Australian National University

Privacy Impact Assessment

ANU Insight

Author: James Walsh
Date: July 2020
Version: 1.0

Australian National University
Canberra, ACT
www.anu.edu.au
CRICOS Provider No. 00120C

Australian National University

Document Approval

Supported By:

(Richelle Hilton, Director, Planning and Performance Measurement) Date

Approved By:

8 July 2020

(Roxanne Missingham, Privacy Officer) Date

1. Contact Details

Name:	Roxanne Missingham and Paul Oakes, Planning and Performance Measurement (PPM)
Phone number:	EXT 57415
Role:	Privacy Officer, and Associate Director, Reporting and Analytics (R&A), PPM
Email:	privacy@anu.edu.au and insight@anu.edu.au

2. Project Description

ANU Insight acts as the central management information reporting system for the University. The system draws, amongst other data items, personal data concerning students, staff, visiting and honorary academics (VaHA), prospective students and contractors. Where listed, emergency contacts of the previously mentioned groups may also be accessible.

All PPM staff responsible for the creation and management of the ANU Insight system are required to agree and abide by the ANU Privacy Policy. All relevant sections of this policy are considered when using or making changes to the system. All PPM staff are required to undertake privacy training, and abide by strict report building protocols to ensure that data is not able to be accessed without permission. Access to the data to build a report is only given after the individual has completed the relevant forms to be able to view the data, and is given on the proviso that it is used only for the purpose of building and testing the reports.

The ANU Insight system is accessible to current staff only, after completion and signature of the ANU Code of Conduct. ANU Staff with access to the system are to use personal information obtained from the system consistent with this policy, which states:

22. A person who obtains information because they are an official of the University must not improperly use the information to gain an advantage for themselves or any other person; or cause detriment to the University, the Commonwealth or any other person.

32.f [All staff should] take reasonable steps to ensure adequate protection of all confidential information

Personal data from the system is not to be provided to any individual, or organisation who has not agreed to the ANU Code of Conduct or an agreed upon Non-Disclosure of Personal Information Agreement, written by the Director, PPM, Privacy Officer, or a member of the University executive. Any staff who provide non-deidentified personal data to a party that

has not agreed to one of the before-mentioned agreements, will be in breach of the ANU Code of Conduct.

3. Threshold Assessment

As personal information is stored and disclosed a PIA is required.

4. Consultation with Stakeholders

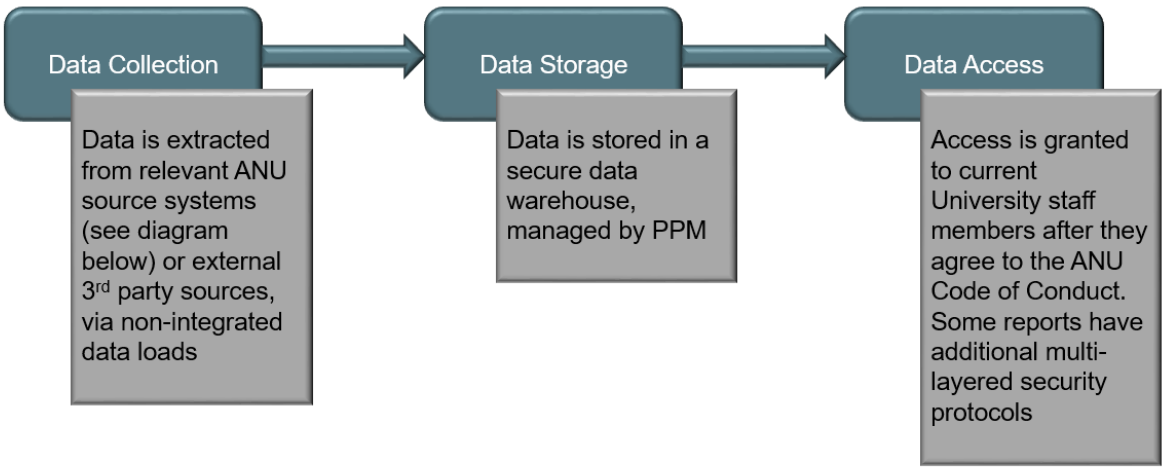
The Privacy Impact Assessment has been prepared consistent with the ANU Guideline: Privacy Impact Assessment. An amended version of this document is conducted for each sub-project that is undertaken on ANU Insight.

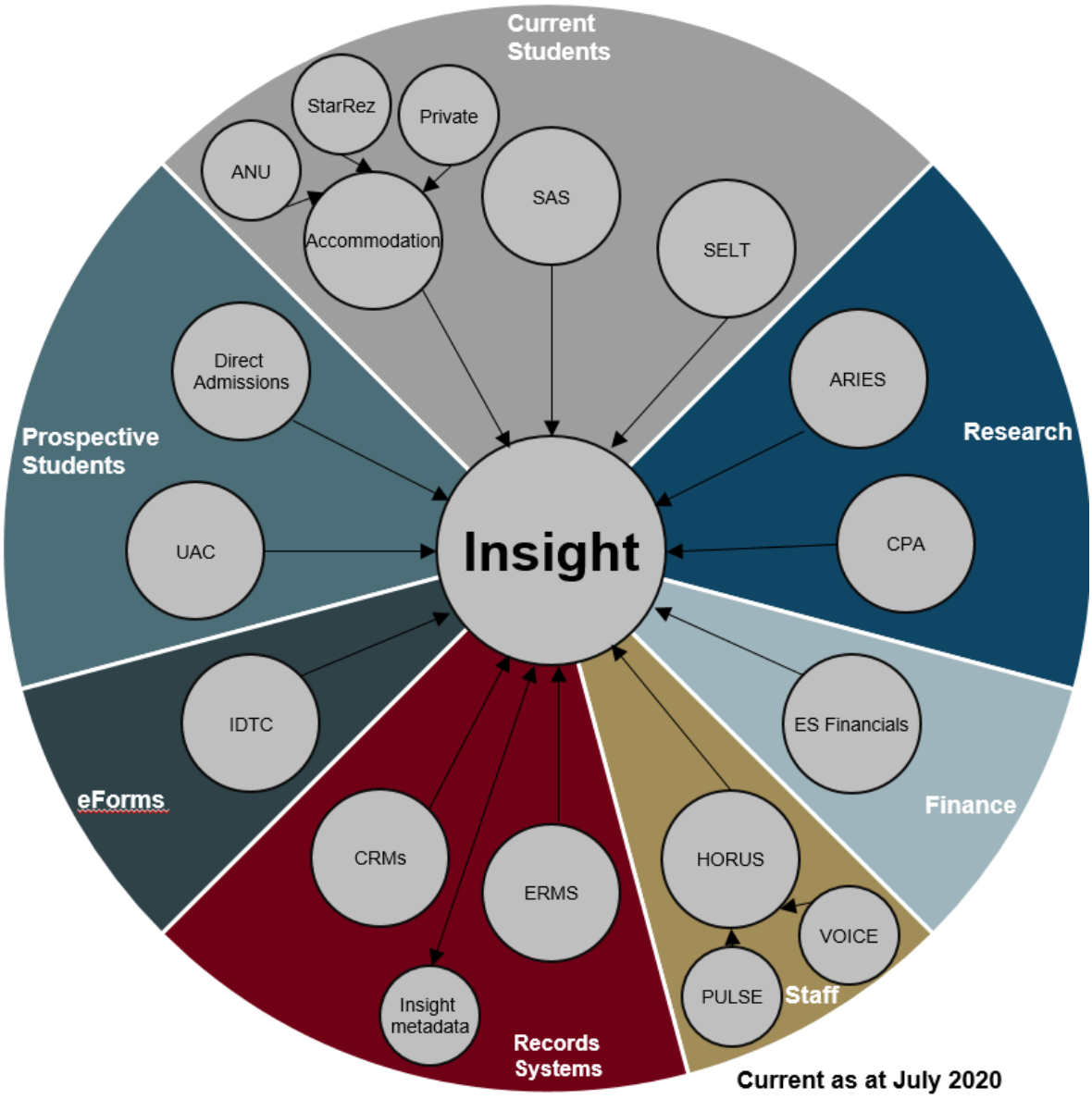
Prior to the acquisition of any new personal data from a source system, the R&A team conduct extensive consultation with:

- The relevant data custodians and their teams, to ascertain what previous consultation has been conducted.
- End users of the reports, to understand their requirements so that the least amount of personal information can be provided whilst still meeting the business need.

If there is an upgrade or new version of ANU Insight reporting suites, the Privacy Impact Assessment will be reviewed by PPM, and updated if required.

5. Information Flows





5.1 Data Collection

Data is collected from various source systems across the University, all of which should have their own respective Privacy Impact Assessment regarding how the data was collected.
The complete list of University source systems that ANU Insight receives a data flow from is (Effective July-2020):

- Human Resources Management System (HRMS)
- Enterprise Systems Financials (ES Financials)
- Student Administration System (SAS)
- ANU Research Information Enterprise System (ARIES)

- ANU Research Costing, Pricing and Approval Tool (CPA)
- Electronic Records Management System (ERMS)
- StarRez (Accommodation)
- University Admissions Centre (UAC)
- ANU Direct Admissions database (ANU Direct)
- Intelledox Digital Transformation Centre (eForms)
- Student Experience of Learning and Teaching database (SELT)
- VOICE Survey database (VOICE)
- Future Student Customer Relationship Manager (in-progress)
  Relationships and Engagement Customer Relationship Manager (future planned)
- ANU Insight users meta-data

The list of systems can increase due to Enterprise projects that also involve reporting requirements

5.2 Data Management

Storage

The data extracted from the source systems is stored in the ANU Data Warehouse. Access to the Data Warehouse is strictly for PPM staff only, and is available only once staff have completed orientation and training which includes the University privacy Pulse modules.

Access

Access to the ANU Insight system is managed by the R&A team which conducts regular system checks & audits to:

- Ensure staff who have left the University have their access removed in a timely manner
- Ensure no individuals are bypassing our access granting procedure
- In the case of prospective student information, an annual check in with end-users is conducted to ensure continued access is required

The majority of reports on ANU Insight require additional approval prior to users being able to see personal data. These generally require the user to fill out a user form for another source system, or for ANU Insight. Access to this data requires approval by the user's Divisional Director, College General Manager, College Dean, or higher.

Some reports on ANU Insight require additional documents such as a Declaration of Conflict of interest form to be completed before access is considered. If there is deemed to be a relevant conflict of interest, an access plan is established between the individual requesting access, and the Director PPM to ensure compliance.

Reports also contain various levels of access. For instance all individuals may be able to view a particular report, but will not be able to see personal information within that report unless they have obtained a higher permission level. Some other reports are not available to any given individual unless there are exceptional circumstances which warrant the use of the

report. In these circumstances, an individual may request access to the data subject to the Associate Director, R&A, and Director PPM agreeing to the access for a defined period of time.

Access to the ANU Insight system is protected by secure log-in via Single-Sign-On or University ID and Password. This allows R&A team members to conduct audit controls to ensure that our security model is working correctly.

Training

Training on how to use the system, which includes a section on the personal and sensitive data contained within the reports, and the user's obligations is provided upon request. Training documentation for each suite of reports, and for the system as a whole is available via the PPM website: https://services.anu.edu.au/information-technology/software-systems/insight
When training is conducted, all personal information is redacted unless everyone in attendance has access to the data already.

Accuracy

An individual can request that data be corrected if there is incorrect data by contacting insight@anu.edu.au which will pass the query on to the relevant source system to ensure that it is changed in the source systems. This is to ensure that ANU Insight & PPM align to the agreed ANU Data & Information Management Principles that have been communicated via the Digital Master Plan.

Nightly extract, load, transform (ETL) processes are checked by R&A staff each morning to ensure that the system has not malfunctioned in the collection of data from the source systems or due to outages. If an issue is found, the relevant steps to correct the data and the reports are taken. Automated processes are in place to support the rapid identification of such situations.

Disposal

Data is not disposed of within the Data Warehouse. The records may be archived if not in use, but are not destroyed as the Data Warehouse is a storage & aggregation system rather than a source system. The treatment of data updates (changes or disposals) in source systems will in part dictate how the Data Warehouse deals with the changes

6. Privacy Management

This section provides an analysis of how ANU Insight may impact upon privacy, both positively and negatively.

#	Privacy Impact	Necessity/Impact Rating/Impact Response	Impact treatment Plan

1	Personal data will be collected and stored in a secure data warehouse	Necessary/ Low/ Mitigate	Data is collected in a responsible way that is consistent with the ANU Privacy Policy and ANU Code of Conduct. Every reasonable precaution has been taken to ensure that no unauthorized access to the data occurs. The Data Warehouse will adhere to the source systems approach to the storage of personal data
2	Personal data will be updated and corrected if incorrect	Necessary/ Positive/ Encourage	Users are encouraged to look for discrepancies in the data and report any issues to the R&A team to ensure the most accurate data is available. Under the Digital Master Plan, this will be undertaken
3	Users may be surprised or upset by a secondary use or disclosure, resulting in privacy complains and/or negative publicity	Unlikely/ Moderate/ Mitigate	Use of ANU Insight data is on the provision that it is for approved University business only. No data should be given to any individual or organisation without first being de-identified, or without appropriate Non-Disclosure of Personal Information Agreements in place.
4	Individuals are not able to easily access their information	Necessary/ Moderate/ Mitigate	Due to system limitations, PPM is unable to provide access to all individuals who have their personal information within the system. If a request for information on what data regarding an individual is stored by the University is made, ANU Insight will comply in accordance with the ANU Privacy Policy.

7. Recommendations

The following table shows recommendations that should be considered for Insight in the future,

#	Recommendation	Urgency	Impact if not completed
1	Review the University's Digital Master Plan and associated Data & Information Management Principles, and incorporate any changes required by these documents	High	Risk of non-compliance with key ANU policies and procedures.
2	Implement a regular review of ANU Insight to ensure compliance with recommendations made by the Data	Medium	Risk of missing opportunities to remain operating in line with

	Governance Committee where applicable and actionable		industry standards of excellence.
3	No new data projects be incorporated into the Data Warehouse the source system having an active PIA in place at the ANU. If/When/Where source system are outside of the control/ownership of the ANU, then a PIA must be undertaken prior to commencement of any contracted work	High	Risk of misusing individual's personal data, or allowing unauthorised access to personal data.
4	Maintenance of an ANU Insight Operational Management folder on the PPM share drive that contains a governance protocol to store all relevant documents in a single source	Medium	Risk of missing key lessons learnt from other projects. Risk of becoming overly dependent on certain individuals with knowledge of policies, and privacy protocols.