CAPILANO UNIVERSITY	POLICY		
Policy No.	Officer Responsible		
B.605	**Vice President, Finance and Administration**		
Policy Name			
Records Management			
Approved by	Replaces	Category	Next Review
Board	**n/a**	**IM&DT**	**June, 2027**
Date Issued	Date Revised	Date in effect	Related Policies
June 25, 2024	**NEW**	**June 25, 2024**	**B.700 Privacy and Access to Information Policy** **OP.604 Acceptable Use and Security of Digital Technology** **OP.606 Student Records Management Policy** **E.301 Philanthropy & Alumni Relations: Data Management Policy**

1. PURPOSE

1.1 The purpose of this Policy is to set out directions and establish responsibilities for the creation, maintenance, retention and destruction of Records at Capilano University (the "University") in line with applicable federal and provincial laws including but not limited to the *Freedom of Information and Protection of Privacy Act* (FIPPA).

1.2 All Records created or received by University officers and employees in the course of their duties on behalf of the University belong to the University and are subject to its overall control.

2. DEFINITIONS

Administrator means an employee that works in a managerial role. This includes, but is not limited to Deans, Associate Vice-Presidents, University Librarian, Directors, Managers, HR Business Partners and any other equivalent positions. Administrators are excluded from or not represented by a union.

Destroy / Destruction in the context of this policy means to eliminate or delete Records beyond any possible reconstruction including through:

a) physical destruction by means of burning, pulping or shredding;

b) secure deletion of electronic Records; or

c) physical destruction of electronic storage media

Members of the University Community means employees, students, board members and volunteers.

Records include books, documents, maps, drawings, photographs, audio or video recordings, letters, papers, and any other thing on which information is recorded or stored by graphic, electronic, mechanical or any other means, but does not include a computer program or any other mechanism that produces Records. Records include email and information stored electronically.

Records Custodians are Administrators with assigned responsibly to manage Records for a faculty or department.

Records Retention Schedule refers to the matrix of retention periods for Records in the custody and control of the University.

Transitory Records are Records of temporary usefulness, required only for a limited time for the completion of a routine action or the preparation of an ongoing Record. Transitory Records do not include those Records required to meet statutory obligations, or to sustain administrative or operational functions. Transitory Records may include drafts, notes, calculations, and superseded documents.

Personal Information Bank means an aggregation of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

3. SCOPE

3.1 This Policy applies to all departments and units of the University, and to all Members of the University Community and any contracted service providers of the University who create, receive or maintain Records at the direction of the University.

3.2 This policy does not apply to:

a) academic instructional material or research data;

b) Records that are subject to solicitor-client privilege or

c) Records that have been identified by the University library to be collected in an archive for historic purposes.

3.3 Directions for the management of student records are set out in OP.606 Student Records Management Policy. Directions for the management of donor and alumni records are provided in E.301 Philanthropy & Alumni Relations: Data Management Policy.

4. POLICY STATEMENT

Records Creation, Access and Maintenance

4.1 Records are created and maintained by academic and administrative units of the University to perform necessary transactions for the management of a BC post-secondary institution including admissions, registration, instruction, research, student care and support, alumni relations, employment, facilities management and other support functions.

4.2 It is the responsibility of individual units that create and maintain records to make sure appropriate security measures are observed, with particular consideration of any Records containing sensitive, confidential or personal information.

4.3 The University will develop and maintain a directory of Records, including the identification of all Personal Information Banks.

4.4 The University will provide access to information through routine release of Records including self-service mechanisms to access personal information where possible. Access to Records not covered by routine release is governed by B.700 Privacy and Access to Information Policy.

Records Retention and Destruction

4.5 Records must be retained for as long as they are required to meet legal, administrative, operational, and other requirements of the University. The University will maintain a Records Retention Schedule which lists the significant categories of records held by the University and sets out the unit responsible for the record category and the appropriate retention period. The Record Retention Schedule will be updated on at least an annual basis with approval by the Senior Leadership Council.

4.6 Records will be retained by the department in which they were received or created unless otherwise listed in the Records Retention Schedule.

4.7 Records need not be retained in printed form but may be stored in electronic format. If paper documents are scanned and an electronic copy is to be preserved, the original paper document may be destroyed unless they are identified for permanent preservation. In such case, the original paper record should be sent to the university archives for management.

4.8 Records must be retained for the periods of time set out in the Records Retention Schedule. For clarity, unless otherwise specified, the periods of time indicated in the Records Retention Schedule should be calculated from the later of:

a) the time the relevant Record is created or received;

b) the last date the relevant Record is used in the course of an employee or service provider's duties to the University, or to make any determination about a student or other individual at the University; and

c) in the case of any Record evidencing a contract, agreement or continuing obligation, the expiration, termination or completion of such contract, agreement or obligation.

4.9 Any Record not captured in the Records Retention Schedule, other than Transitory Records, must be retained for a period of seven years.

4.10 Transitory Records should be retained only while there is an operational need to retain the Record and should be Destroyed before the end of the period indicated in the Records Retention Schedule for the category of Record. Transitory Records created in the preparation of a final record may be Destroyed prior to the expiry of the retention period.

4.11 Records that have been retained for the period indicated in the Records Retention Schedule should be Destroyed promptly at the end of that period unless there is a continuing operational reason to retain them for a period exceeding the retention period. Written approval is required from the Records Custodian and, where different, a senior Administrator (Director level or above) prior to Destruction.

4.12 Records containing confidential material or personal information pertaining to identifiable individuals will be Destroyed in a secure and permanent manner.

a) The University provides confidential shredding bins at locations across campus where paper records can be securely disposed of.

b) Personal information or other confidential materials stored electronically should be securely destroyed by double-deletion, where the file is deleted, and then removed from the applicable Recycle Bin or other location for deleted files.

4.13 Records scheduled for destruction (including Transitory Records) must not be destroyed if they are:

a) identified in current or pending litigation;

b) responsive to a current request made under FIPPA;

c) the subject of an audit; or

d) identified in quasi-judicial and legal proceedings.

4.14 Where Records are to be kept permanently, duplicate Records, not used as working copies, should be Destroyed on the instruction of the Custodian of the permanent Record and with the approval of the Administrator of the department or faculty holding the duplicate Record. Some permanent Records may be identified by the University Librarian as having historical value to the University and be candidates to be held by and preserved for access in an official archive of the University.

5. RESPONSIBILITIES

5.1 The Director, Risk Management (or their delegate) has the responsibility to lead and manage the University's records management activities:

a) communicating the contents of this policy to the University community and educating Administrators, Custodians and employees about their responsibilities with regard to Records management and their obligations under this policy;

b) maintaining the University's Record Retention Schedule; and

c) developing and implementing procedures and guidance to support this policy as needed.

5.2 Administrators are responsible for making sure that:

a) this policy, any related policies applicable to their area and any associated procedures approved by the University are understood and complied with within their faculties and departments; and

b) Records in the custody or control of their faculty or department are retained for the applicable retention period set out in the Record Retention Schedule; and

c) Records containing personal or confidential information are protected from unauthorized access and disclosure, in accordance with B.700 Privacy and Access to Information Policy and related procedures.

5.3 Administrators identified as having a Records Custodian role are additionally responsible for

a) Maintaining an inventory of all faculty or department Records, including those in on and off campus storage;

b) approving the secure Destruction of Records at the end of the applicable retention period;

c) maintaining a record of all such approvals and confirmation of the secure destruction of expired Records; and

d) assisting the Director, Risk Management and Privacy Officer (or delegate) with Freedom of Information (FOI) Requests as needed.

5.4 The Records Custodians retain responsibility for all faculty or department Records except if there is a formal transfer of responsibility to another group or individual, for example if it is determined that the Record should be archived.

5.5 All Employees are responsible for:

a) creating records in a professional and objective manner

b) following the directions outlined in this policy, OP.604 Acceptable Use and Security of Digital Technology and any related policies and associated procedures applicable to their area and for reporting material non-compliance to their Administrator; and

c) when leaving a position or changing position within the University, ensuring any Records they are responsible for are left in the custody or under the control of the University.

6. PERSONAL INFORMATION

6.1 The University seeks to protect the privacy of individuals by ensuring personal information is stored appropriately to restrict unauthorized access and is Destroyed when it is no longer needed and the applicable retention period has passed.

6.2 The University recognizes that personal information about an identifiable individual must be retained for at least one year if the information is used for the purposes of making a decision that affects the individual.

7. STORAGE

7.1 Records kept in storage on- or off-campus must be properly labelled with the name of the department or faculty that is storing the Record, the contents and expiry dates.

7.2 The University contracts with secure off-campus Records storage providers as needed. Corporate Services will establish and manage contracts with and act as the liaison between the department or faculty and the service provider.

7.3 Departments and Faculties that use off-campus storage must maintain an inventory of all Records sent offsite to protect against loss or theft of Records and so Records can be accessed if needed. Inventories should be regularly audited so records that reach the end of their retention period are identified for Destruction in a timely manner.

7.4 Agreements with off-campus Records storage providers will require the organization to return or to confirm the destruction of Records identified for Destruction in a secure and permanent manner.

8. DESIGNATED OFFICER

The Vice President, Finance and Administration is the Policy Owner responsible for the oversight of this Policy. The Administration of this Policy and the development, subsequent revisions to and operationalization of any associated procedures is the responsibility of the Director, Risk Management.

9. RELATED POLICIES AND GUIDANCE

B.600 Privacy and Access to Information Policy

OP.606 Student Records Management Policy

E.301 Philanthropy & Alumni Relations: Data Management Policy

OP.604 Acceptable Use and Security of Digital Technology Policy

Record Retention Schedule

OP.700.01 Right to Request Correction Procedure

Capilano University Main Campus – Confidential Shredding Bins Pick Up & Locations

10. REFERENCES

Freedom of Information and Protection of Privacy Act

University Act

Limitation Act