

Privacy Management Plan March 2015



UTS Insearch

UNIVERSITY OF TECHNOLOGY SYDNEY

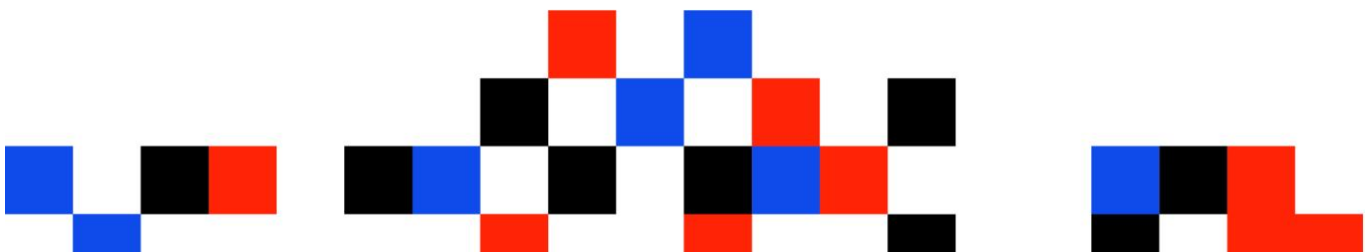


TABLE OF CONTENTS

1	INTRODUCTION	2
2	SCOPE	2
3	DEFINITIONS	3
4	PRIVACY PRINCIPLES.....	4
5	PERSONAL INFORMATION	5
6	REQUIREMENTS OF THE PLAN	6
7	INSEARCH USE OF PERSONAL INFORMATION	6
8	POLICIES, PRACTICES AND CONTROLS.....	8
8.1	CODE OF ETHICS.....	8
8.2	CODE OF CONDUCT.....	8
8.3	EMPLOYEES’ RESPONSIBILITY	9
8.4	COMPLIANCE MANAGEMENT PROGRAM	9
8.5	OTHER LEGAL REQUIREMENTS AFFECTING PRIVACY	9
8.6	COMPLIANCE WITH PUBLIC REGISTER PROVISIONS	9
8.7	PRIVACY OFFICER.....	9
8.8	RESPONSIBILITIES OF THE PRIVACY OFFICER	10
8.9	CLASSES OF PERSONAL INFORMATION	10
9	DISSEMINATION OF POLICIES AND PRACTICES	11
9.1	PRIVACY TRAINING AND EDUCATION	11
10	INTERNAL REVIEW PROCEDURES	11
10.1	THE INTERNAL REVIEW PROCESS	11
10.2	INCIDENT REPORTING	13
10.3	DISCIPLINARY PROCEDURES.....	13
11	PRIVACY AND PROTECTION OF PERSONAL INFORMATION	13
11.1	APPLICATIONS FOR ACCESS TO PERSONAL INFORMATION	13
12	RELATED LEGISLATION	13

1 INTRODUCTION

Insearch Limited (Insearch) is a commercial provider of higher education. Its main operation is the provision of pathway programs for domestic and international students preparing to enter degree programs at UTS, and through its joint venture arrangements provides English language programs for overseas students.

Insearch must comply with statutory obligations under *Privacy and Personal Information Protection Act 1998 (NSW)* (the PPIP Act) and its Information Privacy Principles (IPP), and other responsibilities under the *Health Records and Information Privacy Act 2002 (NSW)* (HRIP Act) and its Health Privacy Principles (HPP). Under s33 of the PPIP Act, Insearch is required to have an established Privacy Management Plan and in accordance with section 33-5, a copy has been lodged with the NSW Privacy Commissioner.

Insearch is considered to be an “agency” pursuant to the *Privacy Act 1988 (Cth)*, and therefore must comply with the private sector principles, namely the Australian Privacy Principles (APP) from Schedule 3 of the [Privacy Act 1988 \(Cth\)](#). These Principles are consistent with the IPP and HPP.

The Insearch Privacy Management Plan (Plan) informs our stakeholders and staff how we manage personal information and explains who a person can contact with questions about the personal or health information we hold, how they can access and amend their information and what to do if they think Insearch may have breached the PPIP Act or the HRIP Act. It is also used as a staff training tool.

All staff and students, and any person employed by Insearch, are required to comply with the legal obligations of Privacy and personnel working in areas most likely to have access to or be exposed to personal or sensitive information must ensure it is safeguarded. However everyone is expected to respect each other’s privacy, maintain confidentiality and comply with the principles.

The Principles and Privacy Act address the collection, storage, security, use and disclosure of personal and health information, and establish the standards for collecting and dealing with personal information to eliminate the risk of misuse of that information. The Principles also allow individuals to exercise control over what happens to their own personal information.

Please refer to [Appendix A](#) for more information about the Principles and Privacy Act, and other privacy-related legislation.

Section 41 Directions: the NSW Privacy Commissioner provides Public interest directions that can be obtained from the Information and Privacy Commission NSW [website](#).

The Insearch Plan has been developed in line with the [information and privacy commission new south wales: A Guide to Making Privacy Management Plans – August 2012](#). This Plan will be reviewed every 5 years, or in the event of any legislative, administrative or systemic changes.

2 SCOPE

This Plan applies to;

- Insearch Board of Directors
- All Insearch employees (including contract and casual staff)
- All Insearch students and student bodies
- Channel Partners
- Joint venture partners and education affiliates
- Consultants and contractors of Insearch
- Conjoint and visiting appointees

Board of Directors

The Insearch Board of Directors is bound by the PPIP Act (NSW) and APP individually and under the corporate governance framework, which incorporates all relevant statutory requirements and legal obligations.

Insearch Employees

Employees are bound by the PPIP Act and APP just as Insearch will apply those same principles to its employees. Insearch regards information concerning its employees as personal information in respect of the PPIP Act and APP, whether it is:

- recruitment material (except information or an opinion about an individual's suitability for appointment or employment as a public sector official),
- leave and payroll data,
- personal contact information,
- performance management plans,
- disciplinary matters,
- complaints by clients, and
- salary and benefit entitlements.

Insearch Students and Student Bodies

Insearch regards all information concerning its students as information protected by the PPIP Act and APPs.

Channel Partners

All Channel Partners must abide by the PPIP Act and APP under the terms of their contracts with Insearch.

Consultants and Private Contractors of Insearch.

Insearch may employ consultants directly to perform a specific function; or contract services in whole or in part to private contractors including data service providers. Private contractors and consultants must abide by the PPIP Act and APP under the terms of their contracts with Insearch.

Joint Venture Partners and Educational Affiliates

Insearch currently has agreements or partnerships with:

1. University of Technology, Sydney;
2. Shanghai University, Sydney Institute of Language and Commerce;
3. IDP Education – ACET Vietnam;
4. ELTI Gramedia – Indonesia.
5. EIC Group (China)
6. International Education Network Inc. (IEN) (Korea)

Insearch will seek to ensure that these bodies comply with the PPIP ACT and APP so far as it is practicable.

3 DEFINITIONS

Personal Information	Any information or opinions (including forming part of a database and whether or not recorded in a material form) about a person where that person's identity is apparent or can be reasonably ascertained. Personal information can include a person's name, address, student number, video recordings and photographs of an individual, and electronic records.
Personal Information held by Insearch	<p>Personal information is held by Insearch when:</p> <ul style="list-style-type: none"> • it is in possession or control of the information; or • the information is in the possession or control of a person employed or engaged by Insearch in the course of such employment or engagement; or • the information is contained in a State record for which Insearch is responsible under the <i>State Records Act 1998 (NSW)</i>
Sensitive Information	<p>All personal information should be considered sensitive, and an individual may indicate that some of their information is particularly sensitive. Examples of highly sensitive information include ethnicity, union membership, sexual preference and medical conditions.</p> <p>The degree of sensitivity of the personal information may influence the way</p>

	in which the information protection principles are applied. The more sensitive the nature of the information, the higher the level of care should be used by staff when dealing with the information, particularly where disclosure to a third party is being considered.
Privacy and Confidentiality	Privacy applies to personal information, irrespective of who provided it to Insearch. It relates to an individual's ability to control the extent to which their personal information, enabling identification, is available to others. Confidentiality restricts Insearch from using or disclosing some information in a way which is contrary to the interests of the person or organisation that provided it in the first place. Confidentiality is defined as a mode of managing private information, by the restriction of access to information to authorised persons, entities and processes at authorised times, in an authorised manner.
Use and Disclosure of Personal Information	Information protection refers to the treatment and handling of personal information within an organisation, particularly when this involves making decision on the basis of the information. Disclosure refers to making personal information available to people outside the organisation, other than to the individual concerned and includes the publication of personal information.
Health Information	Specific type of information as defined in section 6 of the HRIP Act. Health information can include, among other things, information about a personal's physical or mental health, or information about a person's medical appointment.

4 PRIVACY PRINCIPLES

Information Protection Principles (IPP)

Part 2 Division 1 of the PPIP Act (NSW) includes 12 IPP that all agencies must comply with. Sections 8-19 of the Act detail each one of the principles named as follows:

- Section 8 - Collection of personal information for lawful purposes
- Section 9 - Collection of personal information directly from individual
- Section 10 - Requirements when collecting personal information
- Section 11 - Other requirements relating to collection of personal information
- Section 12 - Retention and security of personal information
- Section 13 - Information about personal information held by agencies
- Section 14 - Access to personal information held by agencies
- Section 15 - Alteration of personal information
- Section 16 - Agency must check accuracy of personal information before use
- Section 17 - Limits on use of personal information
- Section 18 - Limits on disclosure of personal information
- Section 19 - Special restrictions on disclosure of personal information

A detailed description of the IPPs is provided in [Appendix A](#).

Australian Privacy Principles (APP)

Insearch is considered to be an "agency" pursuant to the *Privacy Act (Cth)*, and therefore must comply with the private sector principles, namely the Australian Privacy Principles from Schedule 3 of the [Privacy Act 1988 \(Cth\)](#). These Principles are consistent with the IPP and HPP.

There are 13 Australian Privacy Principles that came into effect on 12 March 2014 and apply to Insearch.

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.

5 PERSONAL INFORMATION

Under the PPIP Act and APP, personal information means "*information or an opinion (including forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion*".

Section 4.3 of the PPIP Act specifies what is not considered personal information that includes, for example, information that is contained in a publicly available publication, information about an individual who has been dead for more than 30 years, information contained in a public interest disclosure. .

6 REQUIREMENTS OF THE PLAN

In accordance with the PPIP Act, for a public sector agency, this Plan includes information relating to:

- (a) established policies and practices to ensure compliance with the requirements of the Act;
- (b) the systems and processes for dissemination of policies and practices to relevant stakeholders and persons within Insearch;
- (c) the established internal review procedures under Part 5 of the Act; and,
- (d) all other relevant matters in relation to privacy and the protection of personal information held by Insearch.

7 INSEARCH USE OF PERSONAL INFORMATION

DEPARTMENT/ROLE	KEY FUNCTIONS	MAIN USE OF PERSONAL INFORMATION
Sales and Marketing	Responsible for the recruitment of students into all of our courses, both directly and indirectly through our global network of channel partners. Activities include managing the Insearch brand, publications, surveys, promotional campaigns, PR activities, advertising campaigns and channel partner management.	Publishing Filming Photography Media Ambassador Programs Direct marketing
Hobsons	Maintenance of prospect database Provision of course information	Prospect management and contact Direct marketing
Channel partners	Management of applications from international students who wish to enrol at Insearch and UTS	Prospect management and follow-up Application process Compliance with the Department of Home Affairs requirements
Student Centre	Student's face to face service/support Homestay service Changes/updates on students' information	Assisting with student visas, health cover and whole application process
Student Admissions	Management of student admission Maintenance of student records Maintenance of student files Management of student incidents Management of critical incidents	Student applications Emergency contact information Tax file number management (for Fee-Help purposes)
Student Administration	Timetabling and Enrolment Maintenance of student records Maintenance of student files Student activities and events Graduation events	Dissemination of exam results, transcripts, testamurs. Financial information of students
Student Advisers	Support to students in academic progress and personal challenges Assisting students to overcome adaptableness difficulties	Monitoring student progression and support Assessment and review of students with sanctions
Teaching programs (ELT, Diploma and Foundations)	Teaching, tutoring and assessment of students	Student assessment Course and subject lists Assessment and review of students Monitoring of student progression
Registrar	Student discipline and appeals	Handling complaints and student appeals

DEPARTMENT/ROLE	KEY FUNCTIONS	MAIN USE OF PERSONAL INFORMATION
		<p>Assessment of applications for special consideration</p> <p>Assistance for students with special needs</p> <p>Handling of grievance complaints</p>
Human Resources	<p>Recruitment</p> <p>Remuneration & benefits</p> <p>Talent management and development</p> <p>Employee relations</p> <p>Workplace health & safety for staff</p>	<p>Employment screening to check and verify work history, qualifications and experience, immigration status, clearance to work with children and at times police records.</p> <p>Producing employment-related contracts</p> <p>Setting and administering individual salaries and benefits</p> <p>Managing performance and development</p> <p>Handling complaints and grievances</p> <p>Health-related matters; workplace incidents, workers compensation, personal illness or wellbeing</p> <p>Reporting on people metrics</p>
Payroll Coordinator	<p>The collation, processing and administration of information in order to ensure staff are remunerated through salary, superannuation, incentive and benefit payments.</p> <p>Taxation management.</p> <p>Coordination and security of personnel records and files.</p>	<p>Creation of online personnel records.</p> <p>Arranging salary payments and lodgement into financial and other institutions such as superannuation providers</p> <p>Business and management reporting</p> <p>The provision of personal and sensitive information where authorised.</p>
ICT	<p>Staff personal contact details and profiles</p> <p>Student profiles</p> <p>Management of BI data</p>	<p>Allocation of mobiles, laptops or other technical devices to staff</p> <p>Audits on student/staff use of systems</p> <p>Granting of access to systems (including Internet)</p>
SLT and Managers	<p>Information of direct report staff used in managing the business.</p> <p>Remuneration and benefits</p>	<p>Management of staff</p> <p>Performance management</p> <p>Professional development and review</p>
Governance	<p>Whistle-Blowing Policy</p> <p>Board and Audit & Risk Committee registers</p>	<p>Maintain anonymity and confidentiality as required</p> <p>Personal and contact details</p> <p>Contract management</p>
Finance department	<p>Management of Insearch's financial resources, including accounting systems and payroll</p>	<p>Payment of staff salaries and benefits.</p>
Facilities	<p>Monitor the video surveillance</p> <p>Supplier details</p> <p>Engaging contractors</p> <p>Document storage and destruction</p>	<p>Safety and security of building occupants</p> <p>Induction of Contractors</p>
Joint Venture Partners Educational Affiliates	<p>Monitoring potential students and offering information about courses</p> <p>Management of applications from overseas students who wish to enrol at Insearch and possibly UTS</p> <p>Staff personal information and salary information</p>	<p>Partners/Affiliates shall not disclose to any person, other than Insearch, any student's Personal Information unless that person has:</p> <ul style="list-style-type: none"> • given their written consent to such disclosure; • been provided with the Privacy Notification Form prior to the collection of the Personal Information and the person is an intended recipient; or • the disclosure is one which is otherwise authorised by the PPIP Act or other law.

DEPARTMENT/ROLE	KEY FUNCTIONS	MAIN USE OF PERSONAL INFORMATION
		<p>5.2 The obligation on the Partners/Affiliates under this clause shall not be taken to have been breached where the information referred to is legally required to be disclosed, provided the Partners/Affiliates notify Insearch immediately the request for disclosure is made.</p> <p>5.3 Should Insearch object to the making of the disclosure, the Partners/Affiliates shall abide by that objection. A failure by Insearch to notify any objection shall not operate to relieve the Partners/Affiliates of any obligation at law or create any obligation on the part of Insearch.</p>

Note: When a company or other agency contacts Insearch to verify if a prospective employee is an Insearch graduate, Insearch will confirm:

1. if the person is or is not an graduate,
2. the education level completed,
3. the program finalised.

This information is made publicly available at graduation ceremonies and is not considered personal information under the PPIP Act and Privacy Act.

8 POLICIES, PRACTICES AND CONTROLS

Insearch has implemented a Privacy Policy for students and staff in response to its commitment to the PPIP Act and APP that addresses the collection, storage, security, access and accuracy, use and disclosure of personal information from individuals. The Privacy Policy is available on the Staff Intranet, Student Extranet and Insearch public website.

The [Privacy Statement](#) is also located in the Staff Intranet, Student Extranet and Insearch public website.

This Plan is included as part of the staff orientation process, privacy training sessions, and referenced in other staff development programs.

8.1 Code of Ethics

The Insearch Board of Directors strongly supports and promotes ethical and responsible decision making, and operates within a [Code of Ethics](#) that sets out the core values Insearch applies in achieving its purpose. The Code provides the framework for individuals and groups of people to engage in ethical decision-making within the organisation.

Insearch is committed to being an established, international, commercial provider of higher education, operating with integrity, honesty, courage, compassion, respect and imagination, and expects its staff to perform with integrity, honesty and respect in professional, academic and personal matters, and to comply with the Insearch Code of Ethics and Code of Conduct.

The Code of Ethics is included in all key internal and external publications for students, staff, channel partners and other stakeholders; it is part of the Insearch culture and is applied by staff in the conduct of Insearch business.

8.2 Code of Conduct

Insearch has a [Staff and Affiliates Code of Conduct](#) that explains the principles of behaviour Insearch expects of its employees whilst at work and when representing Insearch in the course of work or at related events. It specifically addresses privacy and confidentiality matters. The Board of Directors, Senior Leadership Team (SLT), managers and all employees are expected to abide by the Code of Conduct. Any suspected breach is treated seriously, fully investigated and may result in disciplinary action..

The Code of Conduct is reviewed periodically and was last updated in 2014.

The Code of Conduct is provided to all new staff with their Employment Offer, reinforced during regular Staff Orientation sessions and is accessible on both the website and staff intranet.

All staff are required to verify their compliance with the Code of Conduct on an annual basis.

8.3 Employees' Responsibility

It is the responsibility of all employees to understand and comply with the key privacy principles.

All employees are expected to act in a professional and ethical manner, comply with internal privacy control requirements, policies and procedures, and follow legal requirements, with a view to maintaining and enhancing the reputation of Insearch.

It is expected that employees recognise signs of potential breaches of privacy, confidentiality issues and lack of discretion, and report these to their respective manager or a senior manager. Employees are also expected to assist with any enquiries and investigations pertaining to privacy breaches and associated misconduct.

Members of the SLT and managers must raise awareness of the privacy amongst staff through development activities and team meetings, and ensure training, induction or orientation programs are exercised.

8.4 Compliance Management Program

In order to comply with the IPP, APP and HPP, applicable laws, regulations, codes and the organisation's standards, Insearch has implemented a risk-based compliance management program.

By implementing compliance management systems, Insearch aims to limit the risk of breaches of legislative requirements and adverse audit findings, including privacy issues or breaches that can have financial and non-financial implications for the organisation.

Related policy and procedure includes: Compliance Management Program, Compliance Reporting Procedure and Register, Policy and Procedure Development Policy, Fraud and Corruption Control Plan, Risk Management Policy. All relevant documents are available on the [Policy and Procedures website](#).

Specific controls include: primary privacy contact, a dedicated privacy email address; the internal audit program; staff training; roles and responsibilities of Board and Committees, the SLT and all managers; the annual compliance reporting procedure, compliance management reports to the Audit & Risk Management Committee addressing changes in obligations, incidents and corrective action, training & communication activity, implemented compliance controls; managing non-compliance through operational level management processes and remedial action.

8.5 Other legal requirements affecting privacy

As part of the Working with Children Check Procedure, criminal record checks are required of Insearch employees and contractors working within Australia. These checks are conducted through the appropriate regulatory body.

8.6 Compliance with public register provisions

Insearch does not hold or maintain any public registers.

8.7 Privacy officer

Privacy is the responsibility of all staff and stakeholders at Insearch. Initial inquiries about information held is usually managed by the manager of the department that holds the information, however, Insearch has a nominated Privacy Officer as the main contact for staff and students to deal with privacy matters.

The Privacy Officer will handle requests from staff or students for access to personal files held and will monitor compliance.

Contact details:

THE PRIVACY OFFICER
Insearch Limited
PO Box K1085
Haymarket NSW 2000
[E] privacy@insearch.edu.au

8.8 Responsibilities of the Privacy Officer

In order to ensure compliance with PPIP Act and APP, the Privacy Officer will review internet contact forms, rates notices, application forms of whatsoever nature, or written requests by which personal information is collected.

The Privacy Officer will also provide advice as to:

- (i) whether the personal information is collected for a lawful purpose;
- (ii) if that lawful purpose is directly related to a function of Insearch; and
- (iii) whether or not the collection of that personal information is reasonably necessary for the specified purpose.

Any further concerns of a legal nature will be referred to Insearch's legal advisers.

Concerning the general implementation of the Plan, the Privacy Officer will ensure that student enrolment forms:

- (i) note the commencement of the new PPIP Act and APP;
- (ii) state that Insearch holds personal information;
- (iii) note that Insearch may use and disclose personal information in various circumstances; and
- (iv) state that for further information, the Privacy Officer should be contacted.

The Privacy Officer may recommend the assigning of designated officers as "Privacy Resource Officers" within the larger departments of the organisation. In this manner Insearch can ensure the information protection principles are more broadly understood and that individual departments have a greater focus on the information protection principles as they may be directly applied into day-to-day functions.

8.9 Classes of personal information

Type of record	Personal information held in record
Student records – maintained in hardcopy files and on student database, includes past students	Personal details (name, address, phone), date of birth, previous education, Aboriginality, country of origin, subjects, marks/grades; may include special entry application details, special needs details, discipline reports, grievance reports, progress reports, special consideration applications, withdrawal details, tax file number, fees and debts, emergency contact information.
Staff files – maintained in hardcopy files and on Lattice database	Personal details, date of birth, employment application, CV, previous employment details, referee reports, employment contract, medical details, salary and banking details, performance reviews, discipline reports, leave applications, medical certificates, EEO details, tax file number, emergency contact information.
Student and staff surveys	Personal details, personal views and comments.
Alumni Records	Personal details.
Medical Records	Personal details, confidential health details.
Subject folders	List of students; assignments identified by student name and ID, assignment mark and comments.
Graduate lists	Names (mailing address in some instances), course.

Grievance records	Personal details, statements, summary of grievance and outcome.
Pay records – maintained in hardcopy and on database	Personal details, salary, banking and deduction details, tax file number.
Supervisor files	Personal details, progress reports on research students.
Homestay Service files	Personal details, next of kin, smoker/non-smoker status, application may contain confidential personal information (e.g., health details, hardship) Homestay family personal details.
Workers compensation files	Personal details, previous medical history, medical reports, medical certificates, rehabilitation reports.
Company registers	Personal information of Directors and committee members.

9 DISSEMINATION OF POLICIES AND PRACTICES

Orientation and training programs, and public awareness information comprise the following elements:

- legislative requirements under the PIPP Act, APP and HRIP Act;
- the fact that corrupt disclosure or use of personal information is a criminal offence;
- the need to appoint members of staff as Privacy Resource Officers, where appropriate;
- the need to attend to areas where breaches are more likely (such as inadequate security for staff and student files or failure to dispose of personal information that is no longer in use);
- all new staff are informed about Privacy as part of a compulsory induction course;
- information about Privacy is on the Insearch [website](#);
- regular updates and reminders about Privacy requirements are sent to the Privacy Officer for dissemination across the organisation and to specific units.

These activities are coordinated by the Privacy Officer, and will be included in the compliance training program currently under development. In addition, some units conduct local privacy and confidentiality sessions to address specific work needs and matters.

9.1 Privacy Training and Education

Staff are required to attend training or awareness sessions to understand Privacy as it relates to their role, and to prevent any breaches due lack of information and/or knowledge. Supervisors and managers of staff who have high level involvement in work practices directly related to privacy matters, ensure these staff members receive the appropriate level of training. Training sessions are conducted each year and attendance by Insearch personnel is compulsory. The compliance training program, incorporates formal training, and on-the-job learning and corporate communications and embeds privacy practices into daily operations through improved awareness and encouragement. It also offers a tracking and reporting tool for staff records.

Notifications on updates/changes to legislation relating to Privacy, Copyright, Records Management and ESOS and The National Code of Practice are emailed to all staff as and when received.

A summary version of the Policy and Plan is provided to all new staff in the “New Staff Orientation Pack”, and the full Plan is accessible on the Staff intranet.

10 INTERNAL REVIEW PROCEDURES

10.1 The internal review process

An application for a review of a potential breach of privacy must:

- a) be in writing [[Application for Internal Review](#)];
- b) be addressed to:
The Privacy Officer

Insearch Limited
PO Box K1085
Haymarket NSW 2000
[E] privacy@insearch.edu.au [T] 61 2 9218 8600

- c) specify an address in Australia to which a notice may be sent; and
- d) be lodged at an office of Insearch Limited within 6 months from the time the applicant first became aware of the conduct that is the subject of the application (or such later date as the agency may allow).

The review will be conducted by the Privacy Officer, where the Privacy Officer is not substantially involved in the matter relating to the application. Other suitably qualified members of staff may be called upon to conduct the review if the Privacy Officer where appropriate. At all times, the review will be held by an employee or officer of Insearch.

In reviewing the conduct that is the subject of the application, the individual dealing with the application must consider any relevant material submitted by the applicant and the Privacy Commissioner.

Insearch will endeavour to complete the review as soon as is reasonably practicable, and will complete the review within 60 days from the day on which the application was received. If the review is not completed within this time the applicant may apply for a review of the conduct concerned to the NSW Civil and Administrative Decisions Tribunal under Section 55 of the PPIP Act.

On receiving an application for an internal review, Insearch must:

- a) inform the NSW Privacy Commissioner as soon as is practicably possible of the application;
- b) keep the NSW Privacy Commissioner informed of the progress of the internal review; and
- c) inform the NSW Privacy Commissioner of the findings of the review and of the action proposed to be taken by the agency in relation to the matter.

Once the internal review has been completed, Insearch may do one or more of the following:

- a) take no further action on the matter;
- b) make a formal apology to the applicant;
- c) take such remedial action considered appropriate;
- d) provide undertakings that the conduct will not occur again; and
- e) implement administrative measures to ensure that the conduct will not occur again.

Within 14 days of the completion of the review, Insearch will notify the applicant in writing of:

- a) the findings of the review (and the reasons for those findings);
- b) the action proposed to be taken by the agency (and the reasons for taking them); and
- c) the right of the person to have those findings, and the agency's proposed action, reviewed by the NSW Civil and Administrative Tribunal.

If an individual believes that Insearch has breached, or is likely to breach, one or more of the Privacy Principles, they may submit a written request to Insearch to investigate the matter. The following procedures will be used to resolve an application for internal review.

- The application is assessed by Insearch's Privacy Officer to determine whether the complaint involves a breach of privacy.
- The Privacy Officer will notify the NSW Privacy Commissioner in writing that an application for internal review has been received.
- The Privacy Officer (or another person appointed by the Managing Director if the matter involves the Privacy Officer) will investigate the matter by considering all relevant material supplied by the applicant and the Privacy Commissioner.
- Every four weeks the Privacy Officer will inform the NSW Privacy Commissioner in writing about progress of the review.
- The review will be completed as soon as possible, and in all cases within 60 days of receiving the application.
- The Privacy Officer will notify the applicant of the following (as appropriate):

- findings of the review;
- reasons for those findings;
- a formal apology from Insearch;
- remedial action to be undertaken by Insearch (which may include compensation);
- Insearch’s undertaking that the breach of privacy will not recur;
- administrative measures that will be implemented to ensure no further breach of privacy;
- reasons for the proposed remedial action and administrative measures;
- the applicant’s right to have the findings and Insearch’s proposed remedial action and administrative measures reviewed by the NSW Civil and Administrative Tribunal.

The Privacy Officer will notify the NSW Privacy Commissioner in writing of the findings and of any remedial action and administrative measures that Insearch proposes to undertake.

The Privacy Officer will initiate administrative measures to ensure that the breach does not recur. Where appropriate, new or revised procedures may be incorporated into the Privacy Management Plan.

The Privacy Officer will provide an annual report on all requests and related outcomes of privacy internal reviews to the Senior Leadership Team, and the Audit and Risk Management Committee.

10.2 Incident reporting

Employees seeking to report privacy issues should, in the first instance, report the matter to their immediate manager. If, for any reason, the employee feels that reporting the incident through this channel would be inappropriate, the employee may report the matter directly to the Privacy Officer, a member of Human Resources or a member of the SLT. Such reports may be made confidentially if desired.

Any person making allegations or providing information in relation to an alleged fraud or other matter involving misconduct must be made aware that the information provided will be relied upon and eventually the person concerned may be asked to give evidence relative to their knowledge of the circumstances. A person who has made a confidential report will not be required to give evidence about their report.

10.3 Disciplinary procedures

The [Grievance and Resolution Policy](#) aims to monitor the transparency of the grievance handling process for staff, and is also supported by the [Grievance - Informal Resolution Procedure](#). Also, the [Whistle-Blowing Policy](#) provides disciplinary processes related to fraud and corruption matters.

11 PRIVACY AND PROTECTION OF PERSONAL INFORMATION

11.1 Applications for access to personal information

Applications should be made to the Human Resources Unit (for staff records) or to the Privacy Officer (for student records). If, having inspected their file, the applicant lawfully alters personal information on that file, the Privacy Officer will send a copy of that alteration to the Human Resources Unit or Student Administration Unit (as appropriate) for attachment to the applicant’s personal file.


Applications that entail searches for extensive documentation located in various units should be referred to the Privacy Officer. These applications will be handled in a manner consistent with reasonable use of resources and without impeding the core business. Applications of a frivolous nature, or that would involve a substantial and unreasonable diversion of resources, will not be accepted.

12 RELATED LEGISLATION

With reference to its holdings of personal information, Insearch has made provision to comply with the following legislation:

- State Records Act (1998)
- Freedom of Information Act (1989)
- Public Interests Disclosures Act (1994) (NSW)

ADMIN USE ONLY

APPROVAL	
Signature:	
Name:	Alex Murphy, Managing Director Date: 17 March 2015
Policy Title	Privacy Management Plan
Policy Owner:	Company Secretary
Policy ID	PO/GOV/02/15
Effective Date:	March 2015

Appendix A: about the privacy laws

This is a general summary of how INSEARCH staff and students must manage personal and health information under the [PPIIP Act](#), the [HRIP Act](#) and other relevant laws. For more information, please refer directly to the Information and Privacy Commission [website](#) or the [Legislation](#).

The PPIIP Act and personal information

The PPIIP Act sets out how we must manage **personal** information.

About personal information

Personal information is defined in s4 of the PPIIP Act and is essentially any information or opinions about a person where that person's identity is apparent or can be reasonably ascertained. Personal information can include a person's name, address, family life, sexual preferences, financial information, fingerprints and photos.

There are some kinds of information that are not personal information, e.g. information about someone who has been dead for more than 30 years, information about someone that is contained in a publicly available publication, or information or an opinion about a person's suitability for employment as a public sector official. Health information is generally excluded here as it is covered by the HRIP Act.

Information protection principles (IPP)

Part 2, Division 1 of the PPIIP Act contains 12 IPPs with which we must comply. Here is an overview of them as they apply to INSEARCH.

Collection

1. We collect personal information only for a lawful purpose that is directly related to our functions and activities.
2. We collect personal information directly from the person concerned or an authorised agency.
3. We inform people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. We tell people how they can access and amend their personal information and any possible consequences if they decide not to give their personal information to us.
4. We ensure that personal information is relevant, accurate, is not excessive and does not unreasonably intrude into the personal affairs of people.
5. By only collecting information that is relevant to INSEARCH's functions as a Higher Education Provider, and making individuals aware, at the time of collection, that we are collecting personal information, INSEARCH ensures the information is relevant to that purpose, is not excessive, up to date and complete.

Storage

6. We store personal information securely, keep it no longer than necessary and destroy it appropriately. We protect personal information from unauthorised access, use or disclosure.
7. INSEARCH ensures that personal information is protected by storing it on secure data servers that are regularly maintained.

Access and accuracy

8. We are transparent about the personal information we store about people, why we use the information and about the right to access and amend it.
9. We allow people to access their own personal information without unreasonable delay or expense.
10. We allow people to update, correct or amend their personal information where necessary.
11. We make sure that personal information is relevant and accurate before using it.

Use

12. We only use personal information for the purpose we collected it for, unless the person consents to us using it for an unrelated purpose.

Disclosure

13. We only disclose personal information with people's consent unless they have already informed of the disclosure when we collected the personal information.
14. We do not disclose sensitive personal information without consent, e.g. ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership.

Exemptions to the IPP

Part 2, Division 3 of the PPIP Act contains exemptions that may allow us not to comply with IPPs in certain situations. Here are some examples.

- We are not required to comply with IPPs 2-3, 6-8, or 10-12 if we are lawfully authorised or required not to do so.
- We are not required to comply with IPP 2 if the information concerned is collected in relation to a court or tribunal proceedings.

We do not use the other exemptions on a regular basis as they are not usually relevant to the work we do, however if required we will aim to be clear about the exemption used and our reasons for using it.

Privacy codes of practice and public interest directions can modify the IPPs for any NSW public sector agency. These are available on the Information and Privacy Commission [website](#).

There are currently no codes of practice that are likely to affect how we manage personal information.

There are public interest directions that may allow us:

- not to comply with IPPs 2-3, 6-8, 10-12 if necessary in order to properly conduct investigations
- to be exempt from the IPPs when transferring enquiries to a NSW public sector agency.

The other public interest directions are unlikely to affect how we manage personal information.

Offences

Offences can be found in s62-68 of the PPIP Act.

It is an offence for us to:

- intentionally disclose or use personal information accessed in doing our jobs for an unauthorised purpose;
- offer to supply personal information that has been disclosed unlawfully;
- hinder the Privacy Commissioner or a member of staff from doing their job.

The HRIP Act and health information

The HRIP Act sets out how we must manage **health** information.

Health information is a more specific type of personal information and is defined in s6 of the HRIP Act. Health information can include information about a person's physical or mental health such as a psychological report, or even information about a person's medical appointment.

In the event INSEARCH receives health information from an individual, all the information will be handled in accordance with the HRIP Act and Health Privacy Principles.

Privacy Act 1988 (Commonwealth)

The *Privacy Act 1988* (Privacy Act) is an Australian law that regulates the handling of personal information about individuals. This includes the collection, use, storage and disclosure of personal information, and access to and correction of that information.

Other laws that affect how we comply with the IPP and HPP

This section contains information about the main laws that affect how we comply with the IPP and HPP.

Crimes Act 1900

Under this law INSEARCH staff and students must not access or interfere with data in computers or other electronic devices unless authorised to do so.

Government Information (Public Access) Act 2009 (GIPA Act) and Government Information (Public Access) Regulation 2009

Under this law people can apply for access to government information we hold. Sometimes this information may include personal or health information. If a person has applied for access to someone else's personal or health information we must consult with affected third parties. If we decide to release a third party's personal information, we must not disclose the information until the third party has had the opportunity to seek a review of our decision.

When accessing government information of another NSW public sector agency in connection with a review, the Information Commissioner must not disclose this information if the agency claims that there is an overriding public interest against disclosure.

Government Information (Information Commissioner) Act 2009 (GIIC Act)

Under this law the Information Commissioner has the power to access government information held by NSW public sector agencies for the purpose of conducting a review, investigation or dealing with a complaint under the *Government Information (Public Access) Act 2009* (GIPA Act) and GIIC Act. The Information Commissioner also has the right to enter and inspect any premises of a NSW public sector agency and inspect any record.

This Act also allows the Information Commissioner to provide information to the NSW Ombudsman, the Director of Public Prosecutions, the Independent Commission Against Corruption or the Police Integrity Commission.

Independent Commission Against Corruption Act 1988

Under this law we must not misuse information we have obtained in the course of doing our jobs.

Public Interest Disclosures Act 1994 (PID Act)

INSEARCH has [Public Interest Disclosure Policy](#) relating to our compliance with the PID Act.

State Records Act 1998 and State Records Regulation 2010

This law sets out when we can destroy our records. It also authorises the State Records Authority to establish policies, standards and codes to ensure that NSW public sector agencies manage their records appropriately.