Records and Information Management Procedures

1. Purpose

These procedures are to be read in conjunction with the Information and Records Management and Security Policy (the Policy).

These procedures apply to information and records in all formats, except in certain instances, as indicated, where the procedure only applies to Records covered by the definition of a Record. Formats include electronic databases, files (Word, Excel etc.), internal and external web content (including social media posts), emails, text messages, chat, posts (in Teams) and paper.

Guidance and advice is available from the Information and Records Management Team and on the University intranet site (https://intranet.victoria.ac.nz/services-resources/record-management)

Guidance and advice on Research data management is available from the Library and from the Research Office in cases where contractual, compliance or ethics obligations may impact the management of research data.

2. Application of Procedure

This Procedure applies to Staff Members.

Part 2: Procedure Content

3. To comply with the principles expressed in Section 3 of the Policy it is expected that:

3.1 All staff:

(a) create and capture full and accurate records of all transactions, decisions and activities;

(b) manage records for use and reuse;

(c) only destroy or dispose of records in accordance with the University's process (see Appendix 1), the Disposal Authority and with the appropriate approvals (see Delegations Framework);

(d) create, save, store and transmit electronic records only in University systems approved by Digital Solutions;

(e) only access or use information where this is necessary for a legitimate university purpose;

(f) keep information secure by:

(i) abiding by all Digital Solutions security standards and guidelines including the "Acceptable Use of Information Systems Statute"

(ii) ensuring that any loss of records is reported to Information and Records Management as soon as it is practical after the event

(iii) ensuring that all devices (phone, tablets, memory sticks etc.) accessing records are password or pin protected, and kept secure at all times

(iv) not sharing any password or pin numbers with any other person

(v) protecting all confidential information and records, including those containing sensitive personal information at all times by:

(A) practicing a "Clear Desk" and / or "Clear Screen" of all unattended information;

(B) locking computers when absent at all times to prevent unauthorised access;

(C) ensuring paper records are locked away when not in use;

(D) ensuring any electronic records accessed on a non-University device is secured from access by any other person;

(E) ensuring any paper records transferred to off-site storage are appropriately protected.

(g) staff must not disclose confidential information unless authorised to do so; ;

(h) complete all relevant e-learning modules;

(i) ensure that records are left within the custody or control of the University when employment ends.

3.2 Managers ensure that:

(a) The University's records management processes for their team are followed and documented;

(b) staff reporting to them (whether permanent, contract or otherwise, including tutors) are aware of, understand and comply with the Policy and procedures;

(c) all business rules, processes or procedures they are responsible for include records management requirements;

(d) staff induction processes include records management responsibilities and expectations;

(e) when staff leave the University, they are requested to move any records into the correct systems (i.e. not leave it in OneDrive)

(f) ongoing information management and security training is provided to staff reporting to them;

(g) there is a prompt adjustment of appropriate system permissions when changes to a user's role or status occur;

(h) paper records are stored in appropriate conditions (i.e. secure, dry and pest proofed);

(i) they are the primary point of contact within that Faculty / School / CSU / Department with respect to information and records management;

(j) they regularly review compliance with the Policy and these procedures particularly when processes change.

3.3 Business Owners (for the business system(s) they are responsible for):

(a) ensure that appropriate access controls are in place to protect information;

(b) authorise appropriate individual access to information;

(c) determine and document who can access the information held within the business system;

(d) approve in writing any requests for data feeds from information systems they are the Business Owner of;

(e) ensure that during any system commissioning, upgrade, migration or decommissioning the information and records management requirements are considered and documented;

(f) ensure that all business rules, processes or procedures, related to the system(s) they are responsible for, include information and records management requirements;

(g) determine the value of the information by classifying information following the Digital Solutions guidelines;

(h) ensure that risk assessments for the information assets are performed particularly when processes change;

3.4 Executive Sponsor:

(a) reports to Senior Leadership Team any risks identified with the information management component of these procedures;

(b) regularly reviews aspects of these procedures to ensure the ongoing appropriate management of information.

3.5 Senior Leadership Team:

(a) supports and models the management and security of information at the University in accordance with these procedures;

(b) is responsible for implementing and maintaining these procedures in line with the Policy;

(c) ensures that all information has an identified Business Owner;

3. 6 Digital Solutions staff will:

(a) liaise with Business Owners and Information and Records Management to ensure that University Information Systems comply with the Policy and these procedures;

(b) liaise with Business Owners and Information and Records Management to assess information and records management in system acquisition, maintenance, upgrades and decommissioning, and implement these practices as appropriate.

3.7 Information and Records Management will:

(a) provide advice and support to staff on how to comply with the Policy and relevant procedures;

(b) be responsible for the creation and delivery of an information and records management programme that includes staff training;

(c) review and approve in principle disposal of records, subject to final approval from the Business Owner;

(d) develop and deliver a self-audit / benchmarking programme to improve awareness and compliance;

(e) escalate issues regarding non-compliance with the Policy as appropriate;

(f) liaise with Digital Solutions and Business Owners to ensure that University Information Systems comply with the Policy.

4. Definitions

In this Statute/Policy/Procedure, unless the context otherwise requires:

Business owner	The person responsible for the creation of the information, for setting the controls, collection and use of the information. There may be more than one business owner.
Business system	An organised collection of hardware, software, supplies, policies, procedures and people which stores, processes and provides access to an organisation's business information[1].
Executive Sponsor	The role with overall responsibility for this policy, which includes establishing and maintaining University-wide information management standards, procedures and guidelines that support this policy. The Executive Sponsor is nominated by the Vice-Chancellor of the University to be the first point of contact for Archives New Zealand. The Sponsor is also responsible for periodic reviews of this policy to ensure the policy aligns with the University's strategic plan and legal obligations.
Information	Information, whether in its original form or otherwise, including (but not exclusively) documents, a signature, a seal, text, images, sound, speech, or data compiled, recorded or stored in in any format (paper, electronic files, databases, texts, social media etc)
Information Systems	Any computer system, telephone or peripherals owned or administered by the University, together with any associated electronic or mobile data storage systems; and any communication devices, wired or wireless network intended for the transfer of information, whether on University campuses or to which Users have access through University facilities, including the Internet.
Record	Information created, received and maintained as evidence and information by an organisation or person, in the transaction of business[2]. Records do not include records created by the academic staff or students of a tertiary education institution, unless the records have become part of the records of that institution[3].
Staff Member	An employee of the University.
University	Means Te Herenga Waka Victoria University of Wellington.

[1] AS/NZS ISO 23081-2:2007
[2] Public Records Act 2005
[3] Public Records Act 2005

User	User of University Information systems.

Related Documents and Information

5. Related Documents

Education and Training Act 2020

Official Information Act 1982

Privacy Act 2020

Public Records Act 2005

Acceptable Use of Information Systems Statute

Privacy Policy

Privacy Notice

Delegation Framework

Cyber Security Procedures

6. Document Management and Control

Approval Agency	Vice-Chancellor
Approval Date	03.06.2021
Last Modified	03.06.2021
Review Date	June 2024
Sponsor	Provost
Contact Person	Manager, Information and Records Management Extn 5985

Appendix 1: Record Disposal Process

1. Annually, staff identify records due for disposal using the Disposal Authority (DA);
2. Staff document records due for disposal using a record destruction authority form (available from the Information and Records Management intranet pages);
3. Staff forward record destruction authority form to a certifying officer for approval to dispose or instruction to retain;
4. Staff carry out the certifying officer's decision;
5. Staff send master-copy of record destruction forms to Manager, Information and Records Management for central storage and management.