential fines and actions
Access direction	Principle 6 gives people the right to access their personal information. If a business or organisation refuses or fails to provide access to personal information in response to a principle 6 request without a proper basis, the Commissioner may now compel the agency to give this information to the individual concerned. Access directions may be appealed to the Human Rights Review Tribunal. The DHB can be fined up to $10,000 for failing to comply with the access direction.
Compliance notices	The Privacy Act 2020 allows the Commissioner to issue compliance notices to agencies that are not meeting their obligations under the Act. A compliance notice will require an agency to do something, or stop doing something, in order to comply with the Privacy Act. Compliance notices may be appealed to the Human Rights Review Tribunal.
Refusing to comply with a compliance notice	Refusing to comply with a compliance notice is an offence under the Privacy Act. A business or organisation that has been issued a compliance notice and fails to change its behaviour accordingly can be fined up to $10,000.
Misleading an agency to get personal information	There is a new fine of up to $10,000 for misleading a business or organisation to access someone else's personal information. For example, it will be an offence to impersonate someone else in order to access their personal information.
Destroying requested information	If someone requests their personal information and a business or organisation destroys it in order to avoid handing it over, the business or organisation can be fined up to $10,000. This includes inadvertent destruction of information; no matter to whom an individual may make a request for their information within the DHB, the DHB is responsible for processing that request and not destroying the information requested, even if it is two separate parts of the DHB responsible for each.
Failing to notify a privacy breach	If a business or organisation has a privacy breach that has caused or is likely to cause serious harm, it must notify the Privacy Commissioner. Failing to inform the Commissioner of a notifiable privacy breach can result in a fine of up to $10,000.

6. Privacy Impact Assessments/ Privacy by Design

6.1 Completing a Privacy Impact Assessment

Where a proposed project, policy, service change or facility design or build may affect the collection, storage, security, access, retention, use and disclosure of personal or health information, the service must assess the privacy risks at the earliest opportunity.

A Privacy Risk Assessment flowchart and Privacy Impact Assessments are tools to help identify and mitigate privacy risks being introduced to the DHB due to the change in the process/ system/ facility or service.

The service undertaking or proposing the change must complete the Privacy Risk Assessment flowchart to determine whether a full Privacy Impact Assessment is required. Click here to access the flowchart. *[link to Privacy Risk Assessment flowchart must be inserted here.* Based on the flowchart, a recommendation is provided as to whether a full Privacy Impact Assessment is required and why.

All Privacy Risk Assessment flowcharts and Privacy Impact Assessments must be reviewed for privacy and security considerations and endorsed by the *local DHB specific approval process to be included here – recommendation that review includes CIO and Privacy Officer approval/ oversight.]*

To understand what is required or what needs to be considered when reviewing a PIA see GCPO website – 'Reviewing a Privacy Impact Assessment (PIA).

***Guideline**: It is recommended that the Privacy Officer have oversight of ALL Privacy Risk Assessment flowcharts/ full Privacy Impact Assessments to ensure that all privacy risks have been identified and appropriately mitigated.*

Further guidance can be found in the Procedure: Privacy Impact Assessments.

6.2 Privacy by Design

The seven principles for Privacy by Design - and the philosophy and methodology they express — can be applied to specific technologies, business operations, physical architectures, networked infrastructure, and entire information ecosystems. The foundation is that privacy is built-in as the 'default setting'. Privacy is embedded throughout the product or service lifecycle from design to disposal. Further information can be found here.

7. Research, Audit, Quality Assurance and Quality Improvement

All research, audit, quality assurance and quality improvement projects should be registered with the DHB's *Research Office – local process to be included here with contact details*. The *Research Office – local process to be included here* will review the proposal and provide the necessary approvals. Should the project require the use of identifiable personal information, Health and Disability Ethics Committees (HDECs) approval may be required. Please contact - *– local contact details to be provided here.*

***Guideline**: Delete this section if not applicable at a local level.*

8. Support and Administration

8.1 Roles and Responsibilities

Protecting personal and health information requires support and vigilance from all DHB personnel. Some roles and responsibilities are defined, refer to Appendix A: Detailed Roles and Responsibilities for detailed information.

***Guideline**: Delete this section if not applicable at a local level.*

8.2 Training

DHB personnel must have an appropriate level of understanding of the legal and professional requirements governing the use of personal and health information. DHB personnel must complete the privacy training/ learning – *local DHB training requirements to be included*. Further e-learning modules are offered by the Office of the Privacy Commissioner.

8.3 Queries and Complaints

If you have queries about the handling of personal or health information or this policy, please contact *local DHB preferred contact and method of communication to be included.*

***Guideline**: Include contact details for your DHB Privacy Officer*

All serious concerns and complaints about privacy and complaints alleging a breach of the Privacy Act 2020 or Health Information Privacy Code 2020 must be directed to the *Feedback/Quality/Complaints Team - local DHB service title to be used.*

9. Associated Documents

***Guideline:** 'Associated Documents' section must be updated to align to each DHB's specific requirements.*

Type	Title/Description
Publications	• Code of Health & Disability Services Consumers' Rights • Health Information Privacy Code 2020
Legislation (see legislation.govt.nz)	• Crimes Act 1961 • Evidence Act 2006 • Family Violence Act 2018 • Health (Retention of Health Information) Regulations 1996. • Health Act 1956 • Medicines Act 1981 • Mental Health (Compulsory Assessment and Treatment) Act 1992 • Misuse of Drugs Act 1975 • Official Information Act 1982 • Oranga Tamariki Act 1989 • Privacy Act 2020 • Public Records Act 2005

Type	Title/Description
Procedures	• Breach of Privacy • Frequently Asked Questions (Resource Information) • Management Requests for health information • Privacy Day to Day (Resource Information) • Statement of Privacy (Resource Information)

Appendix A: Detailed Roles and Responsibilities

***Guideline**: This table provides indicative roles and responsibilities for privacy. This table must be updated to apply to each DHB's requirements. This table is voluntary.*

Individual/ Group	Accountability
DHB Employees	Understand and ensure compliance with the privacy principle requirements, managing personal information safely and with integrity.
	Respect others' information and be mindful when discussing personal information that this is appropriate and in the correct forum.
	Be familiar with the DHBs privacy policies and procedures.
Chief Information Officer	Responsible for implementing security functions to ensure electronic health information is adequately secured against loss and protected against unlawful access, misuse and disclosure.
Governance Body for Privacy Committee	Responsible for setting, maintaining and monitoring privacy standards. Receives reports from the Privacy Committee.
Corporate Records	Responsible for the management of corporate records, with consideration for privacy and security.
	Responsible for ensuring information is stored securely and appropriately with access restricted to an as-needs basis.
Executive Leadership Team	Managing privacy awareness within their respective directorates.
	Responsible for the governance and accountability of the District Health Board in relation to privacy and the Government's Chief Privacy Officer's expectations.
Frontline staff	Are responsible for the identification and initial response to privacy breaches.
	Report all breaches or near misses through the formal incident reporting process. Where allocated, investigate the cause of the breach and provide recommendations for remediation.
	Notification of the privacy breach or near miss to the Privacy Officer.
Human Resources	Manage and safeguard staff records, include appropriate storage; user access and use.
	Responsible to manage the disciplinary process, where required as defined by CM Health's internal policies.
Legal Team	Providing legal advice on the interpretation and application of the Privacy Act and Health Information Privacy Code.
	Providing legal representation on the Privacy Committee
Privacy Committee	Support the DHB to meet its legal obligations under the Privacy Act 2020 and Health Information Privacy Code 2020.
	Direct and oversee the implementation of the DHB's Privacy Strategy.
	Lead the development and implementation of policies, procedures, guidelines and security measures that aim to protect personal information, including health information.
	Review and provide advice in relation to privacy related reports including summary or trend reports relating to privacy KPIs or privacy breach management.
	Lead the development and implementation of privacy related training and education across the DHB.
	Oversight of privacy risks, controls and assurance and related trends.
	Identify and manage privacy maturity improvement opportunities and monitor the implementation thereof.
Clinical Records/ Audit Department	Perform user access reviews to ascertain appropriateness of access.
	Manage the release of patient information as per the DHB procedure/ guideline.

Individual/ Group	Accountability
	Escalate any technical patient information release issues or enquiries to the Privacy Officer or Legal Team for further consultation, as required.
Privacy Officer	Chair of the Privacy Committee
	Responsible for the privacy policy, strategy and programme of work.
	Protects and promotes privacy by encouraging compliance with the Privacy Act 2020 and related Health Information Privacy Code 2020.
	Conduct privacy incident investigations as necessary and prepare investigation summary reports.
	Analyse breach information to assess organisational impact, if applicable. Responsible to communicate and consult on significant breaches with the Chief Medical Officer and Legal Team, as appropriate.
	Responsible for reporting to Executive Leadership Team, Clinical Governance Group and Audit, Risk and Finance Committee.
	Oversee external and internal communication and information sharing in the event of a privacy breach or incident.
	Manage external relationships with the Government Chief Privacy Officer and the Office of the Privacy Commissioner.
Research Committee/ Office	Responsible for the consideration of privacy and ethical aspects of research and audit conducted at the DHB.

Code of Conduct

Mā te kimi ka kite, Mā te kite ka mōhio, Mā te mōhio ka mārama.
Seek and discover. Discover and know. Know and become enlightened.

Purpose

1. The Code of Conduct outlines the standards of behaviour that are expected of our people.
2. It is important that our people understand what minimum standards of behaviour and performance are expected of them while they are undertaking work for Te Whatu Ora - Health New Zealand.
3. Our Code is important because it reflects our legal obligations as an organisation through the Public Service Act 2020 to maintain high standards of integrity and conduct as a representative of the Crown and a public service. Te Whatu Ora needs to observe and comply with all applicable laws, regulations, policies, processes, and guidelines and as a result we expect our people to do the same.
4. It is our people's responsibility to act within the relevant legislation, regulations, policies, processes, and guidelines that apply to them and their work. If there is a difference between a legal requirement and our Code, the legal requirements are to be adhered to.
5. The Code of Conduct applies in addition to our other policies, procedures, and any job specific requirements our people may have.
6. Failure to meet the minimum standards of behaviour in the code may be classified as misconduct or serious misconduct, for which disciplinary action may be taken in line with our Investigations and Disciplinary Policy.
7. This policy supports the Health Sector Principles as set out in the Pae Ora (Healthy Futures) Act 2022 (the Act) and will be updated to reflect the requirements of the New Zealand Health Charter once it has been established. The Charter is a statement of the values, principles, and behaviours that our people throughout the health sector are expected to demonstrate.
8. The examples in this Code are not intended to create a complete and exhaustive list of minimum standards of behaviour.
9. The Code of Conduct relating to Board members is outlined in the Board Governance Manual.

Application

10. This policy applies to everyone in Te Whatu Ora National Office, including permanent, seconded, and temporary employees and contractors (referred to as our people).
11. For other parts of Te Whatu Ora, the corresponding policies that were in place before 1 July 2022 continue to apply until changed by the Board of Te Whatu Ora or its delegate.

Definitions

12. The following definitions are used for the purposes of this policy:

Te Whatu Ora National Office	a) Staff who are working in roles that would **not** have been District Health Board, Te Hiringa Hauora/Health Promotion Agency or Shared Services Agency roles under the previous health system (including staff employed/engaged on or after 1 July 2022); and b) For operational policies other than employment policies, staff who have transferred from the Ministry of Health (MoH) under the Act.

13. This policy is an employment policy and does not apply to staff who have transferred from the Ministry of Health (MoH) under the Act.

Key Principles

14. This section summarises the general principles which guide our disciplinary and investigation processes.

Restorative Approach: The emphasis will be to resolve issues at the lowest level possible and a focus will be placed on restoring relationships.
Fairness: We will act in accordance with our legal obligations and recognise the impact that disciplinary action has on our people.
Te Tiriti o Te Waitangi: We recognise our obligations as a partner under Te Tiriti o Te Waitangi as per the Pae Ora (Healthy Futures) Act 2022

Alignment to Te Whare Tapa Whā

15. This policy is underpinned by the focus that every interaction with our people should be done in a mana enhancing way, guided by Te Whare Tapa Whā specifically:

- Taha Tinana – we aspire to promote and develop conducive environments for our people to flourish;
- Taha Hinengaro – we provide support and care for our people's wellbeing;
- Taha Wairua – we acknowledge and respect our people's diversity and spiritual needs, ensuring a safe workplace;
- Taha Whānau – we are committed to looking after our people by creating an inclusive, whānau orientated and supportive environment; and
- Whenua – we are respectful of our environment and the role we, as an organisation and our people play to ensure healthy, sustainable environments.

16. Enacting such values serves as a means and commitment made by Te Whatu Ora to educate, promote, and develop Te Whatu Ora's workforce, and provide the necessary tools, resources, and training to enable and uphold Te Whatu Ora's commitment to Te Tiriti o Waitangi as the founding document of Aotearoa.

17. This approach enables the reformed health system to provide culturally appropriate care to all New Zealanders who use Te Whatu Ora's services in all settings, with a focus on providing a culturally safe environment for our people.

Policy

18. **Minimum standards of behaviour**

Our Minimum Standards of Behaviour are set out in this Code of Conduct, as well as our other policies and procedures. All our people have a responsibility to meet the minimum standards of behaviour set out in this Code of Conduct.

18.1. **Responsibility**

- All our people have a responsibility to meet the minimum standards of behaviour set out in this Code of Conduct.
- Our people have a responsibility to assist others to act in accordance with relevant laws, policies, procedures and guidelines and a duty of fidelity to report instances of abuse, fraud or unlawful conduct to a manager or People and Capability.

19. **Obligations in respect of Conduct**

19.1. **Treat people fairly and with respect**

- Our people are known for treating people fairly, this helps us create a good environment for our people and visitors. Treating people fairly means that we do not show any favouritism, bias, or self-interest in our work. We must avoid any perceived unfairness that could arise from having any personal interest in decisions we make or from working on matters where we have a close relationship with those involved.
- Therefore, our people have an obligation to treat other employees, contractors, visitors, and members of the public with respect and courtesy.

19.2. **Be professional and responsive**

- People should be mindful that they are representatives of a government entity and Te Whatu Ora at all times, and refrain from conduct that may bring Te Whatu Ora or the government into disrepute.
- It is important that our people are professional and responsive. This is because they are representatives of the government and of our health service.
- Therefore, our people have an obligation to be professional in their dealings with colleagues, contractors, visitors, and members of the community. They have an obligation to be responsive in their communications and ensure that health services are delivered in a timely way.

19.3. **Act lawfully**

- As government employees, it is important that our people act within the laws relevant to their role.
- Therefore, our people have an obligation to take actions in their role that ensure that Te Whatu Ora acts lawfully.

- Our people also have an additional obligation to report unlawful conduct that they see to their manager or People and Capability.

19.4. **Integrity**

- As public servants, it is important that we engage with integrity in our dealings. This allows us to build confidence in our health service.
- Therefore, our people are required to act with honesty and integrity in all their dealings, whether this is with other employees, contractors, visitors, or members of the community.
- Our people will not knowingly mislead or engage in dishonest practices.

19.5. **Harassment and Bullying**

- It is important that we protect the health and safety of those who work for us.
- Therefore, our people are required to refrain from harassing or bullying behaviour. Further details are available in our Bullying, Harassment, and Discrimination Policy.
- We also recognise that there is a range of inappropriate behaviours that may fall short of harassment and bullying thresholds. These include, but are not limited to, poor tone, manner and style as well as being confrontational or adversarial. It can include snide remarks or small comments and people should be conscious of the way their tone, manner, and style impacts on their colleagues.

19.6. **Racism and Discriminatory Behaviour**

- Our people welcome people regardless of their nationality, ethnicity, sexuality, disability, gender identity and other personal attributes.
- Therefore, we will not discriminate against people based on prohibited grounds of discrimination under Human Rights legislation. Further details are available in our Diversity and Inclusion policy.

19.7. **Social Media**

- It is important that we are able to maintain confidence in our public service and in our health system. Social media allows for wide communications to be sent but posts can quickly become available to wider audiences than are intended.
- Therefore, our people must not post or disclose any private or confidential information of the employer on social media, and anything that may bring Te Whatu Ora or the government into disrepute. Further details are available in our Media and Use of Social Media policy

20. **<u>Obligations in respect of impartiality</u>**

20.1. **Political Neutrality**

- As public servants, our people must maintain a politically neutral approach at work to enable us to work with the current and any future governments. Practically, this means that while our people are entitled to have freedom of political expression and association, we must not bring our political views into our work roles.

20.2. **Recruitment**

- Where engaging in recruitment processes, our people must consider all candidates in a way that is free from bias and prejudice. They will make decisions in accordance with the principles of fairness, equity, equal opportunity employment and in alignment with our organisational values.

21. Professional Standards

21.1. **Best Interests**

- As a health organisation, our primary focus is on the planning, funding, and delivery of personal and public health services, and disability support services.
- Therefore, our people must act in a way that is in the best interests of this focus.

21.2. **Maintaining necessary qualifications to enable you to perform your role**

- Our people must maintain any necessary qualifications to enable them to perform their role, including practicing certificates and mandatory learning.

21.3. **Obligation of disclosure**

- Our people will immediately disclose any situations they become aware of which may mean they cannot maintain a valid practicing certificate or other professional certification which is a requirement of their position.
- Our people will be supported to disclose any situation that changes their ability to practice.

21.4. **Obligation of compliance**

- Our people must comply with any rules and regulations of any professional body to which they are a member.

22. Privacy and Confidentiality

22.1. **Confidential Information**

- Our people will keep work-related confidential information private and confidential. They must not discuss confidential information in a public setting without appropriate delegated authority. They must also only access or disclose private and confidential information in accordance with applicable law.

22.2. **Disclosure of Private Health Information**

- Our people must treat information with care and use it only for proper purposes.
- Our people must not access or disclose private health information except where it is lawful to do so.
- Where there is concern or uncertainty as to what may be disclosed, people are encouraged to speak with their manager of People and Capability.

22.3. **Media Statements**

- Our people must seek and gain approval before sharing information on behalf of Te Whatu Ora and/or engaging in any requests to share internal information. See the Media and Use of Social Media policy.

23. **Conflicts of Interest**

23.1. **Definition**

- A conflict of interest occurs when someone is compromised when their personal interests or obligations conflict with responsibilities of their job or position. Refer to the Conflict of Interest Policy for more information.

23.2. **Acting with Integrity**

- Conflicts of Interest must be disclosed in a timely manner in line with the Conflict of Interest Policy.

23.3. **Acceptance of Gifts or Benefits**

- Our people must not use their official position for personal gain. Our people must not provide, solicit, receive gifts and/or benefits without appropriate delegated authority – see the Sensitive Expenditure Policy and Koha and Gifts/Hospitality Policy.

Non-Compliance with the Code of Conduct

24. Our people are expected to conduct themselves in accordance with this Code. Failure to meet the minimum standards of behaviour in the code may:
    - for employees, result in disciplinary action in line with our Investigations and Disciplinary Policy.
    - for independent contractors, failure to meet the minimum standards of behaviour in the Code may result in termination of their contract for services.

25. If any of our people considers that the standards set out in this Code may have been breached by another person, then the matter can be raised with their manager or People and Capability.

Roles and Responsibilities

26. All our people must:
    - abide by the Code of Conduct and other policies and procedures of Te Whatu Ora;
    - comply with the Public Service Commission Standards of Integrity and Conduct; and
    - act in line with Te Mauri o Rongo – NZ Health Charter.

Related Policies and Procedures

- Bullying, Harassment and Discrimination Policy
- Diversity and Inclusion Policy
- Privacy Policy
- Investigations and Disciplinary Policy
- Conflict of Interest Policy
- Media and Use of Social Media Policy
- Sensitive Expenditure
- Koha and Gifts/Hospitality Policy

- Public Service Commission Standards of Integrity and Conduct

Related Legislation

- Employment Relations Act 2000
- Privacy Act 2020
- Public Service Act 2020

OWNER:	People and Capability
CONTACT:	Rosemary Clements
ENDORSED:	15 July 2022
TO BE REVIEWED:	June 2023