He Kaupare. He Manaaki. He Whakaora.
prevention. care. recovery.

29 January 2024

[redacted]

Kia ora [redacted]

Your Official Information Act request, reference: GOV-029984
Thank you for your email of 15 January 2024, requesting the following information under the Official Information Act 1982:

> *Please provide to me, any and all policy and procedure documents, (and any acc staff training documents), that detail, the rules/guidelines regarding the recording and retention and storage of all documentation generated by in integrity services investigation, of either a staff member.... contractor, or an acc client.*

Please find attached ACC's policy and guidance documents regarding information management
The following attached documents govern the management and retention of information across ACC, including Integrity Services:

- Information Management Policy
- Information Management Standards
- Personal Information and Privacy Policy
- Personal Information and Privacy Guidelines

As staff names were not requested, they have been deemed out of the scope of your request and removed.

Further information is publicly available
The Integrity Services Transparency Statement also provides guidance on information storage and retention and is available on our website: https://www.acc.co.nz/assets/corporate-documents/transparency-statement-integrity-services.pdf

As this information may be of interest to other members of the public
ACC may decide to proactively release a copy of this response on ACC's website. Your name and contact details will be removed prior to release. The released response will be made available www.acc.co.nz/resources/#/category/12.

If you have any questions about this response, please get in touch
You can email me at GovernmentServices@acc.co.nz.

Ngā mihi

Jason Hope
Acting Manager Official Information Act Services
Government Engagement

Information Management Policy

POLICY NUMBER	5.0.0
TOPIC	Information Management
OWNER	Deputy Chief Executive – Enterprise Change Delivery
BUSINESS GROUP	Enterprise Change Delivery
AUTHOR	Outside of scope Manager Information Frameworks and Assurance
DATE APPROVED	25th March 2021
APPROVER	ACC Board
NEXT REVIEW DATE	25th March 2024

1 Policy Statement

As a Crown entity, ACC holds information on behalf of the peoples of New Zealand. The information held is related to the duties ACC is responsible for in accordance with the Accident Compensation Act 2001. These duties relate to ACC's major functions: injury prevention, rehabilitation, setting and collection of levies; assessing and paying claims and investment management. This constitutes the primary use of this information.

ACC holds a unique set of information that has significant value, not only for NZ but internationally.

Information is the only enduring asset that ACC holds and should be treated as such. This aligns with the Māori data sovereignty principle of viewing this as a treasure (Māori: taonga). In recognition of the obligations under the Treaty of Waitangi (Māori: Te Tiriti o Waitangi).

To extract the maximum value of this resource, the secondary use of information must be actively promoted and supported for secondary use which includes:

Identifying opportunities for injury prevention initiatives

Improving customer service by improving outcomes, efficiencies and effectiveness

Sharing information for external use in support of insights and research related to accidents, injuries, treatments

Ensuring information is available and representative of the peoples of NZ, including Māori, minorities and marginalised groups to facilitate and support these communities

Partnering with representative groups to promote, support and advise on the appropriate use of ACC information

To ensure that information is fit for purpose, ACC is committed to establishing, maintaining and monitoring modern information management practices to ensure they meet both primary and secondary needs. This includes meeting legal compliance, accountability requirements and stakeholder expectations.

2 Alignment with Government

As a crown entity, ACC is expected to conform and adhere to government policies and practices related to information management as specified by appointed officials. In addition, as ACC is viewed as part of the health and disability sector, we also need to conform to specific sector requirements.

These are described in more detail in Appendix 3.3.

3 Policy Objective

We are committed to establishing modern information governance and management practices that meet our customer expectations, ongoing business needs, security, privacy and legal requirements including:

- Capturing only relevant, and applicable, information
- Securing and storing our information appropriately, recognising that we are a customer-centric organisation
- Documenting actions and decisions as required for legislative, governance and legal reasons
- Managing information as a strategic corporate asset

All our information management practices are delivered in accordance with the principles set out in this policy, and its supporting standards and procedures. ACC is committed to continuous improvement in our corporate information policies, processes and standards.

4 Policy Scope

This policy is intended for all our people, including our board members, consultants, contractors and organisations (including vendors and other third parties) engaged to undertake work on behalf of ACC.

This policy covers all information that we create, ingest, receive, manage, store and share as part of conducting our business.

5 Policy Principles

Our Information Management principles are the foundations for the way that we use information within ACC.

Our information must be managed, secured, and maintained as per our Information Management principles. We must also comply with all relevant legislation and government standards.

Personal and health information makes up a significant part of our information.

The ACC Privacy Policy sets out additional requirements for storage and use of this information and must be read in conjunction with this policy when dealing with personal and health information.

4.1 Our Information is a strategic asset and we actively manage it

Our Information Governance Group (IGG) must ensure that our information assets are professionally managed. This supports our objectives, principles, and the obligations set out in the IGG Terms of Reference.

Active management means:

- We have senior leaders setting strategy, and making sure we are sufficiently resourced to manage our information assets in a consistent, integrated way
- We use our information assets to deliver insights and enable smarter business decisions
- Our change management processes consider, and actively manage, information management risks at both design and implementation stages
- All staff must ensure the information they use is accurate and fit for purpose.

4.2 Our information has clear ownership

All our business-critical information assets must be assigned a Steward (business owner) by subject area, and at least one Custodian (information caretaker) as per our Information Stewards and Custodians Standard.

Stewards and Custodians must ensure that our information is cared for (actively managed) throughout its lifetime. They must also ensure that information access is only granted where needed for the particular role and is disposed of (destroyed or archived) at the end of its lifetime in accordance with our approved disposal authorities.

Clear ownership means:

- We must ensure all staff understand and are able to manage our information within their role
- We must ensure our information is fit for purpose and aligned with the strategic direction set by the Information Governance Group (IGG)
- All our key information assets have defined business owners (Stewards) with agreed delegation of authority
- Stewards are responsible for making decisions related to their assigned information assets
- Custodians support Stewards by ensuring the information they are responsible for is fit for purpose, meets primary and secondary needs, is readily accessible by those that need it and is trustworthy.

4.3 We make our Information fit for purpose

We must manage information to ensure it is fit for purpose, consistently described, trustworthy and meets all needs. We all have a responsibility to conform with required quality requirements by, taking ownership of the information in our care.

Fit for purpose means:

We protect the value of information against misuse, misinterpretation, unnecessary access restrictions or failure to maintain its quality

Active stewardship of our information ensures that it remains fit for purpose. To do so it must be accessible and complete, well described so that it is understood, and can be used with confidence in support of both internal and external:

Evidence-based decision making
Research
Reporting
Analytics, and
Data Mining
Information must be periodically reviewed to ensure compliance with all relevant legislation and standards as shown Appendix 1
Good archiving and disposal practices ensure our information is compliant with the requirements of the Public Records Act 2005.

4.4 We make our information Accessible, yet Secure

We enable the sharing of our information to make best use of the information assets we hold and promote public and government confidence in our information.

We protect the ethical use, confidentiality, integrity and accessibility of information, through active management and adherence to the principles of our Privacy Policy, Information Security Policy and Standards.

Accessible, yet Secure means:

We comply with our obligations under the New Zealand Open Data Charter
We enable appropriate, and prevent inappropriate access and reuse of our data assets
We improve the effectiveness and efficiency of work by allowing people to discover, use, and share information
We enable better, evidence based, decision making
When we share information externally, we ensure appropriate approvals and/or formal agreements are in place, and where relevant will seek advice from the ACC Ethics Panel.
We minimise the risk of uncontrolled release of our information, and the resulting harm arising to our clients, business and personnel
The privacy and confidentiality expectations of all stakeholders are met.

4.5 Our Information is simplified by design, and we standardise it for reuse

Our information architecture and Enterprise Information Management (EIM) Strategy provides the big picture of how our information hangs together. It is designed to provide visibility, promote reuse, integration and efficiency.

Simplified and standardised information means:

A well-managed information architecture that allows people to discover, use and share information
It provides a lean, agile information environment that results in more efficient use of information assets, and promotes cost effective business outcomes
The concept of ‘create once, use many times’ meaning duplication and reinvention is minimised, which allows us to significantly reduce the cost and effort in creating and managing duplicate information

4.6 We all share a common understanding of how we work

All our people and contractors understand their responsibilities as set out in this policy and its supporting policies, standards, procedures and guidelines.

We all work to deliver our information management goals and best practice outcomes for all our customers.

6 Accountabilities

The ACC Board is responsible for ensuring ACC's compliance with the directions to support an all of government approach including the current direction on Information and Communication Technologies (ICT).

To support the Board, each Executive member is accountable for understanding and compliance with this policy and its supporting policies and standards within their business area.

This includes effective implementation of information management practices across our work activities to ensure the principles of this policy are understood and that the relevant legislation and standards are complied with.

The Deputy Chief Executive – Enterprise Change Delivery is accountable for the operational implementation and monitoring of this policy.

7 Responsibilities

All employees are collectively responsible for Information Management.

Role	Responsibilities
Employees including contractors, consultants and temporary staff engaged by ACC	Must read and understand the principles of this policy. Adhere to any reasonable instruction that is given to comply with legislation and best practice. Complete information management training as required so that they: Comply with our documented information management policies and procedures Can create full and accurate records of activities, transactions, and decisions carried out during daily business activity Ensure that such records are maintained by being captured into the appropriate information management system All Information assets are classified in accordance with our Information Security Policy When creating or amending information, they are responsible for its quality Maintain best privacy practices in line with the Privacy Policy, including managing information safely and reporting breaches.
People Managers	Ensuring these principles are understood Creating an environment where appropriate information management practices are present in team thinking, discussion, and decision-making Develop skills and knowledge to support and facilitate staff in information management best practices They communicate expectations with staff, monitor compliance, and ensure accurate reporting.
The Information	Operates with appropriate delegation of responsibility to oversee and

Governance Group (IGG)	govern the information management function and is accountable for Enterprise Information Management Strategy IGG's focus is to ensure that our information is actively managed throughout each stage of its lifecycle as a strategic business asset IGG's roles and responsibilities are set out in by the IGG Terms of Reference Document Appoints required roles and delegates appropriate authority to ensure they can operate effectively in their information role and duties in conjunction with their manager.
Security Advisory Group (SAG) Privacy	Responsible for advising the IGG on the outcomes of the Information security roadmap and the Privacy maturity roadmap.
Content and Records Advisory group (CRAG)	Responsible for the advising the IGG on the outcomes of the content and records (C&R) roadmap and ongoing maintenance of the Information Management Policy.
Deputy Chief Executive – Enterprise Change Delivery	Directs and leads our information management initiatives Holds the positions of Chief Data Officer (CDO) and Chief Information Officer (CIO) as defined in relevant NZ legislation and policy Ensures that our Information is managed and updated, disposed of, or archived in a timely fashion in accordance with our approved disposal authorities Responsible for ensuring Information Stewards and Custodians are trained in the skills needed for their role in our information management Provides Senior leadership representation as chair of the IGG.
Ethics Panel	Advises on any research requests for personally identifiable or potentially personally identifiable ACC data
The Manager of Enterprise Data and Information (EDI) on behalf of the Deputy Chief Executive – Enterprise Change Delivery	Responsible for developing and implementing information systems and governance processes to ensure operational measures and monitoring is in place to support this policy Ensures all staff are aware of the policy and that the appropriate structures and roles are put in place with the right level of training and guidance to operate at the required level Support IM governance groups and roles to enable them to fulfil their obligations and responsibilities.
Information Stewards	Accountable and responsible for implementing operational policy, business value, scope, definitions, rules, standards, structure, content, use and disposal for information and data under their responsibility Make decisions on strategic needs as well as the collaborative needs and external partners and providers Ensure that Custodians are supported by management Ensure that all our information assets for which they are responsible are defined and maintained in the Information Asset Register.
Information Custodians	An inclusive role that accepts one or more delegated information and data custodianship activities on behalf of the Information Steward Manage and support the day to day operation and use of information Custodians use our processes and information management standards to make day to day decisions about information governance.
Deputy Chief Executives	Empower and direct our information management maturity and roadmap goals with appropriate delegation of authority Provide executive support and oversight of all our information management

	activity.
Board	Board is responsible for ensuring the organisation is aware of the need to look after our information through high-quality monitoring and information management practices.

8 Monitoring and oversight

The monitoring and oversight of privacy follows the five lines of assurance model (5LOA).

LOA:	Role	Monitoring & Oversight
1st Line	Employees and People Managers	All people managers monitor the completion of information management modules and training All employees remain alert to potential breaches of the Policy and report potential and actual breaches to their manager All people managers ensure that (i) breaches brought to their attention are documented, (ii) notification of the breach is provided to the owner of the Policy within five days of the breach occurring From time to time we deliberately take actions contrary to a policy's provisions (corporate policy exceptions). When people managers are responsible for a corporate policy exception, the people managers ensure that the exceptions are agreed either using the process in the Policy or by agreement in writing from the Po icy owner.
	Group Risk and Compliance Manager and/or Advisor	Supports employees/groups to determine whether events constitute actual breaches of the Policy Escalates breaches to the Group's Leadership Team and Deputy Chief Executive when appropriate. Updates risk registers as required.
	Policy Owner	The Policy Owner ensures that the Group (and other parts of ACC if applicable) respond appropriately to Policy breaches and requests for exceptions
2nd Line	Enterprise Risk Team	Performs periodic oversight activities intended to assess and/or provide insights into (among other things) compliance with the Policy and the adequacy and effectiveness of the Group's practices to monitor compliance and deal with breaches Reports to the Executive and the Board on the outcomes of such activities.
	Enterprise Data and Information (EDI) team	Provide oversight of all information management aspects in this policy and subject matter expertise to staff and management when required Regularly review and report to ensure the intention of the policy is being honoured Carry out periodic audit and assurance activities on information management practices along with the Enterprise Risk and the Privacy team Supports employees to determine whether events constitute actual breaches of the Policy Escalates breaches to the Group's Leadership Team and Deputy Chief Executive when appropriate Supports the oversight of our information management practices and decision making via the Information Governance Group and sub governance groups.
3rd	Internal Audit (and external	Performs periodic audit activities intended to assess and/or provide insights into (among other things) compliance with the Policy and the adequacy and

LOA:	Role	Monitoring & Oversight
Line	providers)	effectiveness of the Group's practices to monitor compliance and deal with breaches Reports to the Executive and the Board on the outcomes of such activities.
4th Line	Deputy Chief Executives	Ensures each Group has sufficient emphasis on risk management and meeting compliance obligations Ensures effective processes and monitoring are in place to meet compliance obligations for the Policy Acts in an appropriate and timely manner in response to reports received that alert the Executive to opportunities to improve Policy compliance activities.
5th Line	Board	Responsible for approving any material changes to the level 1 Policies, including text related to monitoring and oversight of compliance with the Policy Acts in an appropriate and timely manner in response to reports received that alert the Board to opportunities to improve Policy compliance activities.

This policy will be formally reviewed every 2 years. We acknowledge the changing information management landscape may require policy changes and updates more regularly where technology or best practice changes.

Where practicable these changes will be managed through standards and best practice guidelines.

9 Breaches of Policy

Complying with all policies and procedures is a requirement outlined in the Code of Conduct. Behaviour or actions that are investigated and found to be in breach of the Code of Conduct may result in disciplinary action. Refer to Code of Conduct for further information.

10 Contacts

The Information Management team can be contacted in relation to any queries regarding this policy.

11 Definitions

Our Information	All data and information produced by ACC, and all information under our care regardless of to whom it belongs, or where it originated.
Custodian and Steward	As defined in the Information Stewards and Custodians Standard.
Information	All recorded forms of data, knowledge, facts, intentions, opinions, or analysis, irrespective of the content, or the medium through which it is communicated or stored. Information may be contained in a variety of media, for example: printed documents, handwritten notes, diaries, maps, spatial data, photographic

	data, images, videos, electronic databases, electronic documents, emails, web pages, voice mail and audio records.
Information Architecture	The structured organisation of information and its relationship to business processes and systems. This excludes technical system design.
Information management	The creation and maintenance of complete, accurate and reliable evidence of business transactions in the form of recorded information.
Information Repository	An environment (either electronic or physical) where information is registered, stored, and managed.
Records	A record is any documentation or evidence of business activity and decisions, regardless of format.
Retention and Disposal Schedule	A systematic listing of the records created by an organisation, which informs their lifecycle management from creation to disposal.

12 References

This Information Management Policy is supported by the Information Management Governance structure in Appendix 2. Supporting sub policies, standards, procedures and guidelines are outlined in Appendix 1.

The legislative requirements that our information assets must meet are listed under Appendix 2.

13 Version Control

Version	Date	Material change reason	Who
0.1	13/07/20	Initial Draft	Outside of scope
0.2	26/7/20	EDIS review completed	
0.3	21/9/20	Feedback from reviews added	
0.4	12/10/20	Final preparation for GG's	
0.5	16/04/21	Amendments for Board (minor)	
0.6	26/07/22	Update roles to reflect new organisation structure	

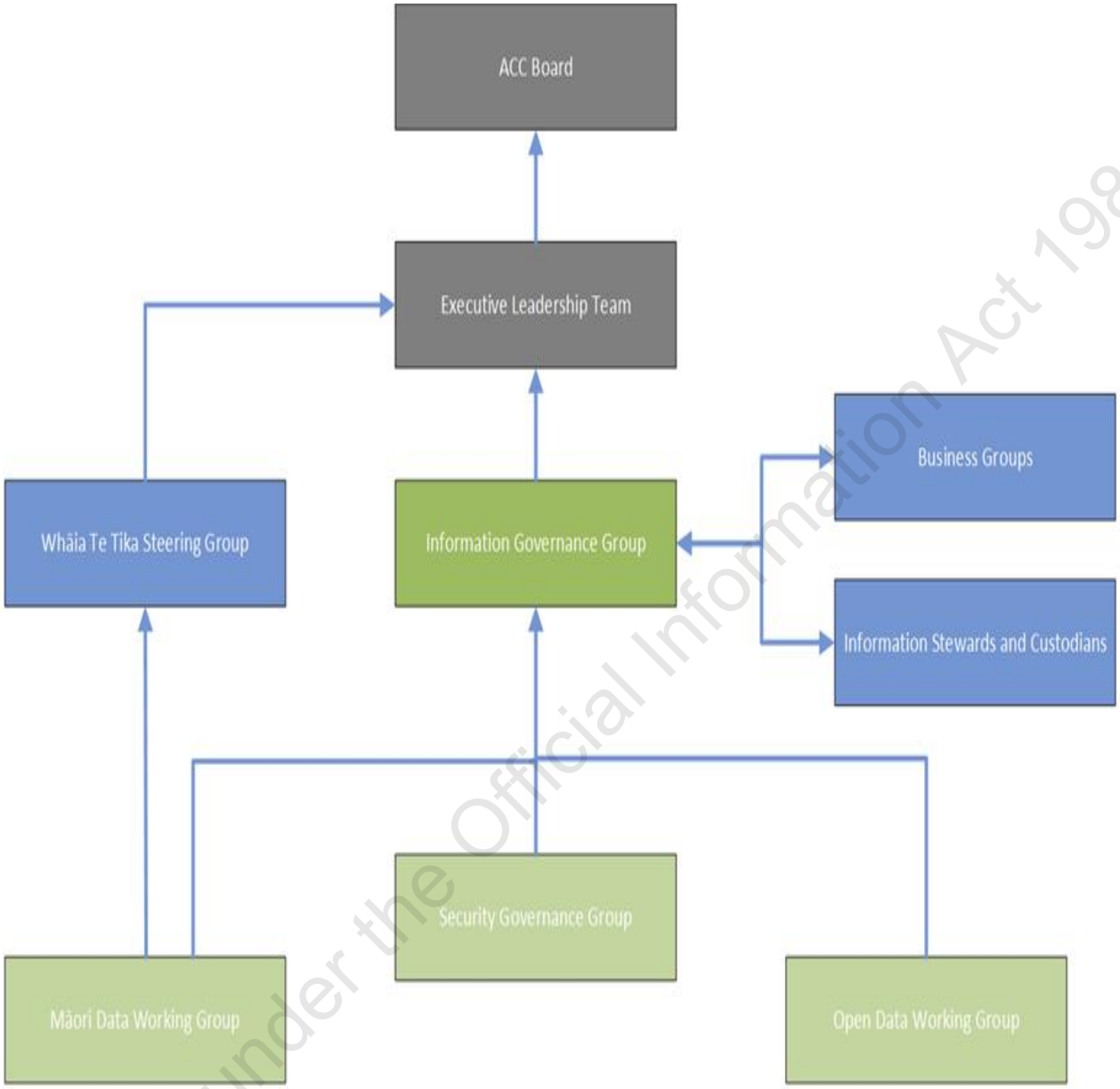
14 Appendices

Please note the following appendices are informative only they are accurate as of the time of publication and should not be considered an authoritative list or source given the changing policy and legislative landscape.

13.1 Appendix 1: Supporting Documentation

Subordinate Policies and Standards
Information Security Policy (Tier 2) Privacy Policy (Tier 2) Cloud Computing Policy (Tier 2) Use of the Internet Policy (Tier 3) Email and Instant Messaging Policy (Tier 3) Information Management Standards (omnibus document) Information Security Standards (omnibus document) Stewards and Custodians Standard Cloud Collaboration Standard
Associated Technology Policy and Standards
Telephony Policy (Tier 3) BYOD Policy (Tier 3) Modern Device Standards Vendor Device Standard
Related Acts, Standards and Codes
Accident Compensation Act 2001 Privacy Act 2020 Public Service Act 2020 Health Information Privacy Code 1994 Public Records Act 2005 Health Act 1956 New Zealand Public Health & Disability Act 2000 Tax Administration Act 1994 Copyright Act 1994 Official Information Act 1982 Contract and Commercial Law Act 2017 Evidence Act 2006 Financial Reporting Act 1993 Public Finance Act 1989 and Public Finance Amendment Act 2004 Resource Management Act 1991 and Resource Management Amendment Act 2005 State-Owned Enterprises Act 1986 Health and Safety in Employment Act 1992 New Zealand Public Health & Disability Act 2000 Data Content Standards (data.govt.nz)

3.2 Appendix 2 – Information Governance Boards



3.3 Appendix 3 – Alignment with Government

As a crown entity, ACC is expected to conform and adhere to government policies and practices related to information management as specified by appointed officials. In addition, as ACC is viewed as part of the health & disability sector, we also need to conform to specific sector requirements.

All-of-Government Official Functions (www.digital.govt.nz)

The NZ Government has established functional leads who are charged with developing and improving designated areas across government. The roles are delegated to specific chief executives by the Public Service Commissioner.

The roles are:

1. Government Chief Digital Officer (GCDO) oversees the development and management of digital for the state sector. The GCDO is responsible for:

setting digital policy and standards

improving investments

establishing and managing services

developing capability

system assurance (assuring digital government outcomes)

2. Government Chief Data Steward (GCDS) supports the use of data as a resource across government to help deliver better services to New Zealanders. The GCDS is the government functional lead for data and ensures that government agencies have the capability and right skills to maximise the value of data. This is achieved through setting data standards and establishing common capabilities, developing data policy and strategy, and planning across the state sector. Focus has been on:

    - Co-developing a Data Stewardship Framework to enable agencies to manage data as a strategic asset and benchmark their data maturity
    - Leading the government's commitment to accelerate the release of open data, including the implementation of the International Open Data Charter
    - Developing data governance across the system through evolving approaches to data ethics and Māori data governance.

3 Government Chief Information Security Officer (GCISO) role strengthens Government decision making around Information Security and supports a system-wide uplift in security practice. The GCISO is the government functional lead for information security. The GCISO's work includes:

    - coordinating the government's approach to information security
    - identifying systemic risks and vulnerabilities

- improving coordination between ICT operations and security roles, particularly around the digital government agenda
- establishing minimum information security standards and expectations
- improving support to agencies managing complex information security challenges.

4. Government Chief Privacy Officer (GCPO) leads an all-of-government approach to privacy to raise public sector privacy maturity and capability. The role sits within the Digital Public Service branch of the Department of Internal Affairs, reporting to the Government Chief Digital Officer. The GCPO is the practice lead for privacy and supports government agencies to meet their privacy responsibilities and improve their privacy practices. The GCPO is responsible for:
   - providing leadership by setting the vision for privacy across government
   - building capability by supporting agencies to lift their capability to meet their privacy responsibilities
   - providing assurance on public sector privacy performance
   - engaging with the Office of the Privacy Commissioner and New Zealanders about privacy.

Statistics NZ (data.govt.nz)

Statistics NZ (as GCDO) is responsible for overseeing official government statistics. Tier 1 statistics are New Zealand's most important statistics, and are essential to help the Government, business, and members of the public to make informed decisions and monitor the state and progress of New Zealand. Tier 1 statistics describe New Zealand s economy, environment, population, society, culture, international relations, and civil and political rights. Tier 1 statistics are also used by a range of organisations to develop new services and products.

One of the 162 Tier 1 statistics is the incidence of injuries annually produced by Statistics NZ using ACC and MoH data.

As ACC supplies data to produce a Tier 1 statistic, ACC must ensure that the Tier 1 statistic is of good quality and has integrity. Producers of Tier 1 statistics must adhere to the Principles and protocols for producers of Tier 1 statistics. Tier 1 statistics must be presented impartially and clearly without judgement and must be managed in such a way to ensure that the statistics are free from undue influence.

Ministry of Health

The Health Information Standards Organisation (HISO) with the Ministry of Health supports and promotes the development and adoption of fit-for-purpose health information standards for the New Zealand health system. HISO works with health providers and shared services organisations, clinical and consumer groups, software vendors and industry bodies, the academic community, the wider government sector and other standards development organisations. It also supports *He Korowai Oranga: Māori Health Strategy* for the effective delivery of health and disability services to Māori and represent the interests of all New Zealanders as consumers of health services and stakeholders in the health system.

HISO links with the international standards community through Standards NZ, SNOMED International for SNOMED CT, and through HL7 New Zealand for HL7 standards.

As a participant in the Health & Disability Sector, ACC is expected to adhere and support the standards produced by HISO.

PREVENTION. CARE. RECOVERY.

Te Kaporeihana Āwhina Hunga Whara

Information Management STANDARDS

Business Group	Enterprise Change Delivery
Author	Outside of scope
Date	August 2022
Next Review Date	August 2025
Version	2.0

Table of Contents

Contents

1 Introduction

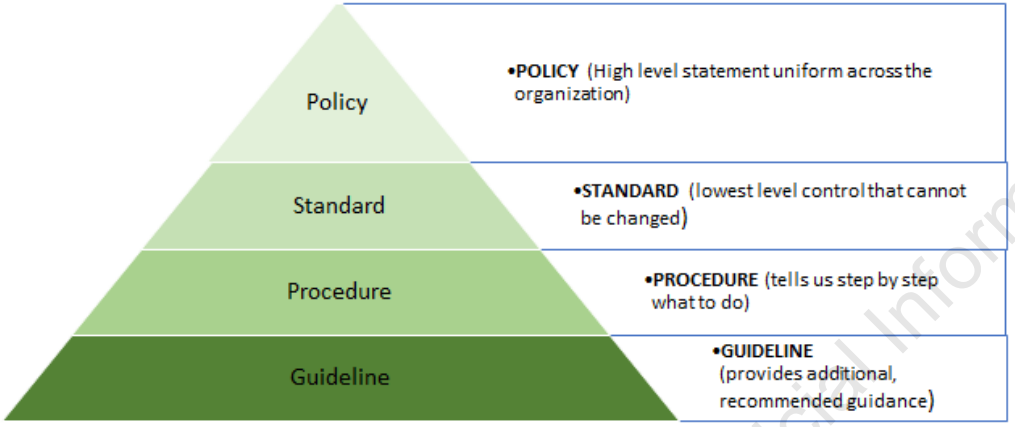
1.1 Purpose

Information is the only enduring asset that ACC holds and should be treated as such. This aligns with the Māori Data Sovereignty principle of viewing information as a treasure (Māori: taonga). In recognition of the obligations under the Treaty of Waitangi (Māori: Te Tiriti o Waitangi).

The purpose of this document is to collate the set of minimum standards that must be applied in relation to information management at ACC.

1.2 How to apply standards

This standard has been developed in line with the Corporate Policy Governance Model's definition of Policies, Standards, Procedures and Guidelines as reflected in the diagram below.



1.3 Key relevant documents

Related Acts, Policies and Standards
Accident Compensation Act 2001
Privacy Act 2020
Copyright Act 1994
Public Records Act 2005
Archives NZ Information and Records Management Standard
ACC Information Management Policy
ACC Information Security Policy
Archives NZ Destruction of Source Info mation After Digitisation

1.4 Definitions

Term	Definition
Authoritative source	A trusted record viewed as a reliable source of information because it can be proved that it has not been tampered with.
Core business system	An authoritative source (a location, technical system, or repository) of data or information within ACC.
Dissemination	To disperse, spread, or share information internally or externally.
Information and records system/ information repository	A system which captures, manages and provides access to records over time e.g. EOS, Guidewire, Salesforce, Te Kahu, SharePoint, etc.
Information lifecycle	When properly managed, every piece of information that is created progresses through a life cycle. The life cycle is divided into five stages: 1. Create/Collect 2. Organise 3. Use and Share 4. Maintain and Protect 5. Retain and Dispose

Intellectual Property	Intellectual property is an intangible asset and refers to creations of the mind: inventions, literary and artistic works, symbols, names, images, and designs used in commerce
Metadata	Information about a piece of information or data which describes the characteristics and attributes of that piece of information or data.
Record	A record is any documentation or evidence of business activity and decisions, regardless of format.
Retention and disposal schedules/ Disposal Authority for ACC records	Retention and disposal schedules set the length of time that ACC keeps certain types of records and the processes for disposing of records at the end of the retention period. The schedules are available on the Information Management Portal at Information disposal and managing documents/records (sharepoint.com)
Shared Drive	At ACC, the phrase 'Shared Drive' refers to the I:\ Drive, J:\ Drive, SharePoint or any ACC Cloud solution where information is created, stored, searched and shared.

1.5 Roles and responsibilities

ACC has adopted the 5 Lines of Assurance (5LoA) model for enterprise risk management and assurance. This model defines the high-level expectations for the Board, Executive, managers, specialist functions and independent assurance providers in identifying, assessing, deciding and assuring about risk in ACC.

The following table demonstrates how the 5LoA model maps to ACC's roles and responsibilities to establish accountability.

Role	Responsibilities
1st Line **All Staff**	• ACC has a legal obligation to comply with the Information Management requirements of the following acts: ▪ Public Records Act 2005 ▪ Accident Compensation Act 2001 ▪ Privacy Act 2020 ▪ Copyright Act 1994 • Staff wilfully and knowingly acting in a manner that breaches these obligations are in breach of the ACC Code of Conduct and may be subject to disciplinary actions • All staff are to comply with the Information Management Policies.
	• All ACC Staff must create full and accurate records of their daily business activity. This includes recording activities, transactions and decisions made when dealing with clients, providers and staff
	• People managers will ensure their staff: ▪ are aware of ACC's Information Management Policies and associated procedures ▪ follow the above policies and procedures

2nd Line **Specialist functions including Risk and Compliance Office (RCO)**	• The Information Frameworks and Assurance Team will support ACC staff by providing a framework to systematically manage ACC information and records • The Information Management Team will support ACC staff by facilitating access to Share Drives and SharePoint sites.
	• People managers and project managers will ensure their staff and teams comply with the requirements of the Copyright Act 1994.
3rd Line **Assurance Services**	• Enterprise Data and Information teams and Information Security teams will conduct periodic audits and support investigations as required in collaboration with RCO and Assurance.
	• Enterprise Data and Information teams and Information Security teams, in collaboration with RCO and Assurance, will conduct periodic audits and support investigations into misuse as required.
4th Line **CEO and Deputy Chief Executives**	The Deputy Chief Executive Enterprise Change Delivery will place organisational controls in support of these standards
5th line **ACC Board**	The ACC Board has overall responsibility for implementing effective risk management. They will review and assesses CEO's and Deputy Chief Executives' reporting and management of objectives

2 Standards subject specific content

2.1 Records management Standard

Many ACC documents are also records. A record is any documentation or evidence of business activity and decisions, regardless of format. All business decisions made must have a record to support the decision and must be stored in an appropriate and accessible location.

ACC staff members, **must,** as part of their daily work:

- Create, and maintain, full and accurate records of your work to provide evidence of your activities or decisions
- Capture all your work records into ACC's core systems, not your personal H:\ drive, email/calendar, or OneDrive/OneNote
- Name your records so that they can be found and reused in the future (see 2.8 below)
- Ensure that, while working at ACC all your work records are:
    - Accessible to authorised ACC staff, now and after you depart
    - Usable, i.e. not corrupted or incomplete
    - Retrievable, i.e. appropriately named and stored in a standard location, e.g. on the shared drive or the Document Store
    - Preserved for future use.

Meetings may be recorded for minute taking purposes only. It must not be kept as the official minutes of a meeting where any business decisions are made.

People managers must ensure their staff are aware of, and follow, ACC's Information Management policies and procedures.

2.1.1 Agile Release Trains

Product Managers are responsible for maintaining the formal records of their release train and **must**:

- Ensure that release train files (electronic and/or physical) are created at the beginning of a release train
- Ensure all historical information is captured and filed as appropriate
- Ensure that all members of the release train team save their work to the release train file

When deciding which release train records to retain, Product Managers should consider:

- The significance of the release train's contribution to the functions performed by ACC
- The importance of the release train to the development of ACC within the New Zealand government infrastructure
- Any residual value to the creators

2.2 Disposal of ACC records Standard

ACC formally contracts record retention and disposal with Archives New Zealand. This contract sets out:

- The many classes (types) of records ACC creates
- How long we must retain records of each class when they become non-current/are no longer active (this varies from months to decades)
- Our disposal action when the retention period ends (destruction, retention, or transfer to Archives NZ for their collection).

Only members of the Information Management team (IM) are permitted to authorise a disposal action.

In the case of missing and lost files or if files are inadvertently disposed of, the Information Management team must be notified immediately.

For help with managing ACC record disposal (including personal work records), email the Information Management team.

2.3 Clear desk Standard

ACC employees must secure all information in their workspace. This includes securing both electronic and physical information:

- At the end of the work day
- When they expect to be away from their workspace for an extended period.

Computer workstations/laptops must be locked (logged out or shut down) when unattended and secured at the end of the work day.

Mass storage devices such as CD, DVD, USB drives, or external hard drives must be locked away when not in use.

Printed materials must be immediately removed from printers or fax machines.

Avoid printing physical copies - documents should be viewed, shared and managed electronically whenever possible.

All documents that:

a) are no longer required, **and**

b) can be destroyed because they do not need to be kept as records of ACC decisions or actions

must be placed in the designated blue shredder bins for destruction.

Storerooms, filing cabinets and drawers must be kept closed and locked when unattended and not in use.

Keys and physical access cards must not be left unattended anywhere in the office.

Each team manager is responsible for enforcing the above standards. Repeated or serious violations of the clear desk standard can result in disciplinary actions in accordance with ACC's Code of Conduct.

If devices or documents go missing, or a workspace may have been tampered with, staff **must** notify InfoSec@acc.co.nz immediately.

2.4 Classification and labelling Standard

The New Zealand Protective Security Requirements (PSR) require ACC to protectively mark information to help keep official information secure. They are a visual reminder of the security measures that apply to information or equipment.

Document classification or markings can be applied to a document manually, or automatically using the Microsoft AIP (Azure Information Protection) tool where available.

Documents with a protective marking or classification **must** be reviewed regularly and declassified when appropriate.

ACC staff who wish to classify or declassify a document but don't know how to do so must contact the Information Security team for advice.

Documents stored on ACC servers may be scanned for sensitive content and where found, may have appropriate security classifications applied automatically.

ACC uses the following security classifications:

UNCLASSIFIED

- Official information that doesn't need a security classification is called 'unclassified information. Most official information fits this category. **UNCLASSIFIED** isn't a formal security classification; is used as a protective marking. It shows a document has been reviewed and the impact from unauthorised disclosure or misuse has been assessed.
- Within ACC, **UNCLASSIFIED** is used to show a document has been assessed, or where an endorsement marking (q.v. 2.4.1 below) may be required on an otherwise unclassified document.
- **UNCLASSIFIED** may also be applied as the default classification for documents subject to software-applied automatic classification.

IN CONFIDENCE

The ACC endorsement markings for IN-CONFIDENCE information are:

- CORPORATE-IN-CONFIDENCE

  Records related to privacy, strategy, risk, compliance, assurance, policy, OIA, and information and technology assets. Strategic finance functions including budgeting, accounting, and financial reporting.

- LEGAL-IN-CONFIDENCE

  Includes all ACC legal advice and litigation records.

- COMMERCIAL-IN-CONFIDENCE

  Includes all records related to ACC Investments, cashflow analysis and monitoring, performance analysis reporting, financial accounting and reporting for investment products and procurement.
  Examples: investments, bonds, draft requests for offer information, tender responses, tender evaluation.

- STAFF-IN-CONFIDENCE

  Includes all ACC staff records
  Examples: personnel files, recruitment information, grievance or disciplinary records.

- EXECUTIVE-IN-CONFIDENCE

  Includes decisions and information associated with executive management of ACC. Such as that data that would normally be restricted to the executive and nominated authorised staff. For example, sensitive financial information created for executive management of ACC.

- CUSTOMER-IN-CONFIDENCE

  Includes all claimant, provider, business customer, and injury prevention records.

In Confidence classifications are used when compromising the information is likely to:

- Prejudice the maintenance of law and order
- Impede the effective conduct of government
- Adversely affect the privacy of New Zealand citizens.

For instance, when the compromise of information could prejudice:

- Citizens' commercial information
- Obligations of confidence
- Measures for protecting the health and safety of the public
- The substantial economic interest of New Zealand
- Measures that prevent or mitigate material loss to members of the public.

Or when a compromise of information could:

- Breach constitutional conventions
- Impede the effective conduct of public affairs
- Breach legal professional privilege
- Impede the government's commercial activities
- Result in the disclosure or use of official information for improper gain or advantage.

When ACC receives documents with a higher security classification, for example from NZ Police, we must ensure they are appropriately declassified before being stored in ACC systems.

ACC **IS NOT** certified to receive, or store documents classified above **IN CONFIDENCE**.

ACC **must** take reasonable care to ensure we do not accept, or store, these documents unless they have been correctly declassified.

Where a document is received that has classification above **IN CONFIDENCE** staff **MUST** contact the Information Security and Privacy teams before dealing with the document.

If staff receive a document with a protective marking and don't know what to do with it, they should contact the Information Security Team at infosec@acc.co.nz

2.4.1 Endorsement markings

Endorsement markings warn people that information has special requirements.

They may indicate:

- the specific nature of information
- temporary sensitivities
- limitations on availability
- how recipients should handle or disclose information.

ACC acknowledges some business areas may need endorsement markings.

Endorsement markings **must** only be implemented where a clear business case exists. The Chief Information Security Officer (CISO) must approve a process for classification, handling and declassification of documents before endorsement markings can be used.

Business units that require endorsement markings should first consult the Information Security Team and read the following: Endorsements | Protective Security Requirements

2.5 Copyright Standard

2.5.1 Copying materials at ACC

ACC staff must only copy materials within the provisions of the Copyright Act 1994. Just because an item, image or file is found on the internet does not mean it is legal to download/copy or use it.

ACC staff are responsible for determining if copyright law applies. This is often the case even if the copyright symbol © isn't present.

'Copying' includes:

- Photocopying
- Duplicating an e-book, or sharing an e-book that is licensed for single-use only
- Copy-and-pasting text, images, or other files from the internet
- Right-mouse click Save As, or "snipping" an image online
- Scanning a document
- Copying the content of a document word-for-word, either by hand or typed.

2.5.2 What qualifies for copyright protection?

Copyright doesn't depend on the physical format of an item. For example, copyright may exist in:

- Written works such as novels, poems, articles, notes and song lyrics.
- Works of dance or mime and scenarios or scripts for films and plays.
- Paintings, drawings, plans and maps.

- Musical scores or arrangements.
- Sound recordings.
- Films, which includes DVDs, Blu-Rays and digital downloads.
- Communications including broadcasts or cable programmes.

2.5.3 What doesn't qualify for copyright protection?

Copyright protection does not apply to some government works, such as:

- Parliamentary bills
- Acts of Parliament
- Regulations
- Bylaws
- Parliamentary debates
- Select Committee reports
- Court and tribunal judgements
- Reports of royal commissions, commissions of inquiry, ministerial inquiries or statutory inquiries.

Be aware that reprints or publications of this material by non-governmental parties may have copyright.

2.5.4 Creating a reference or citation for an item

When using a copyrighted piece of work, reference its title, author, date and other distinguishing information so that the work can be identified and re-acquired in the future. Use a recognised referencing style, such as:

- Harvard System of Referencing Guide
- APA (American Psychological Association) Referencing Guide
  MLA Referencing Guide.

2.5.5 Client files and Copyright materials

Staff working with copyrighted material included in ACC client files must be fully informed and trained on their responsibilities:

- Copyright material must only stay on client files while it is actively used for research purposes. Once the research is complete, the copyright material must be cited appropriately and then removed from the file and destroyed.
- If copyright material is required for a review, hearing or appeal, this is permitted by section 59 if the Copyright Act as a "Parliamentary and judicial proceeding". ACC reviews and appeals meet this definition, but Alternative Dispute Resolution (ADR) does not.
- When archiving a file, cite any research material it contains. If the research material is required in the future, the IM team can retrieve a new copy for ACC staff.
- Copyright material on a client file must not be reproduced nor distributed with the file. If the copyright material is intended for research, or private study by the client and/or their advocate(s), then release is allowed.
- Section 43 of the Copyright Act ("research or private study") sets out the amount of material that can be copied.
- Only material required for research may be scanned into a Virtual Client Folder (VCF). Scanned copies must be replaced by citations when the client file is archived.

2.5.6 Information taken from library research databases

ACC purchases access to external internet-accessible databases, such as Medline and ProQuest. Information from these databases must not be shared with third parties.

2.5.7 Technology systems and software

Technology system specifications must include copyright compliance as part of their business requirements. The Commercial Strategy and Services team is responsible for ensuring software licensing agreements comply with the provisions of the Copyright Act.

2.5.8 Copyright infringements

The Manager Information Management is responsible for responding to notifications of suspected copyright infringements. As per the requirements of the Act, a response is required within fourteen working days of receipt.

2.5.9 Contact for information

Email copyright policy queries to the Information Management team.

2.6 Physical document storage Standard

Before deciding to archive a physical document, it **must** first be considered for digitisation

Staff sending a physical document for offsite storage must clearly and accurately name the document so it can be readily found and/or re-used when required in the future.

When staff send cartons of physical documents to offsite storage, they must compile and include a *transmittal list* in each carton. This list must describe all the contents in enough detail for the physical documents in each carton to be identified and re-used as required.

Physical files can be archived at ACC as corporate records, open claim files and archived claim files.

2.6.1 Corporate records

Corporate records include all records created within the corporate office such as Finance, HR and office administration.

Where possible, these must be digitised and stored in an appropriate digital system of record.

2.6.2 Open claim files

Open files are active client files, stored temporarily, with our offsite storage provider. They are file managed with individual barcodes.

Lodging and retrieving open claim files off-site is done through the ReQuest online web tool.

2.6.3 Archived physical claim files

In Eos, the “archived” status indicates the physical record has been sent to offsite storage.

Claim files are closed in Eos in preparation to be sent to offsite storage.

2.6.4 Onsite physical records

Any business-related records, for example personnel files, should be stored in digital form only.

Where the physical file is required, it must be listed and stored in secured filing cabinets or with ACC's offsite storage provider.

This listing must be stored within a corporate shared drive and updated as required

For queries about the offsite storage of physical documents, email the Information Management team or refer to the SharePoint page 'Managing your documents'.

2.7 Digitisation and Digital document storage Standard

Staff uploading a digital document to an ACC core system (e.g Eos, Hyperion, Promapp, Oracle Financials or SharePoint) must comply with the applicable system's uploading standards. This includes complying with all relevant document naming conventions or practices.

Physical documents digitised for archiving/storage **must** comply with the Archives NZ recommended standards for the digitisation of text and photographic prints.

- **Bit depth**: 8 bit. Greyscale or bi-tonal. **Resolution**: 300 ppi. **File Format**: PDF/A, TIFF, JPEG 2000. **Compression**: Lossless compression
- **Bit depth**: 24 bit. Colour. **Resolution**: 300 ppi. **File Format**: PDF/A, TIFF, JPEG 2000. **Compression**: Lossless compression.

If in doubt, read the system documentation or ask the Information Management team for guidance.
Additional information about post-digitisation information disposal can be found here: Archives NZ advice

2.8 Document naming Standards

Naming documents consistently and accurately will allow ACC staff to find documents when they need it. This means documents can be found no matter where in ACC the document was created, or how long ago.

Inconsistent document naming leads to future problems, including:

- Lowering the chances of finding all relevant documents when searching. This means we risk making decisions based on incomplete knowledge
- Confusion over which version of a document is authoritative, which reduces staff confidence and trust in the systems
- Introducing compliance risk under the Accident Compensation, Privacy, Public Records, and Official Information Acts.

2.8.1 Document file names

File names should describe the document's content while being as brief as practical. The file name should let users find the document using search functions even when it is stored in an unexpected location.

2.8.2 Guiding principles

When naming documents, ask:

- does your file name clearly identify the document's content or purpose?

- did you use words that will still make sense to you when in six months' time you are searching for the document?
- that your file name is meaningful enough so that others using search to look for the document will easily locate it.

Aim to strike the right balance between:

- **Brevity**; keeping titles short. Thirty characters is a sensible maximum name length
- **Usability**; usefully describing the document's content

Personal names

Personal names should not be used as part of file names.

Where it is appropriate to use a personal name in a file name (e.g. staff management documents), use the following format:

First name Last name, for example **Josephine Bloggs** Avoid **Bloggs, Josephine** or **J Bloggs**

Corporate names

When using a corporate name in a file name, use the full form of the name unless its acronym is commonly accepted.

Do not use initial articles in corporate names, e.g. use Treasury, not ***The*** Treasury

Date Format

When identifying an event that occurred on a specific date, use the format **dd month yyyy** (e.g. Debrief – Security alert Shamrock House - 20 July 2022)

Note: a document's creation date is captured automatically as metadata in many systems. As such, the creation date may not be needed as part of the file name.

Dates should only be used in file names to:

- identify a specific event (e.g. an incident, report, meeting, etc.), or
- distinguish between similar documents (e.g. recurring meetings, weekly/monthly/quarterly/ reports)

Acronyms

Acronyms should not be used as part of a file name unless widely recognised e.g. ACC for Accident Compensation Corporation, or MOH for Ministry of Health.

Do not use punctuation such as full stops within the acronym (use NATO not N.A.T.O).

Write all acronyms in uppercase.

Abbreviations

Abbreviations (e.g. rpt, mtg, proc) **must not** be used in file names.

2.8.3 System Specific Guidance

A short-form desktop guide to naming documents for SharePoint is available at Naming your documents (sharepoint.com)

Email queries regarding ACC SharePoint naming standards to the Information Management team.

2.9 Metadata Standard

Where supported, all ACC documents **must** be saved with appropriate Metadata so the documents are searchable and discoverable.

At a minimum, this Metadata should include enough information for a user to find a document using a search engine.

Many ACC systems will automatically label documents with appropriate Metadata

Contact the Information Management team with any concerns or requests for further information.

Personal Information and Privacy Policy

POLICY NUMBER	5.3.0
TOPIC	Care and protection of personal information; privacy
OWNER	Head of Privacy
DATE APPROVED	8 September 2022
APPROVER	Board
DATE OF NEXT REVIEW	25 February 2023

1 Objective

This Personal Information and Privacy Policy (policy) sets out how ACC collects, stores, uses, discloses, retains, and protects personal information.

Personal information is taonga (treasured), and we consider ourselves to be kaitiaki (guardians) of any personal information we receive. For the purposes of this policy, personal information includes health information. We are committed to managing personal information in line with the Privacy Act 2020, the Health Information Privacy Code 2020, any related legislation and recognised best practice.

We have a wide range of statutory functions and duties under the Accident Compensation Act 2001. We collect, use, store and share personal information to fulfil those functions and duties, as well as for related lawful activities. We are entrusted with personal information. It is fundamental that we protect this information and use it only for permitted purposes and in appropriate ways.

Key to our goal of Stewardship/Kaitiakitanga is the value we create for our public and for our partners, including our Māori Treaty partners. Maintenance of public trust and support for the scheme and how we deliver it is critical to the sustainability of the scheme. In order to achieve this everyone at ACC must be well-equipped to protect the personal information entrusted to us by our clients, our people, our providers, and our businesses.

2 Scope

This policy applies to all ACC people, including employees, secondees, and independent contractors.

This policy applies to all personal information we collect and have access to. This includes all information held on claim files about our clients and our people (ACC staff claims), together with all information about our people, providers, and businesses.

This policy is supplemented by the Personal Information and Privacy Guidelines, which further detail how we collect, store, use, disclose, retain and protect personal information.

3 Policy statements

The policy is underpinned by the principles and rules of the Privacy Act 2020 and Health Information Privacy Code 2020. These govern how agencies manage personal and health information throughout the information lifecycle: collection, storage, access, correction, use and disclosure.

3.1 We collect, use and store personal information to carry out our functions and responsibilities under the Accident Compensation Act 2001, as well as for related lawful activities.

We collect, use, and store personal information to perform our functions and responsibilities including as set out in section 3.4 below. Personal information may be obtained from clients, health providers, employers, and other agencies. We also collect personal information about other individuals including our people, providers, and businesses. ACC people who receive or gather information for us are directed by internal guidelines, procedures and training that specify the boundaries of collection and its use.

3.2 We commit to making people aware of the collection of personal information

When collecting personal information from our people, businesses, clients, health providers, employers and other agencies, we must inform them of:

- the purposes for collection
- who will receive their personal information
- any laws under which we are authorised to collect their personal information (such as the Accident Compensation Act 2001)
- what could happen if the client does not provide the personal information we need, and
- their rights to access and request correction of that personal information

We will only collect personal information by means that are lawful, fair and do not intrude unreasonably on an individual's pe sonal affairs. "Fair and reasonable" in this context means we will aim to collect personal information from individual clients rather than third parties unless there is a lawful reason for doing otherwise. When collecting information from third parties we obtain consent from the individual concerned, unless there is a good reason why consent is not required.

We will inform our customers and our people of our purpose for collection and their rights to access and correct that information. Irrelevant and unnecessary personal information will be returned to the supplier or destroyed where practicable.

3.3 We facilitate access to and respect an individual's right to seek amendment of factually incorrect personal information as a key priority

We commit to providing individuals with access to their personal information unless an exception under the legislation applies. Requesters are verified and the information is provided to them within legislative timeframes and boundaries.

We commit to keeping personal information accurate and up to date. We have a clear process for handling amendment requests which our people follow. If there is good reason for not amending the information, we will invite the individual to submit a statement of correction and we will ensure that it is read together with the original document in future.

3.4 We commit to using personal information only for the purpose for which it was obtained and other lawful purposes.

We only use personal information for the purposes for which it was collected, for directly related purposes, and for the purposes of carrying out the Scheme and lawful functions related to ACC, except where limited statutory exceptions apply.

We primarily use information to:

- assess and provide entitlements to compensation, rehabilitation and medical treatment
- assist the evaluation of our services and performance
- contribute to research into injury prevention and effective rehabilitation
- develop policy
- ascertain levy payments and maintain the scheme (including a claims database)
- facilitate training, quality monitoring, system testing and continuous improvement purposes
- enable effective rehabilitation outcomes by sharing relevant information with our partners (employers and providers) to allow them to play an active role in supporting injured people
- act as an employer, which requires us to collect and use personal information about our employees for work purposes
- conduct investigations (including for integrity issues)
- respond to information requests

In line with ACC policies and guidelines, only relevant information is used for any given purpose, including where use involves disclosure.

Where personal information is not relevant or necessary for an activity, all reasonable efforts will be taken to anonymise, cleanse, or otherwise remove personal information.

3.5 Personal information is disclosed to other parties only where there is authority to do so

We may use and disclose personal information to fulfil our legislative obligations and protect the health and safety of our clients, staff and third parties.

We will primarily disclose personal information with the informed authority of the individual concerned. We may also disclose information where authority has not been granted by the individual concerned. In all instances, any disclosure will be with authority either granted by the individual concerned or granted by law.

We will take reasonable steps to ensure third parties protect the personal information we share with them in line with legislation and with the same care we give to it ourselves.

Where personal information may be disclosed outside of New Zealand, we will ensure it is afforded similar, reasonable care as is granted in New Zealand, in line with our legal requirements.

We commit to appropriately using unique identifiers when handling personal information.

3.6 We commit to storing personal information with reasonable safeguards against loss and disclosure and retaining it in line with legislative requirements

The personal information we hold is taonga and must be protected from loss, unauthorised access, use, modification or disclosure. This applies to our electronic systems and all personal information

stored in hard copy. Information regarding how ACC secures personal information is set out in the *Information Security Policy*.

We will store personal information in accordance with the Accident Compensation Act 2001 and Public Records Act 2005 (including disposal authorities as issued by the Chief Archivist). We commit to only holding information for as long as we have a legal reason to hold it.

If we identify we have received personal information that is not relevant to our functions and duties where reasonably practicable, it will be returned or destroyed securely.

3.7 We have clear, consistent processes for reporting, managing and escalating privacy incidents

ACC people or contractors should report a potential or perceived incident, either that they have observed or have contributed to, within 24 hours of becoming aware of the incident or as soon as practicable.

Privacy incidents are breaches or near misses of any of the privacy rules or principles, including this policy, by ACC people or parties contracted to us. Every incident needs to be reported to the Privacy Team and prompt steps will be taken to prevent or mitigate harm resulting from the incident and prevent its recurrence.

We will notify the Office of the Privacy Commissioner and the affected individual or individuals as soon as practicable (and typically within 72 hours) of becoming aware of a breach that we reasonably believe has caused or is likely to cause serious harm, or where we think it is otherwise appropriate to do so, aligned with best practice guidance and our legislative obligations.

We will use the data collected from privacy incident reports to gather insights and lessons learned for reporting purposes in order to better prevent future privacy incidents ensuring a continuous improvement approach to enhancing privacy practices.

3.8 Care of personal information is embedded in everything we do

We provide regular training to ensure both new and existing staff understand the relevant privacy principles for their role, what good privacy practice looks like, and how to appropriately report privacy incidents or raise concerns about privacy and inappropriate behaviour. We will apply a continuous improvement approach to our privacy practices; we will learn from mistakes and frequently review our processes and training to ensure it is fit for purpose.

3.9 We commit to ensuring we have effective policies and processes which reflect current best practice standards

We are committed to ensuring we have effective policies and processes which reflect the most up-to-date best practice standards.

How we handle the personal information in our care is governed by this policy, and our people are guided on best practice by our guidelines and documented processes. We are committed to maintaining and updating these policies, guidelines and processes, with an approach to both continuous improvement and fixed review schedules.

Our business practices and processes, related IT systems and networked infrastructure, have privacy proactively embedded into their design by the completion of privacy risk assessments, anytime they may affect the way we handle personal information.

We will keep our people informed on privacy best practice through regularly updated guidelines that meaningfully connect these policy statements with the work they do.

4 Accountabilities

Board responsibility for privacy and information management is set out in our Board Governance Manual. This acknowledges the Board is committed to managing personal and health information by:

- setting clear expectations regarding privacy and protection of personal information, and communicating them to the executive management
- holding executive management accountable for meeting those expectations
- ensuring effective privacy risk management is fully embedded within our overall risk management activities
- implementing high-quality monitoring and information management practices

Our managers are directly accountable for identifying and addressing privacy risks in their own units to ensure these are captured for reporting to the Board via the Head of Privacy.

All members of the Executive are responsible for driving strong enterprise-wide culture and practices for the care and protection of personal information.

The Deputy Chief Executive – Corporate and Finance, on behalf of the Executive, is accountable for ensuring supporting guidelines, operational measures and monitoring are in place.

5 Roles and Responsibilities

Role:	Responsibility
Board	• responsible for ensuring the organisation is aware of the need to protect our customers' information through high-quality monitoring and information management practices
Executive	• support the implementation of this policy • ensure corporate policies are appropriately endorsed • model best privacy practices and ensure privacy is core to all aspects of our culture •
Deputy Chief Executive – Corporate and Finance	• represents the Executive team in relation to all matters regarding privacy • responsible for ensuring organisational controls are in place to support and raise awareness of this policy; report and analyse privacy incidents to identify root causes of privacy incidents; and develop training to imbed privacy knowledge throughout ACC.
Head of Privacy	• ensures policies reflect relevant legislative or regulatory requirements, rules, standards and codes that apply to ACC • ensures policies include monitoring and oversight mechanisms that reflect the principles of the 5 Lines of Assurance

	• ensures policy content is accurate, relevant, complete and aligned with other related policies and the Corporate Policy Governance Framework • liaises with subject matter experts and relevant groups and committees, including the Enterprise Risk Team and external shareholders (for example: NZ Public Service Association) • ensures policies are communicated, and training activities and guidance documents are in place to support implementation of the policy • ensures mechanisms are in place to monitor compliance with privacy policies • considers and, if appropriate, approves policy exceptions • responds to and addresses any non-compliance issues and ensures processes are in place to identify, manage, record and report policy breaches and exceptions as appropriate • ensures policies are reviewed within a three-yearly cycle or as otherwise required • responsible for the management of the privacy function including: o breach and complaint management o measuring and reporting on our privacy performance o setting our privacy strategy o implementing our privacy maturity plan - privacy risk identification and mitigation o privacy stakeholder engagement
Privacy Officer and Privacy Team	• support compliance with this policy and the relevant legislation • oversee investigations into privacy-related complaints lodged with the Privacy Commissioner and ACC • ensure there is a process in place for responding to requests for access to, or correction of, personal information • participate, as required, in the development and review of this policy's standards and procedures to ensure they meet requirements • ensure the policy owner and leads are informed of any potential future changes that may affect a policy • identify privacy risks and mitigations
1st Line of Assurance	• Managers, People Leaders, and all ACC people should ensure appropriate processes and activities are in place to track compliance • each policy should include monitoring and oversight mechanisms that follow the principles of the 5 Lines of Assurance People Managers have specific responsibilities for: • notifying privacy incidents to their manager • proactively assessing and managing privacy risk • managing all privacy reporting requirements through the Privacy Reporting Tool • liaising with the People and Culture Group where necessary following privacy incidents to ensure consistent follow up with staff

	• owning the unit's Privacy Risk Register and ensuring it is kept current • ensuring ACC people are aware of and recognise the importance of their role in privacy • ensuring ACC people are aware of and compliant with our Personal Information and Privacy Policy, the Privacy Act 2020, the Health Information Privacy Code 2020 and complete their annual privacy training • ensuring new staff induction includes privacy training
Our people	• comply with this policy

6 Monitoring and Oversight

Our Personal Information and Privacy Policy and guidelines have been established to comply with the Privacy Act 2020 and Health Information Privacy Code 2020.

The monitoring and oversight of privacy follows the 5 Lines of Assurance model to provide assurance staff and third-party privacy risks are being managed effectively.

Lines of Assurance:	**Role**	**Monitoring & Oversight**
1st Line	Employees and People Leaders	• all employees: o remain alert to potential breaches of the Personal Information and Privacy Policy and report potential and actual breaches to their manager o maintain best privacy practice behaviours, promote privacy at work, comply with privacy policies, actively participate in privacy training and identify privacy risks • all people managers ensure: o privacy breaches and incidents (near misses etc.) brought to their attention are documented in the Privacy Reporting Tool, o notification of the breach is provided to the Privacy Team within 24 hours of the breach occurring, and o they act to resolve the privacy breach in a timely fashion, obtaining guidance and support from the Privacy Team as/when required
	Policy Owner	• ensures the Group (and other parts of ACC if applicable) responds appropriately to Policy breaches and requests for exceptions
	Enterprise Risk Team	• performs periodic oversight activities intended to assess and/or provide insights into (among other things) compliance with the Policy and the adequacy and effectiveness of the Group's practices to monitor compliance and deal with breaches • reports to the Executive and the Board on the outcomes of such activities
2nd Line	Privacy Team	• supports employees and leaders to determine whether events constitute actual breaches of the Policy

		• supports employees and Leaders to determine actions that are required as a result of the breach • completes root cause analysis of breaches • monthly reporting on our privacy breaches and Enterprise Risk Reporting to the Executive and Board • attestation compliance • delivery of the privacy programme • privacy assurance reviews • ownership of privacy policies and guidelines • specialist advice and support, including privacy-by design • escalates breaches to the Group's Leadership Team and Deputy Chief Executive – Corporate and Finance when appropriate • notification of serious breaches to Office of the Privacy Commissioner • updates risk registers as required
3rd Line	Internal Audit (and external providers)	• perform periodic audit activities intended to assess and/or provide insights into (among other things) compliance with the Policy and the adequacy and effectiveness of the Group's practices to monitor compliance and deal with breaches • report to the Executive, Risk Assurance and Audit Committee and Board on the outcomes of such activities
	Office of the Privacy Commissioner	• provides external monitoring and oversight of our compliance with the Privacy Act through its advice and complaints functions, and public reporting on these. The Commissioner can issue a compliance notice if we are not meeting our obligations under the Privacy Act.

4th Line	Executive	• ensures each Group has sufficient emphasis on building and maintaining privacy risk management and meeting compliance obligations
		• ensures effective processes and monitoring are in place to meet compliance obligations for the Personal Information and Privacy Policy
		• acts in an appropriate and timely manner in response to reports received that alert the Executive to opportunities to improve Personal Information and Privacy Policy compliance activities.
		• receives regular reporting on:
		  ○ privacy as an Enterprise Risk
		  ○ privacy compliance
		  ○ progress against the Privacy Maturity Assessment Framework (PMAF)

5th Line	Risk Assurance	• recommend any material changes to this policy

	and Audit Committee	

	Board	• responsible for approving any material changes to the Level 1 Policies, including text related to monitoring and oversight of compliance with the Personal Information and Privacy Policy
		• acts in an appropriate and timely manner in response to reports received that alert the Board to opportunities to improve Personal Information and Privacy Policy compliance activities
		• responsible for ensuring privacy risk management is in place and also responsible for setting the Privacy Risk Appetite Statement
		• receives regular reporting on:
		  ○ privacy as an Enterprise Risk
		  ○ privacy compliance
		  ○ progress against the Privacy Maturi y Assessment Framework

7 Breaches of Policy

We require any potential or perceived privacy incidents to be reported within 24 hours of becoming aware of the incident or as soon as practicable. This includes incidents that have been observed or directly contributed to.

Our Code of Conduct requires our people to comply with all our policies.

Breaches of this policy can result in a range of consequences for us and our clients.

While we strive to be good guardians of personal information, incidents will happen. When they do, our priority is to make things right. Accidental failures to achieve the standards in this policy will not normally be grounds for disciplinary action. Repeated or deliberate failures (including by failing to report a privacy incident) may result in disciplinary action.

8 Contacts

Questions regarding the interpretation or management of the policy can be directed to the Privacy Team.

9 Definitions

Health Information

Governed by the Health Information Privacy Code, 'health information' is the following classes of information about an identifiable individual:

a) information about the health of that individual, including their medical history;
b) information about any disabilities that individual has, or has had;
c) information about any health services or disability services that are being provided, or have been provided, to that individual;
d) information provided by that 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; and
e) information about that 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.

Personal Information

The Privacy Act 2020 governs 'personal information', that is:

a) information about a living, identifiable individual; and
b) including information relating to a death that is maintained by the Registrar-General under the Births, Deaths, Marriages, and Relationships Registration Act 1995 or any former Ac (as defined in section 2 of the Births, Deaths, Marriages, and Relationships Registration Act 1995).

Information may be personal information even if the individual concerned cannot be identified from the information itself, provided there is some other 'link' in information held by the agency which means the individual is identifiable.

That being the case, personal information may include information that does not actually identify the individual concerned, including information that is only about an 'identifiable' individual by reason of extrinsic knowledge or information, or information that can be linked to an identifiable individual through the use of other information.

For the purposes of this policy, ‘health information’ is included in the definition of ‘personal information’.

Privacy Maturity Plan

Formalises our approach to improving privacy maturity at ACC. It embeds a culture of information stewardship that aligns with the other being made to improve our customers' experiences.

Privacy Maturity Assessment Framework

A self-assessment developed by the Government Chief Privacy Officer to help agencies assess their privacy capability and maturity.

Serious Harm

Serious harm is not defined in the Privacy Act. Examples of serious harm include physical harm or intimidation, financial fraud including unauthorised credit card transactions or credit fraud, family violence, and psychological or emotional harm.

10 References

This policy should be read in conjunction with the Personal Information and Privacy Guidelines, the Privacy Maturity Plan, and the Information Management Policy.

11 Version Control

Version	Date	Change reason	Who
1.1	14/06/2018	Updated old version to new draft	Outside of scope
1.2	10/07/2018	Reflecting comments from Head of Privacy	
1.3	20/07/2018	Reflecting comments of Corporate Policy Review Working Group	
1.4	30/07/2018	Formatting and minor edits	
1.5	11/06/2021	Moved to new template and updated for Privacy Act 2020	
2.0	29/07/2022	Updated to new version to reflect recommendations from the Clark Independent Review	

Personal Information and Privacy Guidelines

Personal Information and Privacy Policy – Objective

ACC's Personal Information and Privacy Policy sets out how ACC collects, stores, uses, discloses, retains, and protects personal information.

Personal information is taonga (treasured), and we consider ourselves to be kaitiaki (guardians) of any personal information we receive. For the purposes of this policy, personal information includes health information. We are committed to managing personal information in line with the Privacy Act 2020, the Health Information Privacy Code 2020, any related legislation and recognised best practice.

We have a wide range of statutory functions and duties under the Accident Compensation Act 2001. We collect, use, store and share personal information to fulfil those functions and duties, as well as for related lawful activities. As such we are entrusted with personal information, and it is fundamental that we protect this information and use it only for permitted purposes and in appropriate ways.

Key to our goal of Kaitiakitanga (Guardianship) is the value we create for our public and for our partners, including our Māori Treaty partners. Maintenance of public trust and support for the scheme and how we deliver it is critical to the sustainability of the scheme. To achieve this everyone at ACC must be well-equipped to protect the personal information entrusted to us by our customers, our people, our providers, and our businesses.

Personal Information and Privacy Guidelines

These guidelines are designed to provide our people with meaningful and practical guidance on how to care for and use personal information in our daily activities, supplement ACC's Personal Information and Privacy Policy. It is important that everyone considers how these guidelines should be applied in the area that you work.

Who this appl es to:

Our Personal Information and Privacy Policy and these Guidelines apply to all ACC people, including employees, secondees, and independent contractors. For specific Accountabilities, including our Roles and Responsibilities, please see ACC's Personal Information and Privacy Policy.

Definitions:

Personal information is defined as information that relates to an identifiable individual.

Personal information includes but is not limited to:

- Staff information
- medical records and history
- the circumstances of injury

- contact details
- records of our customers' interactions with us
- recordings and photographs
- our notes, records and discussions about our customers and their claims
- contact with any health provider
- recordings of calls with us
- financial information, such as bank account details, IRD numbers, income or payments received
- information about an individual’s health, medical history, or disability (health information)
- information about the health services provided to an individual (health information)

3.1 We collect, use and store personal information to carry out our functions and responsibilities under the Accident Compensation Act 2001 and for related lawful activities.

What this means for you

Personal information includes all information about an identifiable individual. Information can also be considered personal information if it can be linked to an individual when combined with other available information. In other words, information that could be used to reasonably identify an individual, when combined with other available information or knowledge.

The types of personal information we have access to include all information held about our customers, our providers, businesses, and our people.

We will only collect personal information by means that are lawful, fair and do not intrude unreasonably on an individual's personal affairs. "Fair and reasonable" in this context means we will aim to collect personal information from individual customers rather than third parties unless there is a lawful reason for doing otherwise. When collecting information from third parties we obtain consent from the individual concerned, unless there is a good reason why consent is not required.

Any collection of data and information must be for a lawful and well-defined purpose. Transparency is important for trust and respect and recogn sing people's mana.

Doing it right

Treating all information as if it was your own. Personal information is taonga (treasured) and we consider ourselves to be kaitiaki (guardian) of any personal information we receive.

- We only collect personal information we need
- We collect information directly from the individual wherever possible and from third parties with the individual's consent, unless there is a good reason why consent is not required
- We consider all personal information with respect, even if an individual is not named
- Every time we handle personal information, we keep in mind ACC's purpose and the purpose for which it was collected
- Asking the question - How does the collection of this information relate to ACC's purpose and contribute towards creating positive outcomes for our customers.
- Respect and uphold the mana and dignity of the people, whānau, communities or groups who share their data and information with ACC
- If collecting data for research purposes, it is de-identified to the extent possible

Doing it wrong

- Collecting irrelevant or unnecessary personal information
- Collecting personal information for use in training purposes
- While working at ACC, Hayden is also completing a PhD on rock climbing safety and uses his EOS access to extract claims data to inform his research.

- Andrew is writing a survey for clients. He chooses to include questions that will not answer the current research question but may be useful in the future.
- Not telling people, in a way that makes sense to them, what data or information is collected about them and why, even if it's used or shared in a way that does not and cannot be used to identify them.

Tips and tricks

- ✓ Ask yourself whether you could identify someone based on the information you're collecting.
- ✓ Ask yourself – Is the information I am collecting necessary for me to provide the requested service? Is there a way of doing so without the collection of personal information?
- ✓ Those who hold people's information can 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 comply with the law, protect people's privacy, and maintain people's trust and confidence.
- ✓ Be mindful of New Zealand's cultural diversity, and the different perspectives, needs and approaches that should influence how we work to benefit individuals, whānau, a community or iwi.
- ✓ When deciding what information to collect and use to develop insights or for research, recognise that different groups and people may value qualitative and quantitative information about themselves differently.

More information

This relates to Privacy Principle 1: Purpose for collection of personal information
This relates to Privacy Principle 3: What to tell the individual about collection
This relates to Privacy Principle 4: Manner of collection
This relates to Privacy Principle 5: Storage and security of information
This relates to Privacy Principle 10: Use of personal information
Behaviours to uphold the Code of ACC Claimants' Rights
ACC Code of Conduct

3.2 We commit to making people aware of the collection of information

What this means for you
We have an obligation to tell anyone we are collecting information from why we are collecting it. In claims, we do this as part of our standard claims management onboarding automatically. In corporate functions, this is mostly going to happen around the personal information of our people for the purposes of people management, i.e., med certs for sick leave, individual CVs. When personal Information is being collected for research purposes consideration needs to be given to why this is being collected, what is the lawful purpose of the research, can the information be de-identified and is the information being collected necessary for the identified purpose. Be transparent and help people understand about the collection and use of their data or information, their right to access and corrections, and what choices they have.
Doing it right
• As part of a customer onboarding conversation, Alex ensures the privacy statement is shared with the customer and they confirm they have understood it. • A customer's rehabilitation needs have changed and we would like them to attend a new assessment. We need additional medical notes so we call our customer to let them know what we need to collect, and how we will be using and disclosing it.
Doing it wrong
• We obtain personal information from a customer's employer without advising the client of what information we require and why? • Using a customer's personal information for a research project or survey when they have declined to participate. • Collecting information about a customer from a 3rd party without their knowledge or consent.
Tips and tricks
✓ Are you using the information for the purpose we've advised it was collected? ✓ Ask yourself - What's being collected or used, why it's required. ✓ If and why it will be shared with other agencies or professionals. ✓ What laws allow the collection or use? If you are unsure, please contact the Privacy Team.
More information
This relates to Privacy Principle 2: Source of personal information - collect it from the individual This relates to Privacy Principle 3: What to tell the individual about collection

This relates to Privacy Principle 4: Manner of collection

3.3 We facilitate access to and respect an individual's right to seek amendment of factually incorrect personal information as a key priority

What this means for you - ACCESS

As an organisation that holds personal information, we must allow individuals access to the information we hold about them.

People can only ask for information about themselves unless they are acting on another person's behalf and have written permission.

Requests for personal information can be received via email, letter, phone or in person.

Once a request has been received, we must acknowledge the request and provide the requested information within 20 working days. The website for the Privacy Commissioner provides a response calculator to allow you to confirm the date we must provide a response to the customer and factors in weekends and public holidays.

There may be some situations where there are good reasons to refuse a request for access to personal information, e.g., the information may breach someone else's privacy or releasing it may pose a serious threat to someone's safety. In these instances, you should discuss these scenarios with your Team Leader or the Privacy Team

Doing it right

- If you're unsure, liaise with the privacy team
- Ensure the information requested relates to the individual making the request.
- Acknowledge the request and use the timeframes calculator on the privacy commission website to ensure we meet our legislative timeframes
- Gary receives a call from a customer who would like a copy of the medical notes we hold relating to his ankle injury. Gary verifies the customer's details and confirms the specific records the customer would like a copy of. At the conclusion of the conversation, Gary documents the conversation and sends the customer an INP01: Personal Info Request Acknowledgment. He then sends the task off for completion.

Doing it wrong

- Jo receives a request from Karen about information ACC holds in relation to her daughter. Jo releases the information, but Karen's daughter is over 18, however, Karen does not have permission to act on her daughter's behalf.
- A customer asks for a copy of a medical report by email, which we are unable to locate. We respond to the other questions in the email, but don't take any further action to find

and provide the medical report. This results in ACC not addressing the request within 20 working days.

Tips and tricks

- ✓ Be proactive and make it as easy as possible for customers to access their personal information.
- ✓ Tell them about their rights and encourage and support them to use those rights.

More information

This relates to Privacy Principle 6: Access to personal information
This relates to Privacy Principle 8: Accuracy of personal information
https://au.promapp.com/accnz/Process/6d831acc-9567-439f-adb1-8a421e364eaf?Area=Process

What this means for you - AMENDMENT

We do our best to ensure all personal information held by us is correct, but mistakes happen. Customers have the right to request that we correct any information they feel is incorrect, inaccurate, or misleading.

We acknowledge and respond to these requests in a timely manner. Legislative timeframes for Personal Information Requests are 20 working days. If the information cannot be corrected, the customer has the right to attach a statement of correction to the information.

Disability, culture, language, or literacy may prevent people from feeling comfortable asking to see their information and can also result in general concerns about where their information is, and which agencies have access to it Offer the information about rights in a safe and comfortable way that supports the Customer's ability to absorb and understand the information being provided.

It's important to note that the Privacy Act 2020 requires agencies to "provide reasonable assistance" to people who wish to request access to their personal information or request correction of their personal information.

Doing it right

- Jo receives a call from a customer who disagrees with statements made by their provider in their latest medical report. The provider confirms this was their accurate opinion at the time. The customer still disagrees, so the customer is asked to submit a statement of correction to ensure it is read together with the original document in the future.
- Jo receives a call from a customer saying their address isn't correct. Jo acknowledges the request and actions it, immediately, informing the customer the correction has been made.

Doing it wrong

- Jim receives a call asking him to update a customer's contact details. He does not check that he is speaking with the individual concerned and it turns out this was a malicious act by the customer's ex-partner.

Tips and tricks

Ask yourself:

- ✓ Am I dealing with the person that the personal information relates to?
- ✓ Have I acknowledged the request?
- ✓ Where does the information need to be corrected?
- ✓ Can I correct it?
- ✓ Is a statement of Correction more appropriate?
- ✓ Have I recorded the request for correction in our systems?
- ✓ Have I responded to the requestor with the outcome?

More information

This relates to Privacy Principle 7: Correction of personal information

Promapp Processes

Add or update business customer contact details

Manage a customer's request to correct personal information

3.4 We commit to using personal information only for the purpose for which it was obtained and other lawful purposes.

What this means for you

We all need to be aware that the personal information ACC holds is in our care for purposes that relate to ACC and what we do. Information should only be used for legitimate reasons, and that relate to the core functions and purpose of ACC.

If you cannot answer the following questions when using information, you should not be using it:

- What is the reason to use this information?
- Is that related to the purpose we collected it for?
- Have we informed the customer it may be used for this purpose?

There might be occasions where we hold information gathered for one purpose that could be lawfully used for another. However, the circumstances within which this is allowed under the Privacy Act are limited, like non-identifiable information making up part of a research project, or de-identified training resources. Where this is proposed, advice should always be sought from the Privacy team first.

Doing it right

- Engage with the Privacy team and/or Ethics Panel when you require advice.
- Aroha, one of Tama's team is unwell with a serious illness. Tama advises the team that Aroha is away but does not share any information about Aroha's illness.
- Ensuring that we are using de-identified data whenever possible or practicable for a research project.
- Use the correct technical processes, methods, and approaches for the kind of analysis or research you are doing
- A GP provides medical notes that did not form part of ACC's request. We advise the GP of the incident and ask that they provide only the information that was requested and securely destroy the incorrect information.

Doing it wrong

- Using personal information for training purposes without the customer providing their authority for their information to be used in this manner.
- Mel's manager discloses her age to some colleagues without her permission.
- Using personal information in a way that is not aligned to the Code of Conduct or Code of ACC Claimants' Rights.

Tips and tricks

- ✓ We should only access, use, or share personal information with others (including ACC employees) in accordance with ACC policies and guidelines.

- ✓ Communicate openly with our customers about how we intend to use their information
- ✓ Ask whether the information you wish to use is both relevant *and* necessary for the purpose you collected it for – less is best when using personal information.

More information

This relates to Privacy Principle 10: Disclosing personal information
Promapp 'Limits on using and disclosing information' policy

3.5 Personal information is disclosed to other parties only where there is legal authority to do so

What this means for you
We hold information that is Taonga to the people it relates to. There are times when we'll have to share information with third parties for ACC to be able to do our job. When we share information, we need to make sure this only happens when we have the authority to do so. There are some limited circumstances where we may be able to share information without client authority. However, the circumstances within which this is allowed under the Privacy Act are limited. For example, occasions when we need to share information to protect our people and others – such as, when we share information relating to a customer's behaviour with the Police to ensure the safety of providers or our people. Where this is proposed, advice should always be sought from the Privacy team first. If you have queries, please raise these with your leader, the Privacy Team or OIA Services. If there isn't a clear link between why we collected the information and our intended disclosure, we need to consider if the disclosure is necessary. We can always confirm with our customers that they authorise us to disclose information.
Doing it right
• Recognise that the trust people place in you, comes with an obligation to care for and respect the information they have shared. • IRD contacts us for information relating to a customer's weekly compensation. Krystal checks Promapp for the process related to sharing information and provides the information back to the requestor. • Jane calls ACC to try and sort out her self-employed husband's levy payments. There is no authorisation on file for Jane to act on her husband's behalf. We obtain verbal consent from Jane's husband and encourage him to complete an Authority to Act form. • A customer contacts us via the ACC Facebook page. ACC's social media team responds to the customer, without disclosing any personal information, and provides them with the details of who to contact about their claim. • Understand to your own satisfaction the potential value of the information you collect, and when it might be used in a non-personal form (for example, to develop new insights that may improve outcomes).
Doing it wrong
• Medical notes are emailed to a provider without checking to ensure the provider is the intended recipient before hitting send. • An advocate who only has authority to act on the customers behalf on claim A, is incorrectly sent information about claim B, which is not covered by the authority.

- Rob discloses information to an individual without verifying that they are an authorised party on the claim record.

Tips and tricks

- ✓ Act as a Kaitiaki of the taonga ACC holds.
- ✓ When discussing customer information within the office ensure that you are being respectful and demonstrating ACC's values.
- ✓ Raise concerns and debrief privately with a team leader or trusted colleague.
- ✓ Consider whether the information being asked for by a third party is information we can share.
- ✓ Never disclose other people's personal information for your own purposes.

More information

This relates to Privacy Principle 11: Disclosure of personal information
This related to Privacy Principle 12: Disclosure outside of New Zealand
Manage Information Requests
Official Information Requests Policy | Nintex Promapp®
Personal information requests Policy | Nintex Promapp®
Requests for customer information policy | Nintex Promapp®

3.6 We commit to storing information with reasonable safeguards against loss and disclosure and retaining it in line with legislative requirements

What this means for you
We typically hold records for 75 years from the date of the last action on a file, to ensure that records are available should claims need to be reactivated or issues arise in relation to decisions made in the past. If we identify we have received information that is not relevant to our func ons, where reasonably practicable, it will be returned or destroyed securely. Recognise the trust that people place in us, which comes with an obligation to care for and respect the information they have shared and use data management processes and tools that provide the appropriate level of security to protect, transfer and store data and information
Doing it right
• Make every effort to ensure personal information remains protected and secure when you are working remotely, this includes when working from home. • Try to work as much as possible electronically. Hard copies of files can be lost or seen by others if being accessed in public places. • Create an environment in your team discussions and decision-making where information management practices are understood and practiced.
Doing it wrong
• Jane decides to complete some work during her morning train commute. Jane opens a document that contains personal information and starts reading it. People around her can see and read the document.
Tips and tricks
✓ Make sure the correct classification tags are on documents. ✓ Conduct regular back-ups of data. ✓ Use password protecting electronic documents that contain significant or sensitive information (for example, health records, financial information). ✓ Avoid transporting physical documents, except where necessary. ✓ Only use our authorised cloud computing services that comply with government standards.

✓ Use the document destruction bins for secure document and information disposal.
More information
This relates to Privacy Principle 5: Storage and Security of information This relates to Privacy Principle 9: Limits on retention of information The easy guide to the information management policy The easy guide to the email and instant messaging policy

3.7 We have a clear, consistent process for reporting, managing and escalating privacy incidents

What this means for you
If you think there has been a privacy incident, you must report this to the Privacy Team immediately. We're required by law to report any serious privacy breaches to the Office of the Privacy Commissioner and to notify affected individuals within a limited timeframe. Reporting allows us to: • fix the problem - where a privacy incident occurs, we will do our best to rectify the situation • learn from the incident and get better • where appropriate, make breach notifications in accordance with the Privacy Act 2020 Anyone can report a potential incident to the Privacy Team at any stage. Reporting privacy incidents allows us to learn from any mistakes and helps us to prevent breaches happening in the future. We aim to grow from them and will take any learnings from the incident to continuously improve our approach to privacy. To report breaches, use the Privacy Reporting Tool or if the matter is urgent or a serious privacy breach that may be notifiable call the Hotline.
Doing it right
• You notice there appears to be an issue with email address verifications which means emails have been defaulting to an o der address. You raise with your team leader *and* follow the procedures for raising with the Privacy team and lodging an incident. • You have been added into a group chat where colleagues are discussing personal information of customers. You immediately alert your people leader. (It might be appropriate to use OK2Say or follow the Protected Disclosures Guidelines if you didn't feel comfortable going to your people leader)
Doing it wrong
• You ve been added to a group chat where colleagues are discussing personal information of our customers. You don't participate in the chat, but you also don't report it. • You send an email to the incorrect recipient. The email contains some personal information of a customer. You identify your error and re-send the message to the correct address but don't report it. • You leave your computer unattended whilst working from home, there is personally identifiable information on your screens visible to your flat mate.
Tips and tricks

Privacy incidents may include:

- ✓ Accidental disclosure to third parties and disclosures to third parties without authority or a lawful reason for doing so.
- ✓ Access of customer files by our people where there is no good business reason for access.
- ✓ Sharing customer personal information with other ACC people without a good business reason.
- ✓ Using personal information for reasons other than its intended purpose.
- ✓ Personal information systems are hacked or accessed unlawfully, either by external third parties or by ACC people.
- ✓ Near misses (where an incident was narrowly averted).

More information

Privacy Reporting Tool
Guide for reporting a breach or privacy incident

3.8 Care of personal information is embedded in everything we do

What this means for you
Making sure we take care of personal information is part of everything we do at ACC – we think about how we're caring for personal information when we do our day-to-day work, develop processes and policy, design systems and communicate with each other and external organisations. New Zealanders must be able to reasonably expect their personal information is collected, used, and shared respectfully, and adequately protected. All ACC people need to keep up to date with best practice and training modules on privacy and know how to raise privacy issues. The process of ensuring privacy is embedded throughout the product or service lifecycle from design to disposal and everything else we do at ACC is often referred to as Privacy by Design and should be incorporated into activities where personal information is collected and used. This may include continuous improvement activities, procurement, or policy development. At the center of the design for a product, service, system, or process that uses personal information should be the mitigation of individual harm and adverse impact of any privacy breach or misuse of information.
Doing it right
• Be kaitiaki (guardians) of personal information by building privacy by design into our systems and process, with guidance from the Privacy team, at the very start of the process. • Mitigate risks by ensuring that privacy recommendations or requirements are completed before your project goes live. • Dane finds an article about a privacy issue at another government agency. He raises this with his manager to ensure that ACC can mitigate this risk. • Not using real customer or claims information when designing training material and using Sandbox environments where possible • Only using de-identified data for research projects where possible.
Doing it wrong
• Designing a new business system or process without assessing the privacy risks involved at the start of the project. • Talking about the latest interesting case you were working on with a friend in the pub and discussing information that would identify the customer. • You suspect a colleague has made a potential breach and it has not been reported, you don't raise it with anyone as you're unsure if it's your responsibility.
Tips and tricks

- ✓ Privacy needs to be part of the planning of any new or updated product, service, system, or process. Privacy considerations should help drive the design rather than being bolted on at the end to address a few privacy risks.
- ✓ Protection and security of personal information should be considered for every stage of the information lifecycle: collection, storage and security, use, access and correction, disclosure, retention, and disposal
- ✓ When you do have to discuss personal information, think about what information is relevant and necessary to share.

3.9 We commit to ensuring we have effective policies and processes which reflect current best practice standards

What this means for you
ACC are committed to a programme of continuous improvement and has policies, guidelines and processes that have been designed to reflect the most up-to-date best practice standards. These documents govern how our people should handle the personal information in our care.
Doing it right
• Leaders are current with processes and guidelines, and they take accountability to ensure their teams are too. • Checking the privacy hub regularly for any updates or refreshers. • If you come across a policy or guideline that is out of date, please raise this with your Team Leader.
More Information

• *Information on ACC policies and procedures relating to ensuring we continue to meet our privacy obligations and best practice can be found in these locations:*
  ○ *The Privacy Hub.*
  ○ *The Information Management Hub*
  ○ *Promapp*
  ○ *Policy Hub*

Legislation relevant to these guidelines

Personal information held by us is subject to:

- the Privacy Act 2020
- the Health Information Privacy Code 2020
- the Official Information Act 1982
- the Code of Claimants Rights
- the Health and Safety at Work Act 2015
- Accident Compensation Act 2001
- the Public Records Act 2005.

Privacy queries or concerns

Our Privacy Team can provide support or respond to any complaints about privacy related matters under the Privacy Act 2020 or Health Information Privacy Code 2020.

You can contact them in the following ways:

The Privacy Officer
Accident Compensation Corporation
PO Box 242
Wellington 6011

Email: Privacy.Officer@acc.co.nz

Phone: 0800 101 996

Information is also available on the Office of the Privacy Commissioner's website at www.privacy.org.nz