Personal Information and Privacy Policy

Responsibility for policy: Chief Operating Officer (Privacy Officer)
Approving authority: Vice-Chancellor
Last reviewed: June 2026
Next review date: June 2031

Application

1. This policy applies to all staff of the University of Waikato.

Purpose

2. The purpose of this policy is to set out the obligations and responsibilities of staff with respect to the collection, protection, access, use, storage, retention, disclosure, sharing and management of personal information governed by and in accordance with:
   - the Education and Training Act 2020
   - the Official Information Act 1982
   - the Privacy Act 2020
   - the Public Records Act 2005
   - the University of Waikato Privacy Statement and
   - where applicable, the European Union General Data Protection Regulation (GDPR).
3. This policy also establishes the requirements for responding to and reporting a privacy breach to the University's Privacy Officer and the Office of the Privacy Commissioner, where required.

Related documents

4. The following documents set out further information relevant to this policy:
   - Ethical Conduct in Human Research and Related Activities Regulations
   - Information and Records Management Policy
   - Office of the Privacy Commissioner website
   - Privacy Breach Procedures
   - Staff Code of Conduct

Definitions

5. In this policy:
   personal information means information about an identifiable individual
   privacy breach means any unauthorised or accidental access to, disclosure, alteration, loss, destruction or issue of personal information as defined in the Privacy Act 2020
   Privacy Officer means the staff member appointed by the University to carry out the functions of a Privacy Officer in accordance with the Privacy Act 2020.

Responsibilities

6. Staff who collect, update, use, store, disclose or share personal information must adhere to the Privacy Principles set out in the Privacy Act 2020; a brief summary of the principles is provided in the Appendix to this policy.

7. Where the University processes personal data that is subject to the European Union General Data Protection Regulation (GDPR), staff must comply with any additional obligations arising under that regulation.
8. Staff may only access personal information for a lawful University purpose and on a demonstrably need-to-know basis.
9. Staff who are undertaking or supervising research must also, where applicable, comply with the regulations relating to the archiving of data and the privacy, storage and use of personal information contained in the University's Ethical Conduct in Human Research and Related Activities Regulations.
10. Staff must take reasonable steps to protect personal information against loss, unauthorised access, modification, disclosure or other misuse.
11. Staff must ensure that personal information is retained, archived and securely disposed of in accordance with:
    - the Public Records Act 2005
    - the Information and Records Management Policy, and
    - any other applicable records retention and disposal requirements.
12. Staff must ensure that the use of emerging technologies, including artificial intelligence (AI) systems, automated decision-making tools and biometric technologies involving personal information is undertaken in accordance with applicable law, University policy and relevant ethical standards.
13. Staff must immediately report any actual or suspected privacy breach to the Privacy Officer in accordance with the University's Privacy Breach Procedures; the Privacy Officer will determine whether a privacy breach must be reported to the Office of the Privacy Commissioner in accordance with mandatory reporting requirements.
14. Line managers are responsible for ensuring that all systems, processes and practices in the areas for which they are responsible conform with this policy.
15. Any questions by staff or students about the interpretation of, or compliance with, this policy must be referred to the Privacy Officer.
16. Requests for personal information and complaints of interference with privacy by staff or students must be referred to the Privacy Officer.
17. The Privacy Officer is responsible for:
    - ensuring that the University complies with the provisions of the Privacy Act 2020
    - dealing with requests and complaints made under the Privacy Act 2020, and
    - working with the Office of the Privacy Commissioner in relation to reporting and investigations conducted under the Privacy Act 2020.

Responsibility for monitoring compliance

18. The Privacy Officer is responsible for monitoring compliance with this policy and reporting any breaches to the Vice-Chancellor, external agencies and affected individuals (where appropriate).
19. Breaches of this policy may result in disciplinary action under the Staff Code of Conduct.

A quick tour of the privacy principles

The Privacy Act 2020 has a set of privacy principles that govern how you should collect, handle and use personal information.

1 You can only collect personal information if it is for a lawful purpose and the information is necessary for that purpose. You should not require identifying information if it is not necessary for your purpose.

2 You should generally collect personal information directly from the person it is about. Because that won't always be possible, you can collect it from other people in certain situations. For instance, if:

- the person concerned gives you permission
- collecting it in another way would not prejudice the person's interests
- collecting the information from the person directly would undermine the purpose of collection
- you are getting it from a publicly available source.

3 When you collect personal information directly from the individual, you must take reasonable steps to make sure that the person knows:

- why it's being collected
- who will receive it
- whether giving it is compulsory or voluntary
- what will happen if they don't give you the information.

Sometimes there may be good reasons for not letting a person know you are collecting their information – for example, if it would undermine the purpose of the collection, or if it's just not possible to tell them.

3A When you collect personal information from a source other than the individual themself, you also need to let them know:

- that the information has been collected
- why it was collected
- who will receive it
- the name and address of the agency that is collecting information and the agency that holds the information.
- if the collection is authorised or required by law, which particular law that is.
- their right to access and correct their information.

4 You may only collect personal information in ways that are lawful, fair and not unreasonably intrusive. Take particular care when collecting personal information from children and young people.

5 You must make sure that there are reasonable security safeguards in place to prevent loss, misuse or disclosure of personal information. This includes limits on employee browsing of other people's information.

6 People have a right to ask you for access to their personal information. In most cases you have to promptly give them their information. Sometimes you may have good reasons to refuse access. For example, if releasing the information could:

- endanger someone's safety
- create a significant likelihood of serious harassment
- prevent the detection or investigation of a crime
- breach someone else's privacy.

7 A person has a right to ask an organisation or business to correct their information if they think it is wrong. Even if you don't agree that it needs correcting, you must take reasonable steps to attach a statement of correction to the information to show the person's view.

8 Before using or disclosing personal information, you must take reasonable steps to check it is accurate, complete, relevant, up to date and not misleading.

9 You must not keep personal information for longer than is necessary.

10 You can generally only use personal information for the purpose you collected it. You may use it in ways that are directly related to the original purpose, or you may use it another way if the person gives you permission, or in other limited circumstances.

11 You may only disclose personal information in limited circumstances. For example, if:

- disclosure is one of the purposes for which you got the information
- the person concerned authorised the disclosure
- the information will be used in an anonymous way
- disclosure is necessary to avoid endangering someone's health or safety
- disclosure is necessary to avoid a prejudice to the maintenance of the law

12 You can only send personal information to someone overseas if the information will be adequately protected. For example:

- the receiving person is subject to the New Zealand Privacy Act because they do business in New Zealand
- the information is going to a place with comparable privacy safeguards to New Zealand
- the receiving person has agreed to adequately protect the information – through model contract clauses, etc.

If there aren't adequate protections in place, you can only send personal information overseas if the individual concerned gives you express permission, unless the purpose is to uphold or enforce the law or to avoid endangering someone's health or safety.

13 A unique identifier is a number or code that identifies a person in your dealings with them, such as an IRD or driver's licence number. You can only assign your own unique identifier to individuals where it is necessary for operational functions. Generally, you may not assign the same identifier as used by another organisation. If you assign a unique identifier to people, you must make sure that the risk of misuse (such as identity theft) is minimised.

Content updated April 2026. Design updated April 2026.