PERSONAL INFORMATION PROCEDURES

1. Purpose

These Procedures are designed to implement the Privacy Policy.

2. Scope

These Procedures apply to all Employees.

3. Definitions

Employee: means a person who is employed or has been employed by the University. Evaluative Material: means any material that is compiled solely for the purposes of determining eligibility for appointment, promotion, continuance in employment or removal from employment.

Personal File: is a file containing documentation relating to an Employee or Student. Privacy Officer: means the person appointed by the University pursuant to the Privacy Act 2020.

Student: means a person who has applied to enrol, or a person who is enrolled at the University

4. Actions

A. Collection of Personal Information – Privacy Principles 1 - 4

The University must not collect Personal Information unless:

- The information is collected for lawful purposes connected with a function or activity of the University; and
- The collection of the information is necessary for that purpose.

When the University collects Personal Information, it must collect it directly from the individual concerned unless one of the exceptions set out in Information Privacy Principle 2(2) applies (see schedule 1).

The University will hold Student Personal File on its Student management Systems that includes:

a) Information on the Student's:
   - Name and address;
   - Date of birth;
   - Identification number, if any, assigned by the University;
   - Course of study and the fees;
   - Changes to their course of study, if any;
   - Citizenship or residency status in New Zealand
   - The progress of the student (including the results achieved) in the course of study.
   - Particulars of any allowances, grants or other payments.
   - Any other information required to assist the University to fulfil its obligations to provide statistical information.
   - Any such other information relating to the Student as may be reasonably required by the University.

When the University collects personal information directly from the individual concerned it must comply with Information Privacy Principles 3 and 4.

B. Security and Storage – Principle 5

The University will hold Employee Personal Information in a personal file(s), the Staff Services Information System and Payroll. Some personal information will be stored in systems that provide access to University resources.

The Employee personal file(s) will be retained for 6 years after the Employee ceases employment. After 6 years the personal file(s) will be destroyed unless there is a good reason why the files should not be.

The University will hold student personal information permanently in ARION. Student information held in other University databases will only be retained as long as necessary for the purposes the information was originally obtained.

C. Access to Personal Information – Principle 6

Any Employee or Student may request access to Personal Information held by the University other than Evaluative Material and other material that is subject to exception under the Information Privacy Principles in the Privacy Act 2020.

If such a request is made then the University will provide the person making the request with access to that information, either by providing a copy or allowing viewing of the Personal Information, within a reasonable time.

Accuracy and Correction of Personal Information – Principles 7 and 8

Anyone is entitled to request correction of their own Personal Information other than Evaluative Material and other material that is subject to exception under the Information Privacy Principles in the Privacy Act 2020.

Where such a request is made the University must decide whether or not to correct the Personal Information.

If the University decides not to correct the Personal Information then it will inform the person of their right to have their request and the University's refusal noted on the personal file.

If the University corrects personal information or attaches a statement of correction to personal information, the University must so far as reasonably practicable inform every other person to whom has been disclosed to the information by the University.

D. Requests for Personal Information

The University will respond to a request for Personal Information within 20 working days of the request (section 44 of the Privacy Act 2020) or longer period (section 48 of the Privacy Act 2020) where:

- Consultation is necessary before a decision can be made to provide access to the Personal Information; or
- The request involves a large quantity of information and complying with the initial time period would place undue stress on the operations of the University.
- The processing of the request raises issues of such complexity that a response to the request cannot reasonably be given within the original time limit.

The University may withhold access to Personal Information pursuant to the Privacy Act 2020 and the Official Information Act 1982 if allowing access would:

- Endanger the safety of the individual;
- Create a significant likelihood of serious harassment of the individual
- Involve unwarranted disclosure of the affairs of another individual; or breach legal professional privilege.

Access may also be withheld if:

- The request is frivolous or vexatious, or where the information requested is trivial;
- The information requested is not readily retrievable; or
- The information requested does not exist or cannot be found.

Evaluative material may be withheld if disclosure would breach an express or implied promise of confidentiality to the person who supplied the material.

The University will not disclose Personal information that it holds about any individual to any person, body or agency unless one of the exceptions in Principle 11 of the Information Privacy Principles applies.

E. Retention Periods – Principle 9

Personal Information will not be held longer than six years after the Employee has ceased employment except for:

- Records of prior service;
- Tax records; and
- Disciplinary records.

Personal Information will be held by the University for six years after the Employee has ceased employment.

5. Responsibilities

Privacy Officers are responsible for ensuring that the University's obligations under the Privacy Act 2020 are met and for liaising with the Privacy Commissioner to develop the policy, procedures and protocols related to Personal Information.

Employees who are provided with Personal Information must comply with the Privacy Policy and these Procedures.

6. Mandatory Reporting Requirements

All suspected privacy breaches are to be directed to a Privacy Officer: Group Director – People & Culture (for staff) and the Group Director – Student Services & Administration (for students).

In circumstances where the University identifies that the breach has or is likely to cause serious harm, the Privacy Commissioner and affected individuals must be notified. Failure to notify the Commissioner of a notifiable breach risk penalties for the University of up to $10,000.

7. Compliance Notice

The Privacy Commissioner can issue a compliance notice where he considers that one or both of the following may have occurred:

- A breach of the Privacy Act, including, interference with the privacy of the individual
- An action that is to be treated as a breach of an information privacy principle (IPP) or an interference with the privacy of an individual under the Act.

Before issuing a compliance notice, the Commissioner will provide the University a reasonable opportunity

to comment on a written notice that describes the breach and the remedial steps the Commissioner considers are needed.

Should the University wish to appeal the notice, they must do so within 15 days of the notice being issued.

The compliance notices will describe the steps that the Commissioner considers are required to remedy non-compliance with the Act and will specify the date by which the University must make the necessary changes.

Failure to comply with the notice within the specified timeframe can result in fines of up to $10,000 as well as details of the breach being publicised.

8. Criminal Offences

It is an offence to mislead an agency to access someone's else's personal information - for example, impersonating someone in order to access information that you are not entitled to see.

It is also an offense for the University to destroy personal information, knowing that a request has been made to access it. The penalty for these offences is a fine of up to $10,000.

9. Policy Base

Privacy Policy

10. Associated Documents

Schedule 1 – Principles of the Privacy Act 2020

Discipline Policy

Official Information Policy and associated procedures

Note: Policies and Procedures can be found on AUTi.

11. Forms/Record Keeping

12. Implementation

These procedures will be implemented once they appear on the Policies and Procedures webpage.

13. Document and Management Control

Reviewed on: 1 September 2020
Due for Review on: 1 September 2020

SCHEDULE 1

PRINCIPLES OF THE PRIVACY ACT 2020

Principle 1: Purpose of collection of personal information

Personal information may only be collected for a lawful purpose. That purpose must be connected with an organisation's functions or activities, and collection of the information must be necessary for that purpose.

Principle 2: Source of Personal Information

Personal Information must be collected directly from the individual to whom the information relates. There are several exceptions to this principle that are set out in section 22 of the Privacy Act 2020. The exceptions that might be most relevant are where the collector believes, on reasonable grounds, that:

- The information is publicly available;
- Collecting the information from the individual directly is not reasonably practical;
- The information will not be used in a way that would directly identify the individual to whom the information relates;
- Collecting the information from the individual directly would prejudice the purposes of the collection;
- The individual has authorised the collection of the information from another source;
- Collecting the information from another source would not prejudice the interests of the individual to whom the information relates.
- Collection of the data would pose a serious threat to the life or health of the individual concerned or any individual
- To avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences.

Principle 3: Collection of information from the individual

When collecting information directly from an individual, the collector must ensure that the individual is aware of:

- The fact the information is being collected;
- The purpose for which it is collected;
- The intended recipients;
- The fact that the individual has a right of access to and a right to request correction of that information
- The consequences for the individual if all or part of the information is not provided.

Principle 4: Manner of collection

Personal Information must not be collected unlawfully or in a way that is unfair in the circumstances or which intrudes unreasonably on personal privacy.

Principle 5: Storage and security

The employer must ensure that any Personal Information that it holds is protected against loss and unauthorised access, use, modification or disclosure.

Principle 6: Access

An individual is entitled to receive confirmation of whether the employer holds personal information and to access that information if it is readily retrievable.

The Privacy Commissioner will be able to direct the University to provide individuals access to their personal information. Access directions will be enforceable in the Human Rights Tribunal.

Principle 7: Correction

An individual may request a correction of Personal Information held by the employer. The employer must respond to this request. If the employer refuses to correct the information and, if the individual requests, the employer must attach to the information a statement noting that a correction has been sought but not made. Where such a statement is attached, the employer must inform all parties to whom the information has been disclosed (as far as practicable) of the existence of this statement and must then notify the individual of the steps taken to do this.

Principle 8: Accuracy to be checked before use

The employer may not use information without taking reasonable steps to ensure that the information is up to date, complete, relevant and not misleading.

Principle 9: Retention

Personal Information must not be kept longer than necessary for the purposes for which it may lawfully be used.

Principle 10: Limits on use

Information that is obtained for one purpose may not be used for another purpose. There are several exceptions to this. The most relevant exceptions are where an employer believes on reasonable grounds that:

- The source of the information is publicly available;
- The use for the other purpose has been authorised by the individual to whom the information relates;
- The purpose is directly related to the purpose of collection;
- The information will be used in a form in which the individual is not identified.

Principle 11: Limits on disclosure

The employer must not disclose Personal Information to a third party. The most relevant exceptions are where the employer believes, on reasonable grounds, that:

- The individual has authorised the disclosure;
- The information will be disclosed in a form in which the individual is not identified.
- The information is publicly available and that in circumstances of the case, it would not be unfair or unreasonable to disclose the information.

Principle 12: Disclosing Information Overseas

The University may only disclose personal information to an agency outside of New Zealand if the receiving agency is subject to similar safeguards to those in the Privacy Act.

If a Jurisdiction does not offer similar protections, the individual concerned must be fully informed that their information may not be adequately protected and they must expressly authorise the disclosure.

Principle 13: Unique identifiers

The employer may not assign a unique identifier to an individual unless this is necessary to enable the employer to carry out its functions efficiently.