Swinburne University of Technology- Privacy Guidelines

Part 1. Summary

1. These Guidelines outline Swinburne's privacy practices and its management of personal, sensitive and health information.
2. Supplementary information is contained in the University's Privacy Procedures which provide additional guidance on the University's privacy practices.

Part 2. Scope

3. These Guideline apply University wide, excluding Sarawak Campus.

Part 3. Overview

4. Swinburne is committed to ensuring compliance with –
    a. the Privacy and Data Protection Act 2014 (Vic) and Health Records Act 2001 (Vic) along with the Privacy Principles in each Act (IPP's and HPP's); and
    b. the Privacy Act 1988 (Cth) and Privacy Principles (APP's), where legally required.

Part 4. Guidelines

Responsibilities

5. All individuals who interact or engage with Swinburne have an obligation to ensure personal, sensitive and health information is collected, accessed, used and disclosed in accordance with these guidelines and relevant privacy collection notices.
6. All staff are required to undertake privacy training upon induction and refresher training every two years, or as directed by the Privacy Officer.
7. Heads of Management Units are required to ensure that Privacy Principles and practices are implemented locally, that all staff have completed the relevant privacy training and ensure that suspected or actual breaches of these Guidelines are managed in accordance with the Data Breach Response Plan.
8. The Privacy Officer is responsible for:
    a. Establishing guidelines for the collection, use, storage, security and disclosure of personal information, sensitive information and health records.
9. The Privacy Officer may also:
    a. provide advice on issues related to information privacy
    b. develop privacy related resources

c. receive and provide responses to relevant regulator(s)
d. assist in the event of a privacy breach or breach investigation
e. monitor completion of privacy impact assessments
f. publish general collection statements.

Collection

10. Swinburne collects personal, sensitive and health information as part of operating as a university, for various purposes including:
    a. education and associated activities, such as research;
    b. employment of staff and engagement of contractors;
    c. providing health services.
11. Swinburne will only collect personal and health information where it is necessary and relevant to Swinburne's functions and activities and will do so in a lawful, fair and not unreasonably intrusive manner.
12. Personal and health information must not be collected from an individual if it is reasonable and practicable to engage with the individual without collecting that type of information.
13. Swinburne will only collect sensitive information where the individual has consented, where the collection is required by law, or is otherwise allowed under the Privacy and Data Protection Act 2014 and the Health Records Act 2001.
14. When collecting personal, sensitive or health information from an individual, all reasonable steps will be taken to ensure the individual understands how their information will be used, who it might be shared with, along with other matters outlined in any relevant Collection Statement.

Collection Statements

15. The area or department collecting the personal or health information is responsible for ensuring a Collection Statement is made available to the individual at, or before the time of collection. If this is impracticable, notice must be given as soon as possible following collection.

16. Collection Statements will include:
    a. why the information is being collected and who the information may be disclosed to
    b. any law(s) that require Swinburne to collect the information
    c. the team or area involved in collecting the information and how an individual can contact them
    d. how an individual can gain access to the information and seek correction of the information
    e. any consequences for the individual if some or all of the information is not provided
    f. how to view the Swinburne Privacy Guidelines and who to contact if an individual has concerns about the way Swinburne has handled their information.

Use and disclosure

17. Swinburne will, in most cases only use or disclose personal and health information collected in the course of university activities for the primary purpose for which the information was collected.
18. Swinburne may use personal and health information for a secondary purpose which is related to the primary purpose, in accordance with the relevant Privacy Principles, where the individual has consented, or where Swinburne is required by law to disclose such information.
19. Swinburne staff must only access personal, sensitive or health Information to the extent that is necessary to perform their role.
20. Swinburne staff must consider the privacy implications prior to any disclosure outside the University.
21. Swinburne staff must consult the Privacy Officer prior to any use or disclosure that was not either consented to, identified as the primary purpose for which the information was collected, or that may be a related secondary use that an individual would reasonably anticipate.
22. Swinburne staff who are requested to disclose information by law should consult the Privacy Officer.

Data Quality

23. Swinburne staff must take reasonable steps to ensure that personal and health information collected, used or disclosed is accurate, complete and up to date.

Data Security

24. Swinburne staff must ensure that personal, sensitive and health information they are responsible for is protected from misuse, interference, loss; and from unauthorised access, modification or disclosure, whether deliberate or inadvertent.
25. Swinburne staff must ensure they are aware of the obligations under the *Public Records Act 1973* (Vic) and any other legislation which may require staff to destroy, deidentify or otherwise transfer information to the Public Records Office when no longer needed by Swinburne.

Openness

26. Swinburne publishes the following documents on the management of personal information -
    a. Swinburne Privacy webpage
    b. Privacy Procedures (which contain supplementary information to these Guidelines)
    c. Privacy Collection Notices
    d. Staff privacy resources (Staff login required).

Access and Correction

27. An individual can request access to their information, or an opportunity to correct their personal or health information held by Swinburne. Requests for access and correction are managed under the *Freedom of Information Act 1982* (Vic).
28. Departments within Swinburne may develop work instructions to enable staff and students' access to their personal or health information held by the University.

Unique Identifiers

29. Swinburne will not assign unique identifiers unless it is necessary to carry out the functions of the University and in accordance with relevant Privacy Principles.

30. If Swinburne uses or discloses a unique identifier that has been assigned to an individual by another organisation it will do so in accordance with relevant Privacy Principles, or other applicable legislation.

Anonymity

31. When it is lawful and practicable, individuals may choose to not identify themselves when interacting with Swinburne. In some circumstances, it may not be possible for Swinburne to provide a service, or services to an individual who chooses to remain anonymous.

Transborder Data flow

Sending information outside of Victoria

32. It may be necessary for Swinburne to send personal, health or sensitive information outside Victoria as part of the University's functions and activities. When transferring such information, Swinburne will:
    a. ensure the recipient is subject to similar privacy obligations as apply in Australia; or
    b. ensure the individual has consented to the information being sent or handled; or
    c. ensure the transfer is authorised under Australian privacy laws.

Procurement and Contracts

33. When planning a Project the Head of Management Unit must ensure the University complies with its obligations under the privacy laws of Victoria and in some cases the Commonwealth.
34. Staff must incorporate a privacy by design approach into the design of major Project, ensuring privacy considerations continue throughout the life of the project.

Privacy Complaints

35. An individual who wishes to complain about the unauthorised use, access, disclosure of their personal information by the University may do so by contacting the Privacy Officer or by lodging a complaint through the Swinburne website.
36. Privacy complaints will be managed in accordance with the Swinburne *Complaints Management Guidelines.* Where the individual is a staff member a complaint will be handled under the University's staff grievance processes.

Part 5. Definitions

The following key terms are used throughout these Guidelines:

Term	Definition
Data Breach Response Plan	Means the Swinburne Data Breach Response Plan
Health Information	Information or an opinion about an individual's physical, mental or psychological health; disability; and other matters relating to the provision of health services.
Personal Information	Information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
Privacy by design	A design approach that aims to ensure privacy is considered before, at the start of, and throughout the development and implementation of a program.
Sensitive Information	A subset of Personal Information that is information or an opinion about an individual's racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices or criminal record. This is a special type of Personal Information which require additional controls and protection.
Privacy Principles	Means the Privacy Principles in the applicable Act- • Information Privacy Principles (IPP's) in the Privacy and Data Protection Act 2014 (Vic) • Health Privacy Principles (HPP's) in the Health Records Act 2001 (Vic) • Australian Privacy Principles (APP's) in the Privacy Act 1988 (Cth)
Project	Means a project, system or process implemented by Swinburne that involves Personal, Health or Sensitive Information.