

Entered by Board Secretary

AGENDA ITEM 20   BOARD DECISION PAPER	
<b>To:</b>	Board
<b>From:</b>	Ryan Marshall, Compliance Manager
<b>Reviewed:</b>	Rodger Murphy, Head of Risk & Legal
<b>Date:</b>	19 June 2024
<b>Title:</b>	Tier 1 Policy

### Aronga / Purpose

1. This report requests the board’s approval of the updated Information and Records Management Policy (Policy).

### Tuku mana / Delegation

2. Board approval is required for Auckland Transport’s (AT) Tier 1 policies.

### Ngā tūtohunga / Recommendations

That the Auckland Transport Board (board):

- a) Approves the Information and Records Management Policy

### Te whakarāpopototanga matua / Executive summary

3. The Policy has been updated and refreshed as part of the standard policy review cycle.
4. Wording has been updated to be more readable and understandable, and hyperlinks have been added to relevant supporting information and documents.
5. The core principles of the Policy have also been expanded on to provide more detail and examples of what is expected in order to comply with the Policy.

### Ngā tuinga ō mua / Previous deliberations

6. The Finance and Assurance Committee endorsed the Policy for approval by the board at its 16 May 2024 meeting.
7. The Policy was last reviewed and approved by the board in February 2022.

### Te horopaki / Background

8. AT regularly reviews and updates its policies to ensure that they are fit-for-purpose, reflect leading practice, address key risk areas in the organisation and align to Auckland Council direction. Policies that are strategic in nature, have reputational impact or provide direction on important operational activities have been classified as Tier One policies. Tier One policies are approved by the board.

### Te hononga ki te “Statement of Intent 2023 - 2026”/ Alignment to Statement of Intent 2023 - 2026

9. While AT’s policies do not align to specific principles in the Statement of Intent, they help to address strategic and operational risks across the organisation and provide guidance on what, why and how we do our work. This enables the business to carry out its activities which align to the Statement of Intent.

### Me mōhio koe / What you need to know

10. The Policy has been updated to align with AT’s core information and records management message of “Easy to Save Easy to find Easy to Share”.
11. The wording of the Policy has been simplified to make the document easier to read and understand. It also includes hyperlinks to relevant documents and sites where more information on information and records management can be found.
12. The principles of the Policy are largely unchanged from the existing one. However, within each policy principle, more detail and context has been added so that users can understand how to adhere to those principles, and where they can access further information.

Entered by Board Secretary

13. The role and responsibilities of the Executive Sponsor for the Policy has been moved from the Chief Technology Officer to the Chief Financial Officer. This is because Archives New Zealand notes that an Executive Sponsor should be reporting to the Chief Executive of an organisation.

### Ngā ritenga-ā-pūtea me ngā rauemi / Financial and resource impacts

14. This paper relates to policy updates and as such does not have financial or resource impacts.

### Ka whaiwhakaaro ki te Tiakanga Taiao / Climate change and sustainability considerations

15. This paper relates to policy updates. Climate change and sustainability considerations are not applicable in this instance.

### Ngā whakaaweawe atu anō / Other impacts

Relationship	Consulted Y/N	Views and Perspectives Received
Māori	Yes: <input type="checkbox"/> No: <input checked="" type="checkbox"/>	We have not consulted on the matters referred to in this paper as they relate to internal AT policy.
Elected members	Yes: <input type="checkbox"/> No: <input checked="" type="checkbox"/>	We have not consulted on the matters referred to in this paper as they relate to internal AT policy.
Council Controlled Organisations	Yes: <input type="checkbox"/> No: <input checked="" type="checkbox"/>	We have not consulted on the matters referred to in this paper as they relate to internal AT policy.



### Ā muri ake nei / Next steps

16. If approved by the board, the updated Policy will be published on AT's intranet and communicated to the business.

### Te whakapiringa / Attachment

Attachment #	Description
1.	Information and Records Management Policy

### Te pou whenua tuinga / Document ownership

Submitted by	Recommended by	Approved for submission
Ryan Marshall Compliance Manager	Rodger Murphy Head of Risk & Legal	Dean Kimpton Chief Executive
		

# Information and Records Management Policy

---

## 1. Purpose

- 1.1. At Auckland Transport (AT), we value information and records as corporate and public assets. Creating and maintaining full and accurate information and records of business activities is an important part of our work practice. Access to appropriately created, received, captured, maintained, protected and trustworthy information and records supports AT's business operations and evidence-based decision-making. It also assures the public that we are an accountable and transparent local authority organisation.
- 1.2. The purpose of this policy is to enable AT to comply with its legal obligations with respect to Information and Records Management (IRM) and Information Governance (IG). This includes outlining a framework for staff responsibilities towards the creation and lifecycle management of AT's business information and records.
- 1.3. This policy supports AT's [Information and Records Management Strategy](#), which details the IRM framework and provides an operational approach towards IRM.

## 2. Scope

- 1.4. This policy applies to:
  - All AT employees.
  - AT representatives (in accordance with the terms of their agreement with AT), including:
    - Contractors;
    - Agency temps
    - Staff on secondment from other organisations/agencies;
    - Volunteers and interns.
  - AT Directors.

Where this policy uses pronouns like “you”, “your”, “we”, or “us”, it is referring to anyone listed in 1.4 who this policy applies to.

- 1.5. This policy applies to all information and records created, received, captured, and maintained as part of AT's business activities, regardless of form, format, or media.
- 1.6. This policy applies to all business systems, applications, repositories, and processes involved in creation and management of AT's information and records.

### 3. Policy Principles

## Easy to save Easy to find Easy to share

- 1.7. AT holds a lot of information and records, and how we manage these business assets is critical. Good information management helps each of us provide better customer service and make our everyday work more efficient. It also helps us meet legal requirements, which as a public agency, AT is required to do. This includes ensuring the organisation's records and information are managed, stored, and maintained in an appropriate manner.
- 1.8. To comply with these obligations, AT's information and records need to be **Easy to save Easy to find Easy to share and** follow the principles below. You can also visit the [information Records Management \(IRM\) Hub](#) resources (links specific to the principles are provided below) or [email the Information Governance \(IG\) team](#) for more information and guidance.

#### Created and managed as part of normal business practice

- 1.9. In our day-to-day operations, we collect and use information and records daily. To demonstrate transparency, we all need to ensure that we create and keep appropriate information and records to support our decision making.
- 1.10. We also need to make sure that the collection of Personal Identifiable Information (PII) or Sensitive Information is only for lawful purposes. Additionally, information and data should solely be used for the purposes specified during collection and not retained for any longer than required. For more information, go to the [IRM hub](#) and Information Security's [Click Aware hub](#).

#### Reliable, trustworthy, accurate and identifiable

- 1.11. For information and records to be reliable, trustworthy, accurate and identifiable, they need to be complete and contain the appropriate metadata (e.g., file name and properties). This gives them context and makes sure their meaning is accurate, and easily understandable. Metadata also needs to be managed, so the integrity of the information is maintained.
- 1.12. To be identifiable, it is important that the context and meaning of the information is understandable to others, and not just yourself. Consider how others, including those carrying out LGOIMA requests, may search for or try to identify information and records you have labelled. File naming plays an important role in this and you can get tips from the [File Naming Convention Standard](#). For example, 'Vision\_Zero\_Engagement\_Plan\_October2020' is far more contextually meaningful than 'Engagement Plan – October 2020'.

### **Accessible, retrievable, and useable**

- 1.13. To make AT's information and records retrievable and useable, we need to store them, so they are accessible for now and as long as they are needed. This means using the appropriate, dedicated repository and doing so in a timely manner. You can find out more about storage and AT's approved repositories on the [IRM hub](#) and in the [Information and Records Repositories Standard](#).
- 1.14. For example, it is not recommended to store business information and records in your OneDrive.<sup>1</sup> This is because they will not be accessible to others when you are on leave or depart AT. For more information about the latter and a handy offboarding checklist, refer to the [IRM hub](#).

### **Protected from unauthorised access, alteration or deletion**

- 1.15. It is crucial that our information and records are protected from those who are not authorised to access them. It is your responsibility to ensure the information you look after is appropriately protected from misuse. This includes carefully considering repository storage and permissions. For example, restricted libraries in repositories with appropriate permission settings can be used to protect Sensitive information.
- 1.16. If the information is to be shared, it should be done so in a controlled manner, and restricted to those who have permission. We need to take special care when sharing (internally or externally) high risk and/ or high value information and records, such as Personal Identifiable Information (PII) and Sensitive information. For example, sharing a link to a confidential document that can be viewed by anyone with the link is not an appropriate method. Instead, use the repository settings to share access to a specific individual. If in doubt, [email the IG team](#) or refer to the [IRM hub](#).
- 1.17. Generally, disposal or deletion of AT records should only be undertaken by the IG team. Ensure that you consult with them before deleting anything you think might be AT information or records that AT needs to retain. This excludes, for example, test or duplicate data, or emails that do not contain business decisions or transactions. For more information about what you can safely delete, refer to the [IRM hub](#) offboarding guidelines.
- 1.18. Whether an alteration of a document is allowed or not, will often depend on the circumstances. For example, editing a working draft of a document is expected. However, a report that has been finalised and published should generally not be altered. To do so would require approval from the document owner and consultation with the IG team.

---

<sup>1</sup> Reference and non-business documents are fine, but we don't recommend storing private personal files in your OneDrive.

## Visit the IRM Hub for more information

- 1.19. If you're not sure how to manage information or records, go to the [IRM Hub](#). This is a great source of information and guidance, which can help you better understand your own and AT's information management obligations.
- 1.20. You can also [email the IG team](#) with any IRM questions you have, and they will be happy to assist you.

## 4. Definitions

Term	Definition
<b>Information</b>	Knowledge communicated or received. The result of processing, gathering, manipulating, and organising data in a way that adds to the knowledge of the receiver.
<b>Information Asset</b>	Unstructured data in physical and/or digital form. Contains information relevant to the organisation's business conduct, which adds tangible and/or intangible value.
<b>Information Governance</b>	<p>Information Governance (IG) describes how information is used. It provides a unified approach for handling information and records, which complies with legal and operational requirements and outlines best practice.</p> <p>IG starts with looking at how information is collected, recorded (physically and digitally) and stored, as well as used (e.g., whether for audit, research or planning management), and on what basis it is shared with others, both inside and outside of AT. The principles of IG incorporate several important policies for using information and records, as required by legislation (e.g., the <a href="#">Public Records Act 2005</a>).</p>
<b>Information and Records Management</b>	<p>Information and Records Management (IRM) is a business function that is critical to the daily operation of every organisation. Effective IRM underpins trustworthy and reliable information and records that are accessible, usable, shareable, and well maintained.</p> <p>It involves the careful management of people, processes, and technology to ensure information and records are handled effectively and lawfully. Furthermore, it requires the planned implementation of effective processes, governance, and infrastructure to manage information and records throughout their lifecycle (e.g., creation, management, use/re-use, destruction, or preservation).</p>
<b>Lifecycle management</b>	<p>Lifecycle management of records addresses three lifecycle phases:</p> <ol style="list-style-type: none"> <li>1. Creation or receipt of a record</li> <li>2. Maintenance, safe storage, retrieval, or general use of a record</li> <li>3. Disposal of a record.</li> </ol>
<b>Local authority</b>	<p>Includes the following organisations defined in section 5(1) of the <a href="#">Local Government Act 2002</a>:</p> <ul style="list-style-type: none"> <li>• Council-controlled organisation (CCO), which includes AT</li> <li>• Council-controlled trading organisation</li> <li>• Local government organisation.</li> </ul>

Term	Definition
<b>Record</b>	<p>A record constitutes information, whether in its original form or otherwise. This includes (without limitation) a document, a signature, a seal, text, images, sound, speech, or data compiled, recorded, or stored, as the case may be:</p> <ul style="list-style-type: none"> <li>• In written form on any material</li> <li>• On film, negative, tape, or other medium, so as to be capable of being reproduced</li> <li>• By means of any recording device or process, computer, or other electronic device or process.</li> </ul> <p>Check out the handy flowchart on the <a href="#">IRM hub</a> for more information.</p>
<b>Personal Identifiable Information (PII)</b>	<p>Any information that could potentially identify a specific individual. This includes a person’s name, address, date of birth, passport number, and credit or debit card number, etc.</p>
<b>Sensitive information</b>	<p>Broadly refers to data that must be protected from unauthorised access to prevent harm to businesses and individuals alike. This includes information that is personal and private (including Personal Identifiable Information), as well as commercially sensitive within a business context (e.g. financial contract with a vendor).</p>

## 5. Roles and Responsibilities

IRM is to be governed through the following staff roles and responsibilities.

Role	Responsibility
<b>AT employees, contractors, and consultants working for or on behalf of AT</b>	<ul style="list-style-type: none"> <li>• Create and maintain complete and accurate information and records. This should be done in Technology-approved business systems and applications, as a routine part of work practice and in a timely manner.</li> <li>• Comply with IRM policies, standards, strategies, processes, and procedures.</li> </ul>
<b>Supervisors and managers (Information Asset Owners)</b>	<ul style="list-style-type: none"> <li>• Ensure staff are certified and trained in procedures relating to information and records.</li> <li>• Ensure staff, including contractors, create and maintain complete and accurate information and records. This should be done in a timely manner and as a routine part of work practice.</li> <li>• Ensure staff, including contractors, complete their IRM obligations before leaving AT.</li> <li>• Ensure staff, including contractors, comply with IRM policies, standards, strategies, processes, and procedures.</li> <li>• Implement IRM policies, standards, strategies, processes, and procedures as design components of information systems, especially where high risk and/ or high value records are created.</li> <li>• Ensure maintenance and management of information systems is consistent with IRM policies, standards, strategies, processes, and procedures.</li> <li>• Ensure systems, service transition and migration strategies are designed to support information and records business continuity and accountability.</li> </ul>

Role	Responsibility
<b>Chief Financial Officer</b>	<ul style="list-style-type: none"> <li>Appointed Executive Sponsor of the <a href="#">Public Records Act 2005</a> – this is a delegated responsibility from the CE..</li> <li>Responsible for oversight over all IRM policies, standards, strategies, processes, procedures, and programmes of work.</li> <li>Ensures there is budget and resources to enable implementation of AT's <a href="#">IRM Strategy</a>.</li> <li>Ensures IRM responsibilities are assigned and cascaded down.</li> </ul>
<b>Head of Risk &amp; Legal</b>	<ul style="list-style-type: none"> <li>Ensures audits controls and processes are in place across the business.</li> <li>Responsible for providing assurance that IRM requirements are being met throughout the business.</li> <li>Provide advice and support to the IG team regarding the handling and mitigation of identified IRM risks and issues they identify.</li> </ul>
<b>Executive Leadership Team</b>	<ul style="list-style-type: none"> <li>Promote the principles of IRM policies, standards, strategies, processes, and procedures.</li> <li>Manage information and records risks within their departments.</li> <li>Ensure staff, contractors and service providers are complying with this policy and associated standards.</li> </ul>
<b>Corporate Information Manager</b>	<ul style="list-style-type: none"> <li>Owns, governs, directs, and oversees delivery of IRM processes, procedures, roadmaps, programmes, and action plans. These should be aligned with AT's strategic and planning framework.</li> <li>Develops and maintains IRM policies, standards, strategies, processes, and procedures.</li> <li>Ensures monitoring controls are in place to benchmark and track IRM trends and compliance.</li> <li>Ensures IRM is governed through appropriate roles, responsibilities, and accountabilities.</li> <li>Monitors and reports on compliance with the <a href="#">Public Records Act 2005</a> and other relevant legislation and AT's IRM related policies, standards, and strategies.<sup>2</sup></li> </ul>
<b>Information Governance team</b>	<ul style="list-style-type: none"> <li>Provide service and coordinate activities that enable implementation of IRM policies, standards, strategies, processes, and procedures.</li> <li>Liaise with staff and Information Asset Owners for the promotion and incorporation of IRM policies, standards and strategies into organisational processes and systems.</li> <li>Liaise with staff and Information Asset Owners to ensure information and records are managed through their lifecycle in accordance with IRM policies, standards, strategies, processes, and procedures.</li> <li>Regularly monitor information systems and processes to ensure they are meeting IRM policies, standards, and guidelines, and apply remedial action, if required.</li> </ul>

<sup>2</sup> Including the [Contract and Commercial Law Act 2017](#), [Local Government Act 2002](#), [Local Government Official Information and Meetings Act 1987 \(LGOIMA\)](#) and [Privacy Act 2020](#).



Role	Responsibility
	<ul style="list-style-type: none"> <li>Develop online training, including the IRM mandatory module, as well as undertake various forms of outreach (e.g. Community of Practice, attendance at team meetings, Viva Engage and Engine Room comms)</li> </ul>
<b>Chief Executive (CE)</b>	<ul style="list-style-type: none"> <li>Ultimate legislative responsibility for ensuring AT meets its statutory obligations and IRM responsibilities.</li> </ul>
<b>AT Board of Directors</b>	<ul style="list-style-type: none"> <li>Responsible for ensuring the Board and Board Committee minutes are properly recorded.</li> </ul>

## 6. Supporting Information

Related documents	Description/comments
<b>Legislative compliance</b>	<ul style="list-style-type: none"> <li><a href="#">Contract and Commercial Law Act 2017</a></li> <li><a href="#">Local Government Act 2002</a></li> <li><a href="#">Local Government Official Information and Meetings Act 1987 (LGOIMA)</a></li> <li><a href="#">Privacy Act 2020</a></li> <li><a href="#">Public Records Act 2005</a></li> </ul>
<b>Supporting documents</b>	<ul style="list-style-type: none"> <li><a href="#">File Naming Convention Standard</a></li> <li><a href="#">Information and Records Disposal Standard</a></li> <li><a href="#">Information and Records Management Hub</a></li> <li><a href="#">Information and Records Repositories Standard</a></li> <li><a href="#">Information and Records Systems Requirements Standard</a></li> <li><a href="#">Information and Records Management Strategy</a></li> </ul>
<b>Related documents</b>	<ul style="list-style-type: none"> <li><a href="#">Acceptable Use Policy</a></li> <li><a href="#">Cloud Computing Security Standard</a></li> <li><a href="#">Code of Conduct Policy</a></li> <li><a href="#">Customer Privacy Policy</a></li> <li><a href="#">Document Classification Standard</a></li> <li><a href="#">Email Security Standard</a></li> <li><a href="#">Information Records Management Standard</a> (Archives New Zealand)</li> <li><a href="#">Information Security Policy</a></li> <li><a href="#">List of Protected Records for local authorities</a> (Archives New Zealand)</li> <li><a href="#">Māori Information Management Strategy</a></li> <li><a href="#">Mobile Device Guidelines</a></li> <li><a href="#">Privacy Policy</a></li> <li><a href="#">Records Disposal Schedule</a></li> <li><a href="#">Risk Management Policy</a></li> <li><a href="#">Scanning Standard</a></li> <li><a href="#">Vital Records Standard</a></li> </ul>

## 7. Compliance

Full compliance with this strategy is required. Non-compliance may result in disciplinary action being taken against employees, in accordance with the [Code of Conduct Policy](#).

If full consideration is not given to the requirements in this policy, there is the risk AT could suffer from information corruption, loss, or inappropriate access. This could lead to:

- Diminished customer trust and confidence
- Reduced ability to demonstrate compliance, as per government standards
- Breaches of Personal Identifiable Information, or Sensitive or Confidential information
- Sanctions for non-compliance, including fines.

## 8. Approval & Review

**Policy Owner:**  
Chief Technology Officer

**Policy Contact:**  
Corporate Information Manager

**Endorsed by:**

**Approved by:**

Chief Executive  
**Approval date:** DD/MM/2024

Auckland Transport Board  
**Next review date:** DD/MM/2027

AT reserves the right to review, amend or add to this standard at any time upon reasonable notice to employees and representative.