

# Privacy Policy and Complaints Handling Procedures

# Contents

1. Policy Statement	3
2. Scope of the Privacy Policy	3
3. How we manage staff and other Related Information	3
4. How we manage Research information	3
5. Compliance with the Australian Privacy Principles (APP)	3
6. Privacy Policy Website Statement	3
7. Privacy Complaints Handling	3
8. Supplementary Information	4
9. Other information	4
10. ANNEX 1: SUMMARY OF THE AUSTRALIAN PRIVACY PRINCIPLES (APP)	4

## **1. Policy Statement**

The Institute will safeguard personal, sensitive and health data about an individual consistent with the Commonwealth and State privacy laws.

## **2. Scope of the Privacy Policy**

The privacy policy applies to (a) research undertaken at the Institute, (b) the management of the databases for which the Institute is the custodian and (c) other personal information.

The protection of an individual's personal information is the responsibility of every person working within the Institute, whether an employee (full time, part time, casual), contractor, consultant to the Institute, or a visiting researcher or student.

The privacy policy and privacy protections apply to all researchers undertaking research using data for which the Institute is the custodian.

## **3. How we manage staff and other Related Information**

The Sax Institute collects personal information relating to employees, contractors, members, and the Board in accordance with relevant Commonwealth and State government legislation and the national privacy principles. The information will be maintained in a confidential and secure environment.

## **4. How we manage Research information**

The Institute undertakes research within a national research governance and compliance framework established through various government and funding body requirements, ethics committees, national policy statements, codes and guidelines for the responsible conduct of research. The key documents for the research governance framework are:

- a. "Australian Code for the Responsible Conduct of Research" (2007);
- b. "National Statement on Ethical Conduct in Research Involving Humans" (NHMRC, 2007);
- c. "Guidelines for Ethical Research in Indigenous Studies" Australian Institute of Aboriginal and Torres Strait Islander Studies, (2002);
- d. "Values and Ethics – Guidelines for Ethical Conduct in Aboriginal and Torres Strait Islander Health Research" National Health and Medical Research Council, (2003).

## **5. Compliance with the Australian Privacy Principles (APP)**

The Institute will comply with the Australian Privacy Principles as outlined in the relevant laws. Summaries of these are annexed to this policy.

## **6. Privacy Policy Website Statement**

The Institute will keep a current Privacy Policy Statement on the website.

## **7. Privacy Complaints Handling**

The Institute is committed to the provision of an effective, efficient and responsive privacy complaints handling regime across all of its activities and programs and will ensure transparency and openness in the early resolution of privacy concerns and complaints.

Complaints will be addressed in accordance with procedural fairness and natural justice.

Procedures for dealing with complaints will be in accordance with the Privacy Act 1988 (Cwth), as amended.

- A complaint registered by an individual may be made by telephone, email or in writing.

- A complaint will be given to the Privacy Officer for assessment and investigation in consultation with the Chief Executive Officer or delegated officer.
- A written acknowledgement will be sent to an individual with 24 hours of complaint being received.
- If the individual makes a formal complaint to the Privacy Commissioner, the Chief Executive Officer or delegated officer will be the respondent on behalf of the Institute.

## 8. Supplementary Information

- Annex 1. Summary of the Australian Privacy Principles
- Annex 2. Summary of the Health Information Privacy Principles
- Annex 3. Privacy Complaints Handling Policy
- Annex 4. Privacy Complaints Handling Procedures

## 9. Other information

- Privacy and Security Compliance program documentation is held separately to this policy.
- Research governance framework is documented in the Responsible Conduct of Research Policy.

## ANNEX 1: SUMMARY OF THE AUSTRALIAN PRIVACY PRINCIPLES (APP)

From 12 March 2014, the Australian Privacy Principles (APPs) will replace the National Privacy Principles and Information Privacy Principles and will apply to organisations, and Australian Government (and Norfolk Island Government) agencies.

For further detail see the [full text of the APP](#).

Australian Privacy Principles — a summary for APP entities

For private sector organisations, Australian Government, ACT Government and Norfolk Island agencies covered by the Privacy Act 1988.

### APP 1 — Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

### APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

### APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

### APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

### APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

### APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

### APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

#### **APP 8 — Cross-border disclosure of personal information**

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

#### **APP 9 — Adoption, use or disclosure of government related identifiers**

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

#### **APP 10 — Quality of personal information**

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

#### **APP 11 — Security of personal information**

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

#### **APP 12 — Access to personal information**

Outlines an APP entity's obligations when an individual requests to be given access to personal information, held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

#### **APP 13 — Correction of personal information**

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.