University of Otago Information Framework

November 2021

Office of the Vice-Chancellor

Vice-Chancellor's Office ❁ Registrar and Secretary to Council's Office ❁ Office of Māori Development ❁
Pacific Development Office ❁ Strategy, Analytics and Reporting Office

University of Otago ❁ PO Box 56 ❁ Dunedin 9054 ❁ New Zealand ❁ https://www.otago.ac.nz/vc-office/about/

Table of Contents

Executive Summary

The University recognises information as a key strategic asset that underpins all University activities. The University's commitment to excellent information management practice in all its endeavours supports the University's core values in:

- excellence in research and teaching, and in administration, support services and technologies
- creation, curation, preservation, and transmission of knowledge
- collegiality and collaboration with and between staff, students, and external organisations, and
- stewardship of the University's heritage, its physical and digital resources, and its intellectual capital.

The University is committed to using and managing its information appropriately and wisely to maximise the operational and strategic value of the information it holds, and to ensure compliance with relevant legislation.

The purpose of this Framework is to provide a high-level and integrated approach to the governance and management of the University's information.

Because information is both ubiquitous and multi-faceted, the University must have a multidisciplinary approach to managing its information across the organisation. This requires clear responsibilities, appropriate policy, and – crucially – teams with different informational expertise working collaboratively together, and with information custodians, to ensure appropriate processes and outcomes.

Consistent with this, the Information Framework outlines the specific roles and responsibilities associated with managing information at the University so that required collaboration can occur, and so pathways for consultation are clear. This is particularly important when processes and technologies with informational implications are introduced or changed, and when information is used in new ways. Additionally, the Framework provides an overarching context for University policies, procedures, and other guidance related to aspects of information management.

In addition to detailing responsibilities and requirements, the Framework may also be used as a resource that staff can consult to understand their own responsibilities and to identify further sources of support and advice.

Governance and Executive Management

University Council

The University Council has governance responsibility for ensuring that the University's information management is legally compliant, that informational risks are managed, and that information is used appropriately in support of the University's goals and strategic direction.

The Council exercises this role predominantly through:

- approval of the Information Framework and other frameworks, statutes, regulations, and governance policies concerned with information
- monitoring of information-related risks through the Audit and Risk Committee, and
- ensuring that informational aspects are adequately addressed in the initiatives and projects it approves.

Reporting on information management to Council is through risk reporting from the Audit and Risk Committee (see below) and/or through reporting of ongoing activities in Triannual Non-Financial Reports.

Audit and Risk Committee

Audit and Risk Committee is a committee of Council. It receives reports on risks and planned audit activities, including those related to information management. It is expected that significant information risks will be reported through the Audit and Risk Committee.

Vice-Chancellor and Vice-Chancellor's Advisory Group

The Vice-Chancellor has overall management responsibility for ensuring that the University complies with legislative requirements relating to information and that information is appropriately used and controlled. The Vice-Chancellor chairs the Vice-Chancellor's Advisory Group (VCAG) which comprises the University's Senior Management Team.

The Vice-Chancellor, in consultation with the Vice-Chancellor's Advisory Group as required, ensures appropriate management of information predominantly through:

- endorsement and oversight of the Information Framework
- approval of non-governance policies concerned with information
- approval of initiatives relating to the management of information, and

- ensuring that informational aspects are adequately addressed in the initiatives and projects it approves and endorses.

Information Custodianship

University information is owned or controlled by the University as a whole, for the benefit and functioning of the University. However, to assist with the operational management of information, certain types of information are managed by assigned custodians of that information. Custodians are normally members of the University's Senior Management Team.

Custodian Responsibilities

For information under their management, information custodians shall:

- be familiar with this Framework and relevant University policies, procedures, and guidelines
- manage information for which they have responsibility to
  - seek maximum practical benefit to the University as a whole
  - ensure legislative compliance
  - ensure compliance with this Framework and with relevant University policies, procedures, and guidelines
- be aware of informational implications of new initiatives and technologies, and manage this appropriately
- report information-based risks via Risk Registers and the Office of Risk Assurance and Compliance
- ensure relevant staff are aware of their responsibilities in relation to information (such staff may report through the custodian, but not in all cases)
- ensure appropriate access to and security of information, and
- delegate and record delegations as appropriate (custodians may delegate responsibilities to other appropriate staff but retain overall responsibility in relation to the information under their management).

Custodians are expected to work with areas that have Specialist Information Portfolio Responsibilities (see page 12) who can provide advice and assist them with meeting their responsibilities.

Additional information on the different aspects of information management is available on pages 8-11 of this Framework. See also Appendix A on Information Security Classifications.

Custodianship of Key Types of University Information

The following list is not intended to be comprehensive but illustrates custodians of key University information. Decisions pertaining to custodianship can be made by the Vice-Chancellor/Vice-Chancellor's Advisory Group.

The table below is to be read in conjunction with University policies that give roles certain specific responsibilities for aspects of information or content. For example, the Director of Human Resources has authority in relation to staff emails.

Where an information type is held in a central system or department, but also held in other devolved departments around the University, it is expected that managers and staff in those departments will follow any directives and advice from the custodian (or relevant delegated authority). See also Manager and Staff Responsibilities below.

Information Type	Custodian	Standing delegation(s)
Academic Board (Senate and Committees) Information	Vice-Chancellor	Manager, Academic Committees and Services
Alumni Information	Deputy Vice-Chancellor (External Engagement)	Director, Development and Alumni Relations
Archived University Records and Historic Material	Registrar and Secretary to the Council	Head, Corporate Records
Business Intelligence Information not otherwise captured in this table	Director, Strategy, Analytics and Reporting	-
Council and Council Committee Information	Registrar and Secretary to the Council	-
Emails held on University Servers	Chief Operating Officer	Director, ITS
Financial Information	Chief Financial Officer	Financial Controller
Graduate Research Student Information (not covered by general student information as shown below)	Deputy Vice-Chancellor (Research and Enterprise)	Dean, Graduate Research School

Health Information held in Academic Divisions	Pro-Vice-Chancellors	-
International Partnership Information	Deputy Vice-Chancellor (External Engagement)	Director, International
IT Systems Information	Chief Operating Officer	Director, ITS
Library Information	Deputy Vice-Chancellor (Academic)	University Librarian
Māori Information (information specific to Māori, including mātauranga Māori, and not otherwise covered by sections in this table)	Director of Māori Development	-
Pacific Peoples Information (information specific to Pacific Peoples, including oral information, and not otherwise covered by sections in this table)	Director of Pacific Development	-
Projects and project information	Project Sponsors Project Steering Committees	Project Managers
Property and Campus Information (new and proposed)	Chief Operating Officer	Director, Campus Development
Property and Campus Information (existing)	Chief Operating Officer	Director, Property Services
Research Contract and Management Information	Deputy Vice-Chancellor (Research and Enterprise)	Director, Research & Enterprise
Research Ethics Information	Deputy Vice-Chancellor (Research and Enterprise)	Manager, Academic Committees and Services
Staff Employment Information	Director, Human Resources	-

Statutes, Regulations, Policies, Procedures, Guidelines and Codes of Practice (at the University level)	Registrar and Secretary to the Council	Responsible Officers for individual Policies, Procedures, Guidelines and Codes of Practice
Student Academic Records	Registrar and Secretary to the Council	Head, Student Experience
Student Accommodation Information	Chief Operating Officer	Director, Campus and Collegiate Life Services
Student Discipline Information	Vice-Chancellor	Various (as per the Discipline Statute)
Student Enrolment and Study Information	Deputy Vice-Chancellor (Academic)	Head, Student Experience
Student Health Information	Chief Operating Officer	Manager, Student Health Services
University Archives in the Hocken Collections	Registrar and Secretary to the Council	Hocken Librarian
Information held in individual schools or departments and not otherwise captured above, including teaching and learning materials[1]	Pro-Vice-Chancellors and Heads of Service Divisions	Normally Heads/Managers of the individual departments concerned
Research Information (specific to research outputs)	Unless otherwise determined by contract, is the responsibility of individual researchers	

[1] See also the University's Intellectual Property Rights Policy on ownership of these materials.

Manager and Staff Responsibilities

All staff have responsibility for the appropriate management and handling of information.

Managers (e.g., Heads of Departments) are expected to:

- be aware of this Framework, and of University policies, procedures and guidelines relating to information
- follow advice and directives from information custodians about specific types of information
- follow advice and directives from relevant staff that have Specialist Information Portfolio Responsibilities (see page 12) about specific aspects of information management and handling, and
- ensure staff under their direction are meeting expectations in relation to information (as below).

All staff are expected to:

- be aware of and follow University policies, procedures and guidelines relating to information, and
- follow advice and directives from their managers, information custodians and relevant staff that have Specialist Information Portfolio Responsibilities (see page 12) about information management and handling.

Aspects of Information Management

Information is multifaceted and information custodians, managers and staff should be aware of the different aspects of information. For some aspects, the University has specialist staff who can assist with advice and ensuring legislative and University requirements are met (see the next section on Specialist Information Portfolio Responsibilities on page 12).

Legislation and University policies relating to specific aspects of information management are listed in Appendix B on page 20.

Beneficial Use of Information

Information is an asset, and whilst being aware of privacy, confidentiality and security limitations, information should be used and shared within the organisation to ensure benefit to the University as a whole.

Māori and Pacific Peoples Information

The University recognises that it holds information from many different cultures, including records that may embody Māori and Pacific Peoples knowledge and perspectives. A commitment to excellence in information management practice supports the University's commitment to the aspirations of the Māori and Pacific Strategic Frameworks and ensures that this documentary heritage is preserved for future generations.

The University acknowledges its commitments under Te Tiriti o Waitangi and its Māori Strategic Framework. Māori information is a taonga and Māori have inherent rights and interests in relation to the collection, ownership and use of Māori information. The University, in consultation with, and through, its Office of Māori Development shall establish processes and protocols to ensure the appropriate treatment of information about or from Māori people and environments.

Privacy of Personal Information

Personal information is *any* information about an identifiable individual. The University holds a vast amount of personal information about students, staff and third parties. It has legislative and ethical responsibilities to manage that information appropriately. This includes:

- not collecting or holding personal information unless this is lawful and there is a good reason to do so
- being transparent about why information is collected
- ensuring information held is accurate and up to date
- making sure information is used in an appropriate way
- ensuring information is secure (some information, such as health or disciplinary information, may need increased levels of security)
- allowing people access to their information in most circumstances, and
- preventing disclosure of personal information to third parties, except in limited prescribed circumstances
- reporting privacy breaches which are likely to cause serious harm to the Privacy Commissioner as soon as practicable after becoming aware of the breach, and in most instances, notifying affected individuals.

The University's key policy on the management of personal information, which all staff should be familiar with, is the Policy on Access to, and Use of, Personal Information. The University also maintains Privacy at Otago, a website with privacy information and resources.

The Registrar and Secretary to the Council is the University's Privacy Officer and the Manager, Policy and Compliance (in the Office of the Registrar) is the Deputy Privacy Officer. The Director of Human Resources is responsible for privacy in relation to all employment information. Privacy advice may be issued by, and be sought from, these roles as appropriate.

Confidentiality of Business Information

The University holds much information about or relating to its business that may be commercially sensitive or otherwise confidential.

Areas managing business information have responsibilities to:

- ensure business information is secure (certain information, such as confidential contracts, may need increased levels of security)
- make clear when information is confidential and when and with whom information may be shared, and
- manage appropriate access to information.

Staff are required to observe confidentiality requirements carefully. As a starting point, it is recommended that staff treat all business information relating to the University as confidential unless it is clearly in the public domain or permission to disclose information has been given under policy; or by the University Council, Chancellor or Vice-Chancellor; and/or by the relevant information custodian. See Appendix A for further information.

Availability of Information

As the University is a publicly funded institution, much of its information is discoverable under the Official Information Act 1982. The Registrar and Secretary to the Council has responsibility for coordinating Official Information Act requests, excluding those relating to employment for which the Director of Human Resources is responsible.

Security of Information

There are two components to the security of University information:

- Cyber Security – the protection of the University's network, systems, and data from cyberattack, and
- Physical Security – the monitor and control of access to the University's facilities and equipment where information is housed.

The University has legislative and contractual responsibilities to protect its information by maintaining security safeguards. These include:

- protecting information wherever it is located, including in systems, in file cabinets, in transit and outside the workplace, from unauthorised or unlawful access, use, alteration, loss and destruction
- providing special protection for certain types of information, such as patient information, that are identified as needing an extra level of security, and
- taking all reasonable precautions to secure information as is reasonable given the circumstances.

Appendix A provides further information on security classifications for different types of information.

Cyber security risk is highlighted as a critical risk. All staff need to be aware of this, be alert to the potential for cyber security attacks, and follow advice and guidance from the Cyber Security team. To reduce the risk of cyber security incidents, staff should utilise trusted and supported University IT systems to store their digital information (ITS maintain a list of Mandatory and Recommended IT Services and Solutions).

The University's key document on the security of digital information is the Cyber Security Framework. The Cyber Security team, led by the IT Assurance and Cyber Security Senior Manager, is responsible for cyber security actions, communication, and reports, and can provide advice on request.

Retention and Disposal of Information

The University holds much information about or relating to its business. As a public office under Government, the University is required to retain certain types of business information for defined periods of time.

Areas managing business information have responsibilities to:

- create and maintain records of activities, transactions and decisions carried out during daily activity
- manage University business information appropriately, including its storage and access
- archive or destroy information, including personal information, when it is no longer required in accordance with the Universities Disposal Authority and relevant legislation
- seek advice or approval before disposing of or deleting University business information, including when:

- decanting
- commissioning or decommissioning software or systems that hold University information, and
- when planning to digitise University information and destroying the paper original.

The University's key policy on the retention and disposal of University business information, which all staff should be familiar with, is the Records Management Policy. This should be read in conjunction with the University's Records Destruction Guidelines.

The Head of the Corporate Records Service is responsible for monitoring the retention and disposal of University business information and can be contacted for retention and disposal-related advice. The Corporate Records Service also maintains a website with information and records management resources and advice for staff.

Specialist Information Portfolio Responsibilities & Sources of Advice

There are a number of specific teams which have responsibility for aspects of information management at the University, including responsibilities for key pieces of New Zealand legislation. These units can offer advice and provide direction on aspects of appropriate treatment of information and should be consulted on significant matters relating to their areas of expertise.

Office of the Registrar and Secretary to the Council

Privacy, Official Information Requests, Information and Records Management, Copyright, Open Access

The Office of the Registrar and Secretary to the Council has oversight of compliance with the provisions of the Copyright Act 1994, the Public Records Act 2005, and, except in relation to employment and staff information, the Official Information Act 1982, and the Privacy Act 2020. It can provide advice and guidance on these matters, as well as requesting information associated with requests under the Official Information and Privacy Acts.

The Office of the Registrar and Secretary to the Council includes:

Privacy Officer

The Registrar and Secretary to the Council is the University Privacy Officer, and the Manager, Policy and Compliance is the Deputy Privacy Officer. They can be contacted in relation to privacy related matters. As below, privacy-related matters relating to staff and employment information are dealt with through Human Resources.

Corporate Records Services

Corporate Records Services is responsible for monitoring the University's requirements under the Public Records Act 2005 through identifying, retaining, and authorising the disposal or deletion of University business information using the New Zealand Universities Disposal Authority (DA).

It is responsible for managing the University's information and records management framework and providing information and records management advice to staff and to teams involved in developing or implementing systems or initiatives that hold or affect University information.

Manager, Copyright and Open Access

The Manager, Copyright and Open Access can advise on all matters relating to copyright, as well as providing advice on open access in relation to research outputs.

Strategy, Analytics and Reporting Office (SARO)

Business Intelligence, Data Use

This Office is responsible for meeting the University's reporting obligations under the Education and Training Act 2020 in providing information to government agencies for planning, funding, and statistical purposes.

It is responsible for the University's data and analysis service and for progressing the University's development of business intelligence capabilities which includes the collation of internal data.

Office of Māori Development

Information specific to Māori

The Office of Māori Development can provide guidance on the appropriate treatment of information about or from Māori people and environments.

Office of Pacific Development

Information specific to Pacific Peoples

The Office of Pacific Development can provide guidance on the appropriate treatment of information about or from Pacific people and environments.

Human Resources

Privacy, Official Information requests (Employment Information)

Human Resources has oversight of compliance with the provisions of the Official Information Act 1982 and the Privacy Act 2020 in relation to employment and staff information.

Information Technology Services (ITS)

Cybersecurity, IT Systems

Information Technology Services is responsible for the provision and maintenance of information and communication technologies for the University. ITS is supported in its work by the shared service, IT Support Services.

ITS provides the structure that supports University information such as the hardware and software, as well as informing the design and strategy on the use of technology within the organisation and ensuring the security of the University's network and systems. ITS is responsible for operationalising the instructions of the business information owners and implementing and advising on the controls identified for the information assets owned by the business information owners that reside in IT systems.

Information Technology Services also includes:

Enterprise Architecture Office

The Enterprise Architecture Office is responsible for providing architectural governance over IT projects and business-as-usual (BAU) processes to ensure that the organisation's IT strategy and investment in technology is aligned to the University's strategic and business goals.

IT Assurance & Cyber Security

IT Assurance & Cybersecurity has responsibility for the security of the University's digital information. It is responsible for planning, building, monitoring, and reporting on information security and controls at the University and providing the University community with advice on cyber-security best practice.

Proctor's Office

Physical Security

The Proctor's Office has responsibility for the physical security of, and manages access to, University buildings. It is responsible for providing advice on security requirements for new build projects and refurbishments and is also able to assist with security audits and risk assessments.

Office of Risk Assurance and Compliance

Compliance, Risk Reporting

The Office of Risk Assurance and Compliance is responsible for reviewing accounting records, information systems and other administrative policies and practices to identify non-compliance with policies or regulatory requirements, including those related to information.

The Office also oversees the University's Risk Registers, which can be used to record information related risk.

Hocken Library

The Hocken Library has a special role as the archival repository for the University and should be the first point of contact for queries relating to accessing University archives in their care.

Document Review

This Framework will be reviewed and updated regularly. Editorial and consequential amendments may be approved by the Registrar and Secretary to the Council. Substantive amendments which do not alter the overall intent of the Framework may be approved by the Vice-Chancellor. Significant changes to the Framework require Council approval.

Version Control

Date	Version	Change	Actioned By
December 2019	0.1	Initial version	Christan Stoddart / Tracey Sim
November 2020	0.2	Released for peer review	Tracey Sim
January 2021	0.3	Incorporated initial feedback	Tracey Sim
May 2021	0.4	Released for final review	Tracey Sim
September 2021	0.5	Endorsed by VCAG	Christan Stoddart
October 2021	1.0	Approved by University Council	Christan Stoddart
November 2021	1.1	Editorial update based on Council feedback approved by Registrar and Secretary to the Council, and framework published	Christan Stoddart

Appendix A

Information Security Classifications

For security purposes, the University categories information into one of four security classifications. This can assist Information Custodians and information experts with ensuring the appropriate controls are in places around information, information systems and information processes.

All University information falls in one of the following categories:

PUBLIC

Public information is clearly in the public domain or authorised for public release by an appropriate

University authority with control over the relevant information (e.g., media releases; Official Information Act responses). Examples include material on the University website; programme regulations; and published accessible research.

- Public information can be shared, transmitted, and stored without special controls.
- Disposal of business information in this category is subject to the Public Records Act, but otherwise no special controls are required.

INTERNAL USE

Internal use information is information about University operations, but not containing personal information or sensitive business information. Disclosure would not adversely affect the University. Examples include administrative emails not containing personal information, internal administrative process documents.

- Internal Use information can be shared internally and with others with a formal relationship to the University, as appropriate to the circumstances.
- No special electronic or postal transmission controls are required.
- Stored files, documents and information should only be accessible to business users, with standard protections against theft, vandalism, compromise, or misuse.
- Disposal of business information in this category is subject to the Public Records Act, and secure disposal should be used.

CONFIDENTIAL

Confidential information is non-public personal information about any identifiable individuals (students, staff, or others) and strategic or commercial business information. Disclosure would adversely affect the University. Examples include student records; emails referring to students; business cases; and emails referring to business opportunities.

Unless otherwise clear from an appropriate approval, a formal classification, or context (e.g., information is clearly in the public domain), University information should be treated as confidential as the default.

- Confidential information may not be shared except with appropriate authorisation or authority.
- Personal information is subject to the Policy on Access to, and use of, Personal Information.
- Moderate controls on transmission are appropriate (e.g., encryption may be considered, stamping envelopes confidential and providing a return address).
- Stored information – whether stored electronically or physically – must be protected against unauthorised use.
- Disposal of business information in this category is subject to the Public Records Act, and secure disposal must be used.

RESTRICTED

Restricted information is very sensitive business or personal information. Disclosure would adversely affect the University. Examples include health information, disciplinary information, and highly confidential business cases.

Information's status as Restricted should be established at a systems or process level and/or information should be clearly labelled to establish it is Restricted.

- Restricted information may not be shared except with appropriate authorisation or authority.
- Staff with access to restricted information should be very limited.
- Personal information is subject to the Policy on Access to, and use of, Personal Information.

- Strong controls on transmission are appropriate (e.g., encryption and password protection).
- Stored information – whether stored electronically or physically – must be protected against unauthorised use and secure, authorised systems must be used.
- Disposal of business information in this category is subject to the Public Records Act, and secure disposal must be used.

Appendix B

Legislation and Policy

LEGISLATION

Copyright Act 1994

Official Information Act 1982

Privacy Act 2020

Health Information Privacy Code 2020

Public Records Act 2005

Information and Records Management Standard

UNIVERSITY POLICY

Regulations

Information and Communications Regulations 2014

Policies

Email Policy

Ethical Behaviour Policy

Information Security Policy

Intellectual Property Rights Policy

Policy on Access to, and use of, Personal Information

Records Management Policy

Web Policy

Procedures

Digitisation of Records Procedures

Remote Access Procedure (including VPN)

Software Security Updates (Patching) Procedure

University Network Interconnection Procedure

Guidelines

Data Access Guidelines

Records Destruction Guidelines

Web Guidelines

Codes of Practice

Responsible Practice in Research – Code of Conduct

Other

Access Framework for University of Otago Records

Cybersecurity Framework

New Zealand Universities General Disposal Authority (GDA)

Resources

Cloud Services

Cloud Services – Information and Records Management Considerations

Microsoft 365

Digitisation

Authority to Retain Public Records in Electronic Form Only

Destruction of Source Information after Digitisation