

# Privacy Procedure

## Section 1 - Summary

(1) See [Privacy Policy](#).

## Section 2 - Scope

(2) See [Privacy Policy](#).

## Section 3 - Definitions

(3) See [Privacy Policy](#).

## Section 4 - Policy / Regulation

(4) This Procedure supports the [Privacy Policy](#).

## Section 5 - Procedures

(5) VU staff, students and agents operating on VU's behalf, are expected to comply with the University's [Privacy Policy](#) and relevant privacy legislation including the Information Privacy Principles (IPPs) and the [Health Privacy Principles \(HPPs\)](#). The IPPs and HPPs are contained in schedules to the [Privacy and Data Protection Act 2014 \(Vic\)](#), and the [Health Records Act 2001 \(Vic\)](#).

(6) This procedure is intended to assist with compliance and is not a substitute for Victorian privacy legislation. Where individuals are in any doubt about their privacy obligations, they should refer to the IPPs (or HPPs as appropriate) and/or seek advice from the University's [Privacy Officer](#).

### Part A - Collecting information

(7) When collecting information about an individual, the main rules to remember are:

- a. only collect information if it is needed (i.e. only collect information if it is necessary for one or more of VU's functions and activities);
- b. Wherever possible, collect the information directly from the individual concerned;
- c. ensure that the information is collected lawfully, securely and fairly;
- d. ensure the collection is not unreasonably intrusive; and
- e. tell people that their information is being collected, why it is being collected and how it is to be used.

## Privacy statements

(8) Before or at the time of collecting information, individuals must take reasonable steps to ensure that the person who is providing the information is aware of the following:

- a. the identity of the organisation collecting the information (e.g. VU or a particular division of VU) and how it can be contacted;
- b. The purpose(s) for which the information is being collected (e.g. student enrolment, research, marketing etc.);
- c. How the information being collected will generally be used and to whom it is usually disclosed;
- d. The fact that the individual is able to gain access to the information;
- e. Whether the collection of the information is required by law;
- f. Any consequences of not providing the information (e.g. VU may not be able to provide a particular service); and
- g. The fact that the University has a [Privacy Policy](#), which is available on the VU website, and a [Privacy Officer](#) who can be contacted with queries or concerns.

(9) VU has the following overarching privacy statements:

- a. The Student Privacy Statement (see [Appendix 1](#) to the [Privacy Policy](#));
- b. The Staff Privacy Statement (see [Appendix 2](#) to the [Privacy Policy](#)); and
- c. The privacy collection disclaimer noted on student enrolment forms.

(10) If the information to be collected is not covered by one of the above privacy statements, a specific privacy collection statement must be drafted, containing the information described in paragraph 8 above.

## Collecting information for research purposes

(11) Researchers are also required to get ethics approval prior to collecting information in accordance with appropriate Research Policies, such as the [Research Integrity Policy](#).

## Collecting information from third parties

(12) If information about an individual is to be collected from someone other than that individual (for example another institution or a parent), VU must have the individual's written permission.

(13) In certain exceptional circumstances, a formal authority may not be required (e.g. for emergency health reasons).

(14) If information is collected about an individual from someone other than the individual, reasonable steps must be taken to ensure that the individual is made aware of the matters listed in paragraph (8) above.

## Collecting sensitive information

(15) Sensitive information is defined in the [Privacy and Data Protection Act 2014](#) and includes religious, political or sexual preference information. It must only be collected if it is essential for VU's operations. In addition, sensitive information should not be collected unless:

- a. the individual has provided their informed consent;
- b. the collection is required by law;
- c. it is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual; or
- d. it is necessary for the establishment, exercise or defence of a legal or equitable claim.

(16) However, VU may collect sensitive information about an individual if:

- a. the collection:
  - i. is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or
  - ii. is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government-funded targeted welfare or educational services; and
- b. there is no reasonably practicable alternative to collecting the information for that purpose; and
- c. it is impractical for VU to seek the individual's consent to the collection.

## **Collecting health information**

(17) Health information is very broadly defined in the [Health Records Act 2001 \(Vic\)](#) and includes information or an opinion about the physical, mental or psychological health of an individual or a disability or a health service provided to an individual.

(18) The collection of health information is subject to very stringent legislative requirements and it must only be collected if it is essential for VU's operations. Health information should not be collected unless the individual has provided their consent or in accordance with the limited exceptions set out in the [HPP1](#).

## **Anonymity**

(19) Individuals generally have the option of not identifying themselves when dealing with VU.

(20) Such a request should be accommodated wherever lawful and practicable. However, the person should be advised that VU may not be able to provide services to them because the nature of VU's work means that it is generally not possible to provide services to, or interact with, students or staff in an anonymous way.

# **Part B - Using and disclosing information - how to respond to common requests for information**

## **Use and disclosure for the primary purpose**

(21) Generally speaking, an individual's information should only be used or disclosed for the purpose for which it was collected - this is considered the "primary purpose".

## **Use and disclosure for a secondary purpose**

(22) However, VU may use and disclose information for a secondary purpose without first obtaining an individual's consent, if the secondary purpose is:

- a. related to the primary purpose in the case of personal information, or directly related to the primary purpose in the case of sensitive/health information; and
- b. the individual would reasonably expect VU to use or disclose the information for that secondary purpose.

(23) It is important to note that the sensitivity of the information will affect a person's reasonable expectation about an appropriate secondary use/disclosure. For example, if a student provides sensitive information (e.g. information about their religious practices) as part of a request for an extension of time, the student would reasonably expect that the information would only be shared to the extent necessary to facilitate the consideration of their request.

## Use and disclosure of health information

(24) In addition to the above requirements regarding the use and disclosure of sensitive information, the [Health Records Act 2001 \(Vic\)](#) has additional requirements regarding health information. Health information must not be used or disclosed unless in accordance with [HPP2](#).

## Use and disclosure for other purposes

(25) Information may be used and disclosed for a different purpose from that for which it was collected if:

- a. the individual has consented; or
- b. it is reasonably believed that the use or disclosure is necessary to lessen or prevent a serious or imminent threat to an individual's life, health, safety or welfare and/or a serious threat to public health, safety or welfare; or
- c. the use/disclosure is otherwise authorised or required by law.

(26) Unless an individual has consented to the use/disclosure of their information, advice should be sought from a [Privacy Officer](#) before a disclosure is made.

(27) From time to time, and where appropriate, VU may use or disclose information (excluding sensitive or health information) for marketing purposes. Where VU engages in marketing, it will ensure that there are a simple means by which an individual may easily request not to be identified in marketing materials.

## Sending information outside Victoria

(28) Staff and agents sending information outside of Victoria as part of VU's functions and activities (e.g. to an interstate campus, or overseas for its international students) must only do so:

- a. if the recipient is subject to privacy principles for fair handling of information that are substantially similar to Victoria's; or
- b. with the individual's consent, or if it is impracticable to obtain their consent if the transfer is for their benefit and they would be likely to consent if they could; or
- c. if contracting with the individual, or with a third party for the individual's benefit; or
- d. in accordance with the applicable legislation.

(29) The [Health Records Act 2001 \(Vic\)](#) contains additional requirements which VU must comply with when sending health information outside of the jurisdiction. See [HPP9](#) for further information.

## Disclosing information to third parties

(30) If a third party requests information about an individual, they must either have the individual's permission to disclose the information, or a legal right to obtain it.

(31) Any request for information on behalf of an individual must be accompanied by a signed written authority from the individual whose information is to be disclosed. For instance, personal information may not be disclosed to parents or to solicitors acting on behalf of staff or students unless a signed authority has been provided.

(32) In some circumstances in which disclosure of the information is sought, permission will already have been obtained via the University's overarching privacy statements for staff and students.

(33) Requests for information about individuals from law enforcement organisations (e.g. Federal or State Police, Police task forces, etc) must be forwarded to a [Privacy Officer](#) as soon as possible. The [Privacy Officer](#) will consider the

request and, if a disclosure is made, ensure it is recorded in the Disclosures Register as required by law.

(34) Information may be disclosed in certain emergency situations, such as to a hospital. Advice should be obtained from a [Privacy Officer](#) where there is any uncertainty.

(35) Examples of common requests for information, and the standard response in each case are listed below:

- a. Government agencies (e.g. [Department of Home Affairs](#), Ombudsman) - refer to Legal Services.
- b. Services Australia and [Centrelink](#) requests - refer to Legal Services.
- c. Requests from lawyers on behalf of staff or students - refer to Legal Services.
- d. Subpoenas or other court correspondence - refer to Legal Services.

## **Disclosing student personal information to parents**

(36) The [Privacy and Data Protection Act 2014 \(Vic\)](#), does not specify a particular age at which a person's privacy rights come into effect. The general principle is that a child or young person may exercise their rights under the Act independently of a parent or guardian if they have sufficient understanding and intelligence to give valid consent or to make their own decisions. Generally speaking, the University will consider that its students are sufficiently mature and intelligent to make their own decisions in relation to the distribution of their personal information, even if that student is less than 18 years of age.

(37) Student personal information should not be provided to parents or to other family members in the absence of the express consent of the student.

(38) There may be exceptions to this rule — for example, if a student has an intellectual disability or is subject to a Guardianship Order. Any queries should be referred to Legal Services.

## **Use of Unique Identifiers**

(39) VU will not assign unique identifiers unless it is necessary to carry out its functions efficiently. Staff and student identification numbers are considered necessary for this reason.

(40) VU will not adopt as its own a unique identifier assigned to an individual by another organisation (eg. tax file number, driver's licence number).

(41) The University's use or disclosure of a unique identifier assigned to an individual by another organisation will be in accordance with [IPP 7](#) or other applicable legislation.

# **Part C - Accessing and correcting information**

## **Requests by individuals for access to their own information**

(42) Wherever possible VU will let people see their own information in the simplest way possible.

(43) Whenever VU receives a request from a student or staff member to access or obtain their own information, the identity of the individual should be verified before any information is provided.

(44) In most cases, an individual's request for information about themselves will be able to be provided to them directly by the relevant business area:

- a. Students wishing to access their own personal information should contact the [Student Contact Centre](#) in the first instance via:
  - i. Phone: +61 3 9919 6100; or

- ii. Online: ask a question or search for answers on [ASKVU](#) (external link).
- b. Staff wishing to access their own personnel files should:
  - i. apply in writing to the Director, People & Culture Business Services via:
    - (45) Email: [PC.Queries@VU.edu.au](mailto:PC.Queries@VU.edu.au)
    - (46) Mail: Director, People & Culture Business Services, Victoria University, Footscray Park Campus, PO Box 14428, Melbourne City Mail Centre, MELBOURNE VIC 8001; or
  - ii. arrange an inspection of personal information, under the supervision of a staff member from People and Culture.

(47) Where a request for access is denied, reasons must be provided.

(48) However, there may be occasions where a request from an individual will need to be carefully considered before a determination can be made about whether the information can be disclosed. For instance, information may not be able to be disclosed where the information was given in confidence, or where disclosure may have an unreasonable impact on another person's privacy. If a request for information about an individual is not straightforward, it may need to be considered in the context of a formal [Freedom of Information Act 1982 \(Vic\)](#) (FOI) application.

(49) For advice about whether a request for information should be submitted as an FOI application, contact a [Privacy Officer](#).

(50) Further information about the FOI process can be found on the [FOI webpage](#).

## **Correcting information**

(51) If VU holds information about an individual, staff must take reasonable steps to correct the information where an individual is able to satisfactorily demonstrate that it is inaccurate.

(52) If an individual and VU disagree about whether their information is inaccurate, the individual may request that VU associate with the information a statement setting out that the individual believes the information to be inaccurate. VU must take reasonable steps to accommodate such a request.

(53) Where a request for a correction is denied, reasons must be provided.

## **Correcting health information**

(54) The [Health Records Act 2001 \(Vic\)](#) contains additional requirements which VU must comply with when correcting health information. See [HPP6](#) for further information.

## **Part D - Maintaining data quality**

(55) All VU business units must take reasonable steps to ensure that the information they hold is accurate, complete, and up-to-date.

(56) Maintaining data quality is everyone's responsibility and staff and students are expected to provide VU with accurate and up-to-date information and to inform VU of any changes to their personal information (for example by regularly checking and updating information held on staff and student portals).

## **Part E - Securing, storing and retaining data**

(57) VU stores information using electronic and hardcopy record systems. All staff and each operational area must

take reasonable steps to ensure that:

- a. information is protected from misuse, loss, unauthorised access or modification, or improper disclosure;
- b. practices, procedures and systems (including electronic and physical) are in place to ensure that the information is stored (and if necessary moved) safely and securely;
- c. the information has not been changed or been tampered with;
- d. all records containing personal, sensitive and health information are kept in a secure location and cannot be accessed by unauthorised persons;
- e. Authentication processes (for identification) are adhered to, in that a person accessing or providing information are who they claim to be; and
- f. Requirements around retention of information are complied with, according to the [Records Management Policy](#), [IT policies](#), and related procedures.

## Managing records

(58) Operational areas at VU must ensure that records are retained in a way that is consistent with the following:

- a. [Records Management Policy](#);
- b. [Physical Records Storage Procedure](#);
- c. [Disposal of Records Procedure](#);
- d. [Access to Records Procedure](#); and
- e. [Security of Records Procedure](#)

(59) Records Services are also available to provide advice and guidance on matters involving records management. They may be contacted at:

- a. Records and Archives Services, Victoria University, PO Box 14428, MELBOURNE VIC 8001
- b. Telephone: 9919-5093
- c. Email: [records@vu.edu.au](mailto:records@vu.edu.au)

## Development of IT systems

(60) VU's information technology department maintains hardware, systems and security procedures in line with IT policies and procedures.

(61) If staff or any operational area of the University is seeking to develop or implement new IT systems which are likely to involve the collection, storage and/or disclosure of individuals' information, they must ensure their system is compliant with the relevant VU IT and Records Management requirements.

(62) At the planning stage of such systems or projects, consideration should be given to whether a [Privacy Impact Assessment \(PIA\)](#) should be prepared. A PIA is a detailed consideration of the potential privacy impact and risk posed by a project or initiative. The purpose of a PIA is to assess whether it is safe to proceed to the implementation stage of a project, in light of VU's privacy obligations.

## Projects handling information

(63) Where staff or any operational area of the University are seeking to develop or implement new projects which are likely to involve the collection, storage and/or disclosure of individuals' information, at the planning stage of such projects, consideration should be given to whether a PIA should be prepared.

## Part F - Disposing of and destroying information

(64) VU will take reasonable steps to destroy or permanently de-identify information which is no longer required for any purpose in accordance with:

- a. the [Public Records Act 1973 \(Vic\)](#);
- b. the [Health Records Act 2001 \(Vic\)](#); and
- c. the [Records Management Policy](#), and all related Procedures including the [Records Disposal Procedure](#), and upon consultation with Records Services.

(65) No one at VU should destroy the information unless they are confident they are permitted to do so. Staff should consult with Records Services if they are unsure about destroying any information.

## Part G - Privacy Support

### University Privacy Officer

(66) VU has a [Privacy Officer](#) who carry out the following functions:

- a. oversee and monitor compliance with the [Privacy Policy](#) and this Procedure;
- b. support relevant operational areas in the management of any complaints arising under the [Privacy Policy](#), this Procedure or the related legislation;
- c. maintain a Disclosures Register;
- d. conduct an ongoing review of VU's practices and processes to ensure that they are compliant with the relevant legislation, policy and best practice;
- e. educate, train and assist University staff on their responsibilities under the [Privacy Policy](#) and this Procedure; and
- f. address privacy queries or concerns.

### Queries or concerns about privacy

(67) VU strives for continuous improvement and if anyone has a query or concern about privacy, they can contact a Privacy Officer at [privacy.officer@vu.edu.au](mailto:privacy.officer@vu.edu.au).

(68) The [Privacy Officer](#) may refer to complaints from staff to the [Staff Complaint Resolution Policy](#) or, in the case of students, the [Student Complaints Policy](#).

(69) For complaints from outside VU, the [Privacy Officer](#) will generally refer to the [Public Complaints Policy](#) to seek resolution of the matter.

## Section 6 - Guidelines

(70) Operational areas within VU may develop guidelines tailoring the requirements under this Procedure to suit their business needs.

(71) [Appendix 1](#) to the [Privacy Policy](#) is the Privacy Statement for the collection of student information.

(72) [Appendix 2](#) to the [Privacy Policy](#) is the Privacy Statement for the collection of staff information.



## Status and Details

<b>Status</b>	Historic
<b>Effective Date</b>	24th June 2019
<b>Review Date</b>	24th June 2022
<b>Approval Authority</b>	Vice-Chancellor
<b>Approval Date</b>	24th June 2019
<b>Expiry Date</b>	17th July 2024
<b>Accountable Officer</b>	Trish Roberts Deputy Chief Financial Officer trish.roberts@vu.edu.au
<b>Responsible Officer</b>	Lisa Filippin General Counsel lisa.filippin@vu.edu.au
<b>Enquiries Contact</b>	Lisa Filippin General Counsel lisa.filippin@vu.edu.au