UC Policy Library

Privacy Policy

Last Modified	May 2021
Review Date	October 2021
Approval Authority	General Counsel | Registrar
Contact Officer	Information and Records Manager – Office of the General Counsel | Registrar

Introduction

This document provides information on the University's approach to meeting its obligations and ensuring compliance by the University community with the provisions of the *Privacy Act 2020 (New Zealand Legislation website) ("Privacy Act").*

This document covers the privacy principles, identifies those within the University responsible for ensuring compliance and the types of personal information the University retains.

Definitions

Affiliated person/s or organisation/s – organisation/s which, or person/s who, work in an official capacity with University students and/or alumni and may be subject to a Memorandum of Understanding (MOU) or agreement with the University such as the University of Canterbury Students' Association (UCSA), student Halls of Residence and UC International College (UCIC).

Authorised staff – any member of staff employed by the University, who in their capacity at the University and for the purpose of their role, or to perform their work, is required to access, collect, use or distribute information and includes general staff who are responsible for providing assistance to students whose academic progress is of concern.

Elected/nominated official – any member of a University committee whether paid or unpaid and whether elected, seconded, nominated or self-nominated.

Evaluative Material – "evaluative or opinion material compiled solely—

(a) for the purpose of determining the suitability, eligibility, or qualifications of the person to whom the material relates—

(i) for employment or for appointment to office; or

(ii) for promotion in employment or office or for continuation in employment or office; or

(iii) for removal from employment or office; or

(iv) for the awarding of contracts, awards, scholarships, honours, or other benefits; or

(b) for the purpose of determining whether any contract, award, scholarship, honour, or benefit should be continued, modified, or cancelled; or

(c) for the purpose of deciding whether to insure any person or property or to continue or renew the insurance of any person or property." (Section *23(2B) Official Information Act 1982 (New Zealand Legislation website)*; see also *Section 50 Privacy Act 2020 (New Zealand Legislation website)*).

Personal information – any official information held about an identifiable person that is of a personal nature, such as name, date of birth etc. that could be used to identify that person. See the full list of the types of information collected in *section 3 "Personal Information"*.

Sensitive personal information – a subset of personal information; sensitive personal information is typically determined by considering the potential or actual loss of dignity, humiliation, or injury to feelings that would result if that information is lost, inappropriately accessed, or used. Sensitive personal information is information relating to health, racial or ethnic background, or criminal records.

StudyLink – a service of the Ministry of Social Development which provides financial support to students.

Third party – any person or organisation other than the University or a member of the University.

Unit – a generic term referring to any college, school, department, centre, division, service area or academic unit of the University, as appropriate in the particular context.

Policy Statement

The document applies to any University staff member, student or any person who works in a paid or voluntary capacity, whether an elected/nominated official or not, and any affiliated person/s or organisation/s (known as the University community) who deal with personal information relating to other students, staff, alumni and/or members of the public.

The purpose of this document is to provide a foundation of best practice to ensure compliance by the University community with the provisions of the *Privacy Act 2020 (New Zealand Legislation website) ("Privacy Act").*

It should be noted that Student Health and any counselling service offered within the University will be subject to the *Health Information Privacy Code 1994 (Office of the Privacy Commissioner NZ website)*, being a code of practice issued under the *Privacy Act.*

1. Privacy Principles

The University will collect, use, store and disclose personal information as necessary to carry out its purposes (core functions and activities), including its statutory functions, in alignment with the *Privacy Act 2020 (New Zealand Legislation website)* and this document.

The *Privacy Act 2020 (New Zealand Legislation website)* requires that public sector organisations such as the University comply with the IPPs as set out in Part 2 of the Act. The University has established processes and procedures which align with the summarised privacy principles below.

At the heart of the *Privacy Act 2020 (New Zealand Legislation website)* are 12 Information Privacy Principles (IPPs) which outline how personal information is to be collected, stored, used and disclosed (refer below). This document is designed to apply the concepts contained in the IPPs to the University environment. For more detailed information on privacy not covered within this document refer to the *Privacy Act 2020 (New Zealand Legislation website)* and the *Office of the Privacy Commissioner NZ (Office of the Privacy Commissioner NZ website)*.

1.1. Purpose of Collection

IPP1 is a collection principle. An agency should not collect personal information unless it is for the lawful purpose connected with a function or activity of that agency, and it is necessary to collect that information for that purpose.

1.2. Source of Personal Information

IPP2 outlines that personal information must be collected directly from the individual concerned unless the collection is believed to be an exception on reasonable grounds, such as the information is already publicly available.

1.3. Collection of Information

IPP3 outlines that during collection of personal information, an agency must take reasonable steps to ensure the individual is aware of the fact the information is being collected, for what purpose, and who will use it.

1.4. Manner of Collection

IPP4 outlines that the personal information must not be collected by unlawful means or means that are unfair or intrude on the personal affairs of the individual.

1.5. Storage and Security

IPP5 outlines the standards that organisations must meet for the accuracy, currency, completeness and security of personal information.

1.6. Access

IPP6 outlines access rights to personal information held by an agency.

1.7. Correction of Information

IPP7 outlines access and correction rights, giving a general right of access to personal information and the right to have that information corrected if it is inaccurate, incomplete or out of date.

1.8. Checking Accuracy of Information Before Use

IPP8 specifies that an agency must take all reasonable steps to ensure information is accurate, complete, relevant and not misleading prior to using that information.

1.9. Retention of Information

IPP9 specifies that an agency cannot keep information for longer than is required for the purposes for which the information may be lawfully used.

1.10. Limits on Use

IPP10 specifies that an agency cannot use information that has been collected for one purpose, for another purpose that was not originally specified.

1.11. Limits on Disclosure

IPP11 outlines the limits under which an agency may disclose collected personal information. For example, personal information must not be disclosed unless the agency reasonably believes that the disclosure is authorised by the individual and is in connection with the purpose for which it was obtained.

1.12. Unique Identifiers

IPP12 says that a unique identifier must not be assigned to individuals, unless it is necessary to enable the agency to perform its functions efficiently. This provides a safeguard against the creation of a single identifier that could be used to cross-match data across agencies.

2. Purpose, Collection, Consent, Use and Disclosure

2.1. Purpose of Collection

The purposes for which personal information is collected and used by the University include:

a. Administering teaching programmes including (but not limited to)
   i. maintaining records of student progress;
   ii. ranking of students;
   iii. details of tuition fees;
   iv. providing information technology (IT) services;
   v. providing library services;
   vi. providing equal opportunity access to teaching programmes;
   vii. assigning student identification numbers;
   viii. providing general assistance to students;
   ix. identification of course supervisors/teaching or academic staff and qualifications; and/or
   x. seeking guidance from appropriate peers/colleagues within the University in the resolution of any teaching problem, research and scholarship, audit, and scholarships administration.

b. Maintaining a repository of knowledge and expertise.

c. Providing services to society (for example critic/conscience of society, dissemination of information to the community, and maintaining external relationships).

d. Discipline and traffic enforcement.

e. Providing administrative assistance to Halls of Residence, the University of Canterbury Students' Association and the University of Canterbury Foundation.

f. Strategic budgeting and forecasting.

g. Administering and planning human resources (including health and safety).

h. Reporting/disclosing information to Government bodies or other agencies for the purposes of funding or to meet contractual/legislative obligations. For

example, the Ministry of Education, Department of Work and Income, Inland Revenue Department, NZ Immigration Service, Ministry of Foreign Affairs and Trade, Te Puni Kokiri, tribal trusts and other financial support organisations, the *Office of the Ombudsman (Office of the Ombudsmen website),* and the *Office of the Privacy Commissioner (Office of the Privacy Commissioner website)*.

i. Use of Federation Services. The University is a member of the *Tuakiri New Zealand Access Federation (Tuakiri REANNZ website)*, which is a service that enables students, staff, and others to seamlessly access certain IT resources using a single set of user credentials. Some federated services require sharing unique identifiers or personally identifying information (which can include preferred name, UC user code, affiliation as staff, student, or alumni, or an anonymous token to identify an individual to the service). Students, staff, and others who use services registered with the Tuakiri Federation may have their information disclosed in the form of tokens for the purposes of accessing services. No data will be released until users log in to the service for the first time.

j. Supplying student email addresses which are hosted by Office 365, a Microsoft platform. Student's preferred name, enrolment status ('enrolled' or 'alumni'), user code and password are provided to Microsoft in order to open their Office 365 email account as a license requirement. The data collected by Microsoft through the University's use and administration of the Office 365 services is covered by Microsoft's privacy statement and practices. Students should be aware that their customer data (including all text, sound or image files) will not be disclosed to any third parties unless required by law. Information about the security of the services of Office 365 data can be found online at *Office 365 Trust Center (Microsoft Office website)*. Students should also be aware that the services of Office 365 may enable access to third-party services, such as Facebook or other Microsoft products and services, such as Bing Maps or Yammer. Privacy practices for these products may differ from the services. Use of such services, and any information provided to them, is governed by their service specific privacy statements.

k. Supplying information provided via the use of web applications as detailed in the forthcoming *Schedule of Approved Website Software and Services ("Schedule")* as required by licence to facilitate the University's use of these applications. The data collected by these applications is covered by their respective privacy policies and statements, which are provided via the forthcoming *Schedule*. The schedule includes an explanation of the purpose the application is used for.

l. Providing information to other tertiary institutions for student transfer purposes or in the administration of conjoint teaching agreements.

m. Publication, in the graduation programme, of awards conferred by the University.

n. Maintaining alumni records.

o. Marketing/public relations (although consent will be obtained from an individual if the University wishes to use his/her name/photo for publicity).

p. Fundraising and maintaining donor records.

Note: *The University does not collect information for the purpose of reporting to parents, relatives or employers even though any of these people may be paying tuition fees. While the University reserves the right to refuse a request for access to information, any arrangement for reporting to employers paying for work related study or to any agency providing scholarship assistance must be arranged prior to course-work commencing with the written consent of the student.*

2.2. Collection of Information

The University collects information from staff and students during enrolment and employment processes when commencing at the University. Information may also be collected via the student identification card system or by verbal or written correspondence during a person's employment or period of study. It can also be provided to the University by other educational institutions or Government bodies, according to statutory requirements.

The University makes use of third party software and services as part of its website. This software contributes towards the University's functions, and may record information including, but not limited to, browser type, the user's internet server address and domain name, the user's IP address, time, date and duration of the visit, pages accessed, documents downloaded, the previous site visited, and cookies. This information is used to improve website services and for targeted marketing.

The University's use of software and services on its website is under the terms of agreements with the software and service provider and their policies. These terms and policies are provided in the forthcoming *Schedule of Approved Website Software and Services*.

Information collected by other means, such as online forms, follow the consent and privacy guidelines provided by the University web team during the creation of the forms. (For a consent statement template for forms *refer to Appendix A*.)

The University may also collect statistical information to assist both itself and other government bodies to provide the most appropriate educational courses and facilities to students. When this information is disclosed, it is checked for privacy implications. Any compilation or publication of those statistics will not reveal the identity of the individual from whom it was collected unless explicit consent is obtained from the individual.

[Refer to the *Student Community Online Survey Policy (PDF, 300KB)* if you are thinking of doing a survey that involves requesting or collecting personal information and data from cohorts of students.]

Any collection of information that is not consented to during the above processes requires specific consent from the individual whose personal information is being collected in alignment with *section 2.3 "Consent by Individuals"* below.

2.3. Consent by Individuals

Consent given by individuals to collect information should be obtained and noted. If personal information is used only for the purposes stated for its collection and use at the time consent is given, then further consent or authorisation is not required.

If a matter arises that will necessitate using collected information for purposes not previously disclosed and/or agreed to, then new consent is required. This should be informed consent: the person must be aware of all the intended uses/disclosures for the personal information and that there is no obligation to give such consent.

2.4. Student Declaration

Students sign a declaration during enrolment which allows for the collection and use of specific information according to the conditions of the declaration. This declaration can be viewed on the *UC Privacy Statements web pages (University Privacy Statements web page)*.

2.5. Use and Disclosure

The University may use an individual's personal information in a number of ways, according to the consent given by the individual at the point of collection, including

- to carry out the University's functions and activities;
- to provide information about the University's courses and facilities to students or prospective students;
- to provide educational services and to determine and provide appropriate support services and facilities to students;
- to administer and manage processes such as admission, enrolment, scholarships, accommodation, billing and collection of fees and charges, examinations and academic standing; and
- to administer and maintain information technology services and facilities for the University.

University staff seeking assistance or guidance in the management of an issue from colleagues/peers, should not identify the person concerned unless it is necessary.

No personal information relating to disabilities/medical conditions is shared without the informed consent of the individual, unless it is necessary to prevent or lessen a serious and imminent threat to individual or public safety. In these circumstances only, this information may be provided to the relevant authority. This may include authorities such as UC Security and Campus Community Support staff, the Police or other emergency responders.

2.5.1. Disclosure of Information to Third Parties

The University will take reasonable steps to ensure that personal information is not disclosed to third parties except in certain circumstances, including where

- the individual has consented to the release; and/or
- the release of the information is a condition of a student's sponsorship or enrolment; and/or
- the University is authorised or required by law or regulatory requirements to disclose the information to, for example but not limited to, the IRD or StudyLink; and/or
- the information is provided to a third party that provides services to the University in alignment with its core function, in which case the University will ensure that the service provider agrees to preserve the confidentiality of personal information; and/or
- the University is not prohibited from disclosing the information, as described in the *Privacy Act 2020 (New Zealand Legislation website).*

If there has been a request by an individual for personal information about another individual then this request will be treated under the *Official Information Act 1982 (New Zealand Legislation website)* (see the University's *Official Information Policy (PDF, 195KB)*). See *section 4.2 "Access to Information – Official Information Requests and the Privacy Act".*

2.5.2. Student Number

Unless required by law (e.g., the National Student Identification Number), the University does not use the same number as another agency to identify a student, other than as specified in section 2.1(i) about the Tuakiri New Zealand Access Federation.

2.5.3. Marketing

The University does not sell, rent or trade personal information. Where organisations or businesses seek to inform individuals about employment, other opportunities or membership of professional organisations, it is acceptable for the University to receive the material and send it out on the organisation's behalf, recouping any associated costs from the organisation or business. Otherwise, if no

consent to receive marketing material has been obtained from individuals, a request to market to individuals directly would be declined.

Individuals who receive this information will then have the ability to 'opt in' to an opportunity if they wish to be contacted or involved further with the external organisation/business. The University will not disclose personal information externally.

2.5.4. Third Party Contractors

Under the *Public Records Act 2005 (New Zealand Legislation website)*, the University must create and maintain full and accurate records of personal information in accordance with normal, prudent business practice. This includes activities carried out by contractors on the University's behalf. These records must also be maintained in an accessible format over time.

Third party contractors working for the University are bound by specific confidentiality/non-disclosure agreements. Where they may be required to collect, use, store, or distribute personal information, contractors or other third parties will be required to work within the provisions of this policy (e.g. see *section 4.1 "Security of Information"*) and the *Privacy Act 2020 (New Zealand Legislation website)*.

2.5.5. Disclosure of Information via Telephone, Text or Email

University staff must not give personal information out over the phone or send personal information by facsimile, text, or email, unless the staff member is reasonably satisfied that the receiver is a person to whom that personal information may be disclosed, or is the individual to whom the personal information relates. Steps a staff member may take to ensure identification of the receiver include calling the individual back at a known telephone number, asking for a student identification number, recognising the receiver's voice, or validating an individual's identity by asking specific questions that can be verified by the staff member (e.g. date of birth or courses studied last semester).

2.5.6. Outcome in Disciplinary Procedures

If the University receives a complaint about a person (staff member or student), thereby invoking any disciplinary procedure, the complainant will be advised from the outset that while it is the usual practice of the University to advise the complainant that an outcome has been reached, he or she will not normally receive full details of the action (if any) taken against that person.

2.5.7. Enquiries from the Police or Process Servers from the Court or Other Government Officials

Important note: If a University staff member receives a request from the police, a process server from the Court, or other government official (including immigration) to access personal information, the request is referred to the **University Privacy Officer** (details in *section 8 "The Role of the University Privacy Officer"*).

A request from the police will be managed following the processes for release of information pursuant to the *Official Information Act 1982 (New Zealand Legislation website)* (including confirming the identity of the requester).

While personal information may be released to these agencies (*refer to section 2.5.1 "Disclosure of Information to Third Parties"*), to avoid prejudice to the maintenance of the law (including the prevention, detection, investigation, prosecution and punishment of an offence) it is not the University's policy to provide open access to such information. There will be times when it is appropriate for these agencies to obtain a warrant from the Court ordering release of the information.

If the Police are seeking the assistance of a University staff member to contact a student or staff member

- in case of accident, sudden death or emergency – reasonable assistance is given to find the person concerned and ensure that person has the opportunity to speak with the Police in private.
- in non-emergency cases (e.g., return of lost items), the University staff member should make a reasonable effort to contact the person concerned and advise him or her to contact the Police.

3. Personal Information

The types of personal information the University will normally collect and maintain for its purposes are listed below.

3.1. Examples of Personal Information that may be Collected:

- Full name and any alias or previous names.
- Contact details (including address, telephone and email address/es).
- Date of birth.
- Disability information (to provide appropriate facilities and equal opportunity access to University services).
- Emergency contact/s.
- Gender*.
- Nationality/citizenship*.
- Ethnic identification*.
- Qualifications/academic records.

- Presence/location on-site.
- Use of the UC website, including
  - internet address of the browser;
  - internet server address;
  - domain name;
  - IP address;
  - date, time and duration of visit to website;
  - pages accessed and documents downloaded;
  - previous site the user visited;
  - type of web browser software used, and
  - cookies.
- Information Technology accounting information including records of emails sent and URLs of pages and sites accessed by individuals.

*These questions normally represent statistical information required for Ministry of Education funding and to inform best practice in University equal opportunity policy development and implementation. As per the *Human Rights Act 1993 (New Zealand Legislation website)*, sensitive personal information will not be used to discriminate.

3.2. Specific Information that may be Collected from Students:

- Courses for which a student seeks to enrol.
- Prior education/occupations including identification of last secondary school attended.
- Details of concurrent enrolment at other tertiary institutions.
- Details of any relevant disqualification.
- Student progress.
- Details of vehicle/s requiring student parking permits.
- Photograph/s (for identification purposes).
- Information on behalf of government/regulatory bodies, such as WINZ and StudyLink.
- Banking/credit card information.
- Correspondence between the University and the student.
- Personal information relating to the investigation and resolution of a disciplinary matter.

3.3. Specific Information that may be Collected from Staff:

- Recruitment information:
  - Application form (e.g., including confirmation of eligibility to work in New Zealand, qualifications, previous experience, list of referees, criminal convictions, health issues relevant to the job);
  - Curriculum vitae;
  - Evaluative material (references from previous employers, University staff)*;
  - Equal Opportunity Monitoring information (ethnicity, gender, disabilities);
  - Evaluative tests;
  - Criminal record check (relevant to the job); and
  - Health record checks (relevant to the job).
- Salaries/wages.
- Details of job including units, titles, nature of job and employment contract (e.g., fixed term individual), dates of employment, hours worked and leave plans.
- Bank and tax information.
- Emergency contact details.
- Details of vehicle/s requiring staff parking permits.
- Photograph/s (for identification purposes).
- Languages spoken.
- University committee memberships.
- Further evaluative and non-evaluative material for promotions/other applications and performance review materials. This may include course surveys, statistical information which is accessible by the Learning and Teaching Committee, the relevant Heads of Departments/Heads of Schools and the individual concerned.
- Correspondence between the University and the staff member.
- Personal information relating to the investigation and resolution of a disciplinary matter.

*****Care is taken to ensure that a prospective staff member is aware that previous employers or other University of Canterbury staff may be contacted to avoid inappropriate disclosure of the job application.

3.4. Specific Information that may be Collected from the Public/Alumni may include

- banking/credit card information;
- details of current employer – particularly for workers of other agencies contracting with the University;
- education and career history;
- correspondence between the University and a member of the public; and

- personal information relating to the investigation and resolution of a disciplinary matter.

4. Management of Personal Information

4.1. Security of Information

The University will take reasonable steps to protect the personal information it collects from misuse and loss and from unauthorised access, modification or disclosure. Personal information is normally stored by the University in electronic form, which is protected from unauthorised access by a password system. University staff have access to personal information only to the extent that it is required for them to carry out their duties.

Personal information in hard-copy form may also be stored in a secure place in the University department that uses that information.

The University applies a records management framework that requires information to be destroyed or archived according to the *Public Records Act 2005 (New Zealand Legislation website)* disposal requirements and in compliance with this legislation, will not retain information for longer than necessary for its intended usage. These retention and disposal requirements are detailed in the *General Disposal Authority for New Zealand Universities DA337 (University Information and Records Management web pages)*. See also *section 4.5 "Record Keeping"* below.

4.2. Access to Information – Official Information Requests and the Privacy Act

If an individual makes a written request to the University for access to their own personal information the University may hold, the University will provide the individual with access to that information under the provisions of the *Privacy Act 2020 (New Zealand Legislation website)* unless there is an applicable exception within the IPPs.

If an individual makes a written request to the University for access to another individual's personal information (i.e., not their own information), the release of that information will be governed by the provisions of the *Official Information Act 1982 (New Zealand Legislation website)* and/or the *Privacy Act 2020 (New Zealand Legislation website)* as required. The request may be withheld under the provisions of these Acts to protect privacy or released, if no privacy interest exists to impede release.

4.2.1. An Individual Requesting Access to Information

The University verifies the identity of the requestor to ensure it is the individual concerned or his/her agent (for verifying via telephone, *refer to section 2.5.5 "Disclosure of Information via Telephone, Text or Email")*.

The University responds to such requests as soon as practicable but no later than 20 working days. The University contacts the requester and advises if more time is needed and the reasons for such a delay.

If the person making such a request is not satisfied with the time taken to provide the information, he/she is advised of his/her right to complain to the Office of the Privacy Commissioner.

If the individual has requested urgency then the individual is required to give reasons.

For more details around the procedural provisions relating to access to and correction of personal information, refer to *Part 4* of the *Privacy Act 2020 (New Zealand Legislation website).*

4.2.2. Students' Access to Results and Examination or Final Test Scripts

Students are entitled to obtain, upon request, their own grades and marks. Students may also view final scripts for each item of assessment under supervision. Students are referred directly to the appropriate unit for individual items of assessment, examination and test results not held by the Records, Examinations and Graduation office (REG).

The University and its units provide the information on grades/marks or access to scripts as soon as possible and not later than 20 working days from the date of the request.

If a student requests a copy of a script, the unit will forward the request to the Records, Examinations and Graduation office in Registry as soon as possible so that the student's request may be answered promptly.

For further information on student access to results refer to the *University Regulations (University Regulations website)*.

4.2.3. Students' Access to Aegrotat, Compassionate Pass and Related Reports

Students will normally be entitled to access special consideration and related reports/records (including applications for special conditions for examinations and tests) subject to the exceptions contained in *Part 4* of the *Privacy Act 2020 (New Zealand Legislation website)*.

4.2.4. Transfer of Requests

In certain circumstances, personal information may be held by a number of organisations for various purposes. In instances where the University receives a

request for access to information that is no longer held by the University, or that is closely connected with the functions or activities of another organisation, the University must promptly (not later than 10 working days after the request is received) transfer the request to that other agency and inform the individual making the request accordingly.

4.3. Accuracy of Information

The University endeavours to ensure that the personal information it collects, uses, or discloses is and remains accurate, complete and up to date. If an individual believes that the personal information retained by the University about them requires changing or updating they should contact the relevant department administrator, business unit or, if necessary, the **University Privacy Officer** (*information in section 8 "The Role of the University Privacy Officer"*).

4.4. Privacy Complaints or Breaches

If an individual wishes to access or change their personal information, or to lodge a complaint about a possible breach of privacy or has any query on how personal information is collected or handled, they should contact the **University Privacy Officer** (information in *section 8 "The Role of the University Privacy Officer"*).

4.5. Record Keeping

The IPPs apply to both physical (hard-copy) and electronic files or collections of personal information, including data. A significant portion of the personal information collected by the University is held on electronic databases; other information is stored in unstructured digital formats such as email, electronic documents or images/film.

In some instances digital records (such as email, records stored in non-University, cloud-based repositories, or on removable storage media such as USB drives, hard drives or CDs) pose a significant risk of unauthorised access, loss or alteration. No sensitive personal information should be stored in uncontrolled systems or locations.

Personal information stored digitally has access restricted to only those staff needing to access it, and is deleted from the system when no longer required for the purposes identified in *section 2.1 "Purpose of Collection"*. This disposal is determined by reference to the *General Disposal Authority for New Zealand Universities DA337 (University of Canterbury website)*.

Deletion of information should be approved in line with the University records disposal framework. If in doubt, consult with the *University Privacy Officer* or the *University Information and Records Manager*.

Personal information stored in hard-copy formats is kept in a secure location (i.e., locked), accessed only by staff who are authorised for the purposes outlined during collection and, if it is accessed or retrieved from storage, a note recording its access and return is logged. Other steps taken to keep hard-copy personal information secure include

- keeping non-current material in locked filing cabinets or cupboards,
- ensuring personal information is not exposed to unauthorised people,
- locking offices while not in use, and/or
- ensuring personal information is not left on desks or open work spaces overnight.

Personal information is destroyed with safeguards taken to prevent inadvertent disclosure of the information

- by shredding or placement in a locked bin which has the contents disposed of in a confidential and secure manner; and
- with expert assistance if disposing of computer hardware.

4.6. Work Taken out of a Unit

It is recognised that there are critical times when staff may need to remove personal information from a business unit or college (e.g., job applications or marking). It is preferable that this information is only accessed offsite via electronic means through University networks. If that is impossible and it is absolutely necessary that personal information is to leave a business unit or college, staff must take the following precautions:

- Personal information travels securely – it is in a locked briefcase, or on an encrypted, password protected media file or device.
- Multiple instances of electronic personal information **must not** be copied to removable storage media or removed from secure systems. Examples of this type of personal information include
    - databases of student information,
    - databases of staff information, and
    - spreadsheets of personal information such as alumni lists.
- If travelling by public or private transport, information must not be left unattended at any time.
- During the time it is away from the University, all reasonable steps are taken to ensure the information is not accessed by unauthorised people.

4.7. Misuse of Personal Information

Without limiting the definition of misuse of personal information, the following practices are unacceptable to the University*:

- Intentionally breaching the *Privacy Act 2020 (New Zealand Legislation website)*, the *Official Information Act 1982 (New Zealand Legislation website)* or the access restrictions imposed by the *Public Records Act 2005 (New Zealand Legislation website)*.
- Reading or copying personal information to which the reader/copier has no authorised access.
- Divulging personal information given under an express undertaking it will remain confidential or, intentionally divulging personal information to any person who is not an authorised recipient of that information without lawful excuse.
- Intentionally introducing false or misleading material into any University database or file/record, or falsifying such records or deleting such records without authorisation.
- Using personal information for any purpose other than the purposes identified in *section 2 "Purpose, Collection, Consent, Use and Disclosure"* unless the individual has given explicit, informed consent to do so.

**Note: Section 105A Crimes Act 1961 (New Zealand Legislation website), "Corrupt use of official information". It is an offence if an official corruptly uses or discloses any information, acquired by him or her in his or her official capacity, to obtain, directly or indirectly, an advantage or a pecuniary gain for the official or any other person.*

4.8. Personnel Files

Personal information gathered from and/or about a successful applicant for employment or appointment at the University, will be retained on their personnel file for the purpose of considering and evaluating any other application they may make for employment or appointment by the University in any role other than that for which they originally applied to the University.

4.8.1. Unsuccessful Job Applications

Information relating to unsuccessful applications are destroyed[1] following the closing-off of the file for appointment, unless applicants request that their applications be retained for future consideration for other similar vacancies, should

[1] Destruction is governed by the *General Disposal Authority for New Zealand Universities DA337 (University of Canterbury website)*, Class 7.1.1 and with reference to the University's *Records Disposal Framework (UC Information and Records Management website)*.

they arise. In such instances, notice will be provided to give the applicant an opportunity to update the information provided.

4.8.2. Evaluative Material Related to Job Application

Evaluative material is maintained centrally with any regular personnel file/record but it is sectioned off (either physically within the same file or into separate files, or electronically using access rights and metadata) from the non-evaluative material (appointment letters, employment agreements, salary histories, leave records, etc.).

This information is available to those staff members normally party to that evaluation process, or who require it for a further authorised and specified purpose. It is not automatically available to the individual concerned (see the grounds for refusal in *Part 4* of the *Privacy Act 2020 (New Zealand Legislation website)*) and should be removed prior to an individual reviewing their personal file/record.

4.8.3. Retention of Personnel Records

All personnel records are retained only for as long as needed, and then disposed as either archives or destroyed based on their values as determined by section 7 of the *General Disposal Authority for New Zealand Universities DA337 (University Information Management web pages)*.

4.9. Collection and Distribution of Students' Assessed Material

Academic departments ensure that the collection and distribution of student work is secure. If assignments are collected or distributed using an online learning system (e.g., Learn), only authorised staff may access course details and receipt submitted material, or access and distribute grade information. The mark or grade that a student receives for a piece of work, is only disclosed to authorised staff,[2] e.g., those staff members normally party to that assessment process or staff who require access in order to perform their work. If assignments are collected by using locked postal boxes in a public area, departments check the boxes are cleared regularly to avoid overflow. Class lists are not downloaded and published outside of any online learning system (such as Learn), in any format or venue:

- Where work and grades are distributed in person, cover sheets with only the student's name and/or identification number are visible.
- Assessments must not be left outside offices or in hallways without being monitored or secure.
- If grading or assessment information is communicated orally, it is done in an area where others cannot overhear it.

5. Sensitive Personal Information

5.1. Management of Sensitive Information

The University recognises that some personal information can be more sensitive than other personal information (refer to definitions). To determine sensitivity, the question is whether an individual will suffer any actual loss or humiliation, loss of dignity and/or injury to feelings, if the information is lost or inappropriately accessed or used. For example the inappropriate disclosure of an individual's mental health status would be considered a breach of sensitive personal information.

Sensitive personal information recorded physically should not be left in staff pigeonholes or in-trays. It must be in a secure or locked area.

Hard-copy internal mail which contains sensitive personal information is sent in a sealed envelope and labelled as "strictly private and confidential" and "to be opened by the addressee only", rather than using the reusable internal mail envelopes.

Special consideration applications or related records (including applications for special conditions for examinations and tests) are considered sensitive personal information. It may be appropriate to store any medical or psychological evidence with the UC Health Centre.

Sensitive personal information is normally kept separate from any general file/record about an individual, either physically or in a digital environment, using access controls and metadata tags. This information is only accessible to the parties directly involved (although some material may be withheld from the individual concerned – see the grounds of refusal including evaluative material in the *Privacy Act 2020 (New Zealand Legislation website)* and *section 2.5 "Use and Disclosure"*).

When supplying information via telephone, email or text messages, the receiver of the information should be verified as per *section 4.5 "Record Keeping".*

6. Email

6.1. Email Management and Handling of Personal Information to Prevent Breaches

With regard to email, members of the University should refer to the *IT Policy Framework (PDF, 138KB)* and the following:

- Email is not guaranteed to be a secure or private form of communication. Unauthorised people may read emails by a variety of methods, for example, through reading the contents of an unattended screen, through maintenance of the Exchange server or desktop, through incorrect addressing, forwarding, or through hacking.
- Emails sent or received by a University staff member might be subject to requests for access under the *Official Information Act 1982 (New Zealand*

Legislation website) and the *Privacy Act 2020 (New Zealand Legislation website).*

- Personal information is not sent by email, unless by careful consideration it is deemed reasonable to send the personal information by email.
- Sensitive personal information (refer *to section 5*) is not sent by email, unless in all the circumstances, it is reasonable to send sensitive personal information by email. If an email containing sensitive personal information is sent, a 'test email' should be sent first and the intended recipient should be identified either by phone or by an appropriate identifier in a return email. The message or an attachment to the email may also be encrypted using a password which has been given to the intended recipient by phone or other secure and independent means.
- When sending emails, care must be taken not to send (or 'Cc' or 'Bcc') to other individuals who do not require the information.
- Where possible, attachments sent with an email message are opened on the email message prior to sending, to review and confirm whether the correct file has been attached.
- University staff members should check email folders regularly (but at least annually) to ensure there is no personal information which should be deleted, or captured/migrated for inclusion on an electronic file or in an electronic system, or printed for inclusion on a physical file. Personal information should only be retained if it is needed for the purposes of University business, including audit and retention requirements.
- No one should forward any personal information contained in an email to a third party, without the author's permission.

6.2. Legal Disclaimer on Emails

The use of email disclaimers is required as a protection against legal threats in instances such as breach of confidentiality (accidental or otherwise), transmission of viruses, negligent misstatement, and employer liability.

This policy mandates the use of a standard email disclaimer. This disclaimer is applied to all outgoing emails from the University.

6.2.1. Email Disclaimer Appended to all Outgoing Emails from the University

The following information must be attached at the end of each outgoing email from all University email accounts:

"This email may be confidential and subject to legal privilege, it may not reflect the views of the University of Canterbury, and it is not guaranteed to be virus free. If you are not an intended recipient, please notify the sender immediately and erase all copies of the message and any attachments."

IT Services shall append this disclaimer to all University staff emails leaving the campus network.

The full text of the disclaimer available at the above URL is *also in Appendix B* of this document. For further information on best practice for email etiquette refer to *Email Management at UC (University Information and Records Management web pages)*.

7. Responsibility for Compliance

7.1. Compliance with the Policy

All University community members are responsible for compliance with this document. To assist with compliance, the University has appointed a **University Privacy Officer** (see *contact details* below).

All of the Senior Management Team must encourage compliance with this document and put in place systems/procedures to facilitate compliance, including nominating a member from their portfolio for the Information Management Network (refer to *section 7.2: "Information Management Network"*).

The University undertakes at least one Information Network meeting relating to privacy issues per year (notification of which is given at least two weeks in advance), chaired by the University Privacy Officer or his/her delegate. The University Privacy Officer (or approved delegate) maintains a regularly updated web page and uses other formats as required.

7.2. Information Management Network

Each portfolio and college delegates first-line responsibility for privacy issues to a Privacy Nominee. Collectively, this group of nominees is known as the Information Management Network, which covers further information management support beyond privacy and is supported by the **University Privacy Officer** with training, awareness raising and investigations by staff from the Information and Records Management Office *(further information in section 8 "The Role of the University Privacy Officer"*). Membership of the Information Management Network is voluntary and is in addition to the normal duties and requirements of each member.

The Information Management Network will

- provide first line support for staff and students from each college or SMT member's portfolio on privacy issues or concerns, in particular, by providing advice and guidance and in answering basic queries;
- where necessary, escalate matters of concern to the University Privacy Officer or the *University Information and Records Manager* as appropriate;

- provide support to respective Senior Management Team members on privacy issues affecting their portfolios/colleges, and act as a resource for use in projects that will affect privacy matters; and
- meet on a regular basis to share experience, gain knowledge and take advice from the University Privacy Officer.

8. The Role of the University Privacy Officer

The University Privacy Officer is a role mandated by the *Privacy Act 2020 (New Zealand Legislation website).* At the University, the General Counsel | Registrar is the **University Privacy Officer**. The University Privacy Officer encourages compliance with the IPPs within the University, deals with requests under the *Privacy Act 2020 (New Zealand Legislation website)* and in the case of any complaints or investigations, works alongside the Privacy Commissioner.

While the Privacy Nominee (*refer to section 7.2: "Information Management Network"*) is available to answer any privacy-related queries, any matter not covered by this document should be referred to the *University Privacy Officer.*

Related Documents and Information

Legislation

- Crimes Act 1961 (New Zealand Legislation website)
- Human Rights Act 1993 (New Zealand Legislation website)
- Official Information Act 1982 (New Zealand Legislation website)
- Privacy Act 2020 (New Zealand Legislation website)
- Public Records Act 2005 (New Zealand Legislation website)

UC Policy Library

- Intellectual Property Policy (PDF, 534KB)
- IT Policy Framework (PDF, 212KB)
- Official Information Policy (PDF, 204KB)
- Risk Management and Compliance Framework (PDF, 797KB)
- Student Community Online Survey Policy (PDF, 300KB)

UC Website and Intranet

- Email Management at UC (University Information and Records Management web pages)

- General Disposal Authority for New Zealand Universities DA337 (University Information and Records Management web page)
- Records Disposal Framework (University Information and Records Management web pages)
- Special Consideration Regulations (University Regulations web page)
- UC Privacy Statements (University Privacy Statements web page)
- University Regulations (University Regulations web page)

External

- Health Information Privacy Code 1994 (Office of the Privacy Commissioner NZ website)
- Office 365 Trust Centre (Microsoft Office website)
- Office of the Ombudsman (Office of the Ombudsman website)
- Office of the Privacy Commissioner (Office of the Privacy Commissioner website)
- Tuariki REANNZ (REANNZ website)

Contact details

For further information on this document or any privacy-related matters, contact:

The University Privacy Officer (General Counsel | Registrar)
University of Canterbury
Private Bag 4800
Christchurch
New Zealand
Ph: +64 3 366 7001
Fax: +64 3 364 2174

The University Information and Records Manager (University Information and Records Manager).

Appendices

- Appendix A: Consent Template
- Appendix B: Entire Text of University Email Disclaimer

Document History and Version Control Table			
Version	**Action**	**Approval Authority**	**Action Date**
For document history and versioning prior to 2013 contact ucpolicy@canterbury.ac.nz			
1.00	• Major review of document and conversion into new template.	Vice-Chancellor	Oct 2013

	• Combined University *Legal Disclaimer on Email Policy* into this document. • Updated Hyperlinks.		
1.01	Review date pushed out to reflect wider changes.	Policy Unit	July 2015
1.02	Minor formatting changes.	Policy Unit	Aug 2015
2.00	Scheduled review by Contact Officer – minor changes including Contact Officer and Approval Authority.	Policy Unit	Nov 2015
2.01	"Faculty" references changed to "College" to reflect College-Faculty merger.	Policy Unit	June 2016
2.02	Unscheduled review, additional clauses added to reflect student first technology changes, hyperlinks updated or added.	Policy Unit	Dec 2017
3.00	Scheduled review, minor changes to content layout and introduction	Policy Unit	April 2019
3.01	Change to review date in anticipation of legislative amendments.	Policy Unit	March 2020
3.02	Scheduled review pushed out for 6mths	Policy Unit	May 2021

Appendix A

Consent Template

Note: If the form is electronic and cannot be signed as per the below example, either include a check box or state 'that by submitting this form I agree to…'

Template:

In submitting this form [or insert other, such as 'responding to this survey' etc.] I agree to my details being used for the purposes of [insert reason for data collection, e.g. administering/managing the conference/evaluating programme]. The information will only be accessed by necessary University staff. I understand my data will be held securely and will not be distributed to third parties. I have a right to change or access my information. I understand that when this information is no longer required for this purpose, official University procedure will be followed to dispose of my data.

I understand that the information is held by [insert department/school/contact person/s]…… University of Canterbury, Christchurch and that I have the right to access and correct my personal information.

……..

(name of individual)

……..

(date)

Appendix B

Entire Text of University Email Disclaimer

All email sent from the University of Canterbury may be confidential and subject to legal privilege. If you are not an intended recipient, you may not use, disseminate, distribute or reproduce such email, any attachments, or any part thereof. If you have received a message in error please notify the sender immediately and erase all copies of the message and any attachments. Any views expressed in any message are those of the individual sender and may not necessarily reflect the views of the University of Canterbury.

The University of Canterbury does not guarantee that any email or any attachments are free from computer viruses or other conditions which may damage or interfere with recipient data, hardware or software. The recipient relies on its own procedures and assumes all risk of use and of opening any attachments.