Information Management Policy

POLICY NUMBER	5.0.0
TOPIC	Information Management
OWNER	Chief Technology and Innovation Officer
BUSINESS GROUP	Technology and Innovation
AUTHOR	Out of scope Manager Information Frameworks and Assurance
DATE APPROVED	25th March 2021
APPROVER	ACC Board
NEXT REVIEW DATE	25th March 2023

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:

1. Identifying opportunities for injury prevention initiatives
2. Improving customer service by improving outcomes, efficiencies and effectiveness
3. Sharing information for external use in support of insights and research related to accidents, injuries, treatments
4. Ensuring information is available and representative of the peoples of NZ, including Māori, minorities and marginalised groups to facilitate and support these communities
5. 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 Chief Technology and Innovation Officer (CTIO) 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 Governance Group (IGG)	• Operates with appropriate delegation of responsibility to oversee and 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 and Privacy advisory group (SPAG)	• 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.
Chief Technology and Innovation Officer (CTIO)	• 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 Head of Enterprise Data, Information and Security (EDIS) on behalf of the CTIO.	• 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.
Executive	• 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 Policy 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 Chief 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 Information and Security (EDIS) 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

LOA:	Role	Monitoring & Oversight
		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 Chief when appropriate • Supports the oversight of our information management practices and decision making via the Information Governance Group and sub governance groups.
3rd Line	Internal Audit (and external providers)	• Performs 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 • Reports to the Executive and the Board on the outcomes of such activities.
4th Line	Executive	• 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	Out of Scope
0.2	26/7/20	EDIS review completed	Out of Scope
0.3	21/9/20	Feedback from reviews added	Out of Scope
0.4	12/10/20	Final preparation for GG's	Out of Scope
0.5	16/04/21	Amendments for Board (minor)	Out of Scope

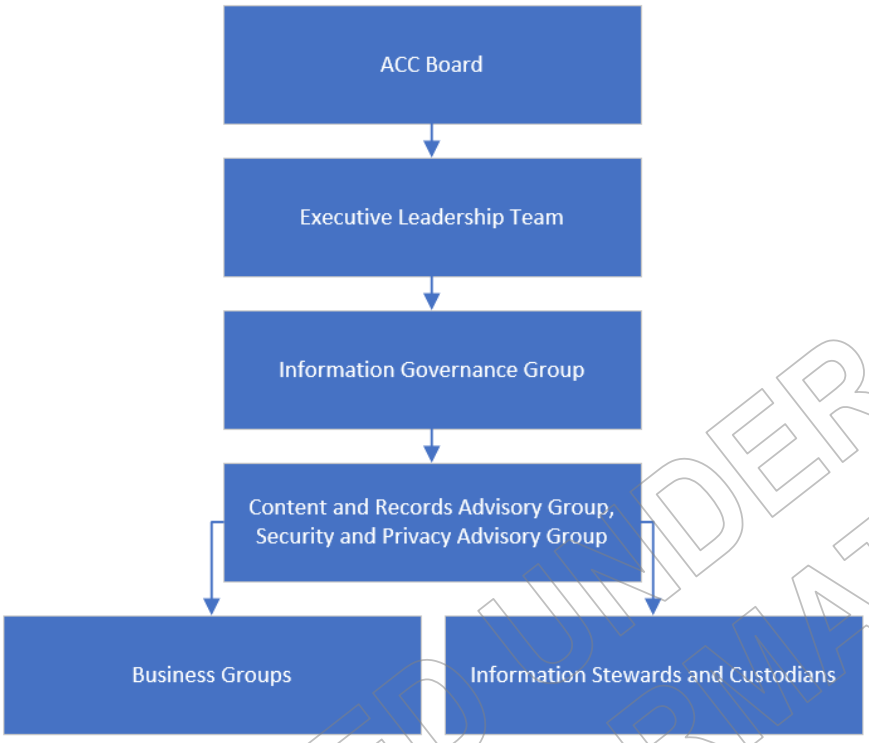
14 Appendices

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.