Data and Information Classification Framework

Purpose

(1) The Data and Information Classification framework establishes a unified, university-wide approach for classifying and managing data at ACU. It replaces the previous framework to address inconsistencies and provide a single standard for academic, administrative, and research data. The framework distinguishes personal information from non-personal information, recognising that personal information is subject to distinct legal definitions and handling requirements that do not apply to other data types and that vary by jurisdiction.

(2) This framework provides guidance on how information and data will be classified in line with the ACU Data and Information Governance Policy and Procedure.

Scope and Application

(3) This framework applies to:

a. Everyone using Business Information (BI), Personal Information (PI) & Research data across ACU, including vendors, contractors & third-party service providers
b. All ACU data assets, whether digital or physical
c. All stages of the data lifecycle: creation, capture, access, use, storage, transmission, sharing, archival, and disposal

(4) This includes but is not limited to:

a. Enterprise information and ACU business records
b. Personal, sensitive, and confidential information
c. Research data and research-related information
d. Intellectual property and commercially sensitive information

Classification Decision Guidance

(5) When determining classification, consider:

a. Does the data contain personal or sensitive information?
b. Is the data subject to legal, regulatory, or ethical obligations?
c. What is the impact if the data is disclosed or misused?
d. Does the dataset combine multiple classifications?

Data and Information Classification Framework

Level	Classification	Business Information (BI Non-PI) Description	Personal Information (PI) Description	Default Access Requirements	Handling Requirements	Examples
1	Highly Sensitive	Highly sensitive commercial, legal, financial, or operational information requiring the highest level of protection, including legally privileged material and regulated institutional data, where unauthorised disclosure would cause serious legal, financial, or reputational harm to the University.	Sensitive personal information that needs extra care because the individual has little or no real choice about how it is used (cannot freely consent to or control) or because the context creates stronger limits or constraints on how the information can be handled.	Limited access provided to specified individuals based on their roles and having a specific and justifiable need to access and use the data. For BI, Authorized persons that have a specified requirement for the data/information as defined by legislation or regulatory requirement.	Transmit and Store only in restricted secure environments and business systems approved by ACU with mandatory logging, access reviews, encryption, and governance controls including Data Loss Prevention capabilities are active.	Highly sensitive information relating to commercial projects or matters. Personal Information examples include use in care, safeguarding, or support contexts, relating to individuals whose circumstances create vulnerability due to power imbalance, limited capacity to consent, or impaired decision-making; or subject to safeguarding requirements, or other constraints. Research data containing identifiable and/or re-identifiable personal data and/or health data including data related to vulnerable individuals or communities (such as persons under the age of 18 and First Nations people)

Level	Classification	Business Information (BI Non-PI) Description	Personal Information (PI) Description	Default Access Requirements	Handling Requirements	Examples
2	Sensitive	Commercially, strategically, or reputationally sensitive business information that is limited to specific roles or groups, where unauthorised disclosure could cause moderate harm or disadvantage to ACU, but is not subject to statutory or regulatory protection. Includes: commercial projects, financial and operational reporting at a business unit level, audit and review materials, management and planning documents.	Personal Information that may only be collected, used or shared for the specific purpose the individual consented to (or where the law allows), and must be protected more carefully than ordinary personal information.	Accessible only by an identified group of ACU staff within a defined access group (e.g., based on levels, roles, projects, or business units) and with a defined academic or business need. May include consultants or contractors (if directly required to deliver their services) who have signed a non-disclosure agreement (NDA) (or equivalent) using the approved ACU template.	Transmit and store only in ACU-approved secure business systems Mandatory encryption, logging, access reviews, and governance controls. Protections relative to data type and sensitivity.	BI relating to commercial projects or matters where disclosure could jeopardise the project or harm ACU's reputation or interests. Audit and review data. Financial data at a business unit level. Operational and management reporting data. Research data containing personal data other than identifiable and / or re-identifiable personal or health data or data on vulnerable people or communities. Sensitive Personal Information includes information about an individual's health (medical, dental, mental, disability, fitness, adjustments and reports, pharmaceutical, biometric in a health context, predictive genetic information), racial or ethnic origin, religious or philosophical beliefs, political opinions or associations, sexual orientation or practices, trade union or professional association membership, criminal record.

Level	Classification	Business Information (BI Non-PI) Description	Personal Information (PI) Description	Default Access Requirements	Handling Requirements	Examples
3	Internal	Operational, administrative, and reporting information intended for general use across ACU, where accidental disclosure would have low impact and is unlikely to cause material harm. This includes internal reports, campus and faculty data, and other non-commercially sensitive information. Includes: internal performance and activity reports, Data Hub dashboards, procedures, guidelines, and internal communications. May be shared with approved external partners to support approved business activities under appropriate controls like data sharing agreements, access restrictions.	Non-sensitive personal information used with the individual's consent or where the law allows, for routine organisational purposes by authorised staff with necessity (such as delivering services, managing employment or education, and providing systems and facilities). Normal protections apply.	Accessible by authorised ACU staff, contractors / consultants or other approved 3rd parties (where required) who have signed a non-disclosure agreement (NDA) or equivalent using the approved ACU template. Access to Personal Information by staff authorised in their role with necessity to access	Transmit and store only in ACU approved secure systems.	BI Internal reports that are not commercially sensitive or highly sensitive. Non-sensitive personal information including contact details (personal email, mobile number, address), employment information (ID, work history, job title), academic information (student ID, enrolment details, grades, comments), financial information (bank account or credit card numbers), demographic details (date of birth, non-sensitive gender or language preference), transactional data (service usage, logs)

Level	Classification	Business Information (BI Non-PI) Description	Personal Information (PI) Description	Default Access Requirements	Handling Requirements	Examples
4	Public	Business information approved for unrestricted public release, where there is no confidentiality, commercial, or reputational sensitivity concerns and no negative impact to ACU if disclosed. Includes: annual reports, public web content, marketing and promotional material, published statistics, and public-facing research outputs. Published, de-identified research datasets.	Personal information that has been explicitly approved for public release, either through individual consent or lawful authority, where there are no privacy or sensitivity concerns. Includes: staff names, titles, and contact details published on ACU websites, and other publicly authorised profiles or biographies.	Publicly accessible	Can be transmitted and stored using public websites, third party, shared services / repositories.	Examples include ACU Annual Reports, public web pages, marketing material and ACU Pocket Statistics. Published, de-identified research datasets.

Status and Details

Status	Current
Effective Date	18th March 2026
Review Date	18th March 2028
Approval Authority	Deputy Vice-Chancellor (Corporate)
Approval Date	2nd March 2026
Expiry Date	Not Applicable
Responsible Executive	Russell Parker Chief Information and Digital Officer
Responsible Manager	Pallavi Khanna National Manager, Data Excellence
Enquiries Contact	Information Technology