

Data and Information Governance Policy

Version 3 – Approved 3 July 2026



Purpose:

Effective management of information and cyber security enables the strategic objectives of the University to be met while managing risks and protecting systems and information from cyber threats. This policy outlines our commitment to responsibly manage risks, and safeguard systems and information in a way that controls and protects, while maximising the value of information in an ethical and compliant way and minimising the cost and risk of holding information.

		Approved by
1	Privacy	
1.1	The University will embed a culture of privacy that respects individual's rights.	Vice-Chancellor
1.2	The University will ensure contemporary privacy practices are used to govern the collection, management and use of personal information.	Vice-Chancellor
1.3	The University will ensure that data, which is collected and managed to assist evidence based organisational decisions, is only used in ways that respect the privacy of individuals.	Vice-Chancellor
1.4	The University will only share data with a partner organisation where it is clear when the information is requested that it can be used for these purposes and where the university is confident the partner organisation will meet the University's standards for the protection of privacy.	Vice-Chancellor
1.5	The University will act appropriately and respond diligently if there is a suspected breach of its privacy obligations, mitigating against any harm to staff, students and our stakeholders.	Vice-Chancellor
1.6	Disciplinary action may be taken where a privacy breach is found to be intentional.	Vice-Chancellor
1.7	The University may use personal information if it is needed to protect people from material threats to personal safety and wellbeing.	Vice-Chancellor
2	Cyber security	
2.1	The University will identify and manage cyber security risk to systems, assets, data, and capabilities.	Vice-Chancellor
2.2	The University will implement appropriate cyber security controls to protect the delivery of critical infrastructure services.	Vice-Chancellor
2.3	The University will maintain frameworks, plans and systems to identify the occurrence of cyber security events, respond to events and restore the capabilities or services.	Vice-Chancellor
2.4	Users of the University's information, communication and technology services and facilities will understand their cyber security obligations and report all cyber security incidents and events.	Vice-Chancellor
3	Information, communication and technology (ICT) services and facilities use	
3.1	University information, communication and technology services and facilities are for use by authorised users only and governed by appropriate controls.	Vice-Chancellor

3.2	University information, communication and technology services and facilities will be used in a manner that supports the University mission and values and may only be used for University business and limited appropriate personal use.	Vice-Chancellor
3.3	University information, communication and technology services and facilities are only for appropriate, legal and ethical use.	Vice-Chancellor
3.4	The University may, where appropriate, monitor and restrict the use of University's services and facilities.	Vice-Chancellor
3.5	The University will only allow authorised privately owned information, communication and technology devices to connect to University services and facilities.	Vice-Chancellor
3.6	Systems and applications will be designed, deployed, maintained and decommissioned according to their value and their confidentiality, integrity and availability requirements.	Vice-Chancellor
3.7	The University encourages the ethical, responsible, and sustainable implementation and use of technology, including artificial intelligence. Staff and students must ensure these technologies are used in a manner that protects privacy, promotes fairness, avoids harm and advances the common good.	Vice-Chancellor
4.	Artificial Intelligence (AI)	
4.1	(Use) The University's approach to AI is guided by considering whether the use of AI serves or diminishes the scholarly, creative and critical work that gives our University its distinctive purpose and public value.	Vice-Chancellor
4.2	(Innovation) The University encourages the use of AI for innovation across teaching and learning, research activities and professional services in accordance with the University AI Risk Appetites.	Vice-Chancellor
4.3	(Workforce) In accordance with principle 4.1, AI will be used to augment human expertise and creativity in a way that values human vision, expertise, reasoning and judgement. Where AI is used to inform or support decisions such as assessment, peer review, consulting or decisions that may affect an employee's working conditions, the final decision must be made by a staff member accountable for the outcome as a delegate.	Vice-Chancellor
5	Data and Information management	Vice-Chancellor
5.1	The University will ensure appropriate governance for management of data and information that is consistent with regulatory, legal, risk, environmental and operational requirements.	Vice-Chancellor
5.2	The University classifies data and information according to sensitivity and risk and applies governance, controls and permissible uses proportionate to that classification.	Vice-Chancellor
453	The University will ensure that data and information, recognised as an asset, is available for use and reuse where appropriate.	Vice-Chancellor
5.4	University staff will ensure that information is created and captured to support all university functions and activities.	Vice-Chancellor

5.5 Members of the University community will ensure that data and information is appropriately stored, accessed, shared, preserved and disposed of protecting it from loss and unauthorised access.

Vice-Chancellor

Definitions and acronyms: [Information](#)

3 July 2026 *Once printed this is an uncontrolled document:* [Version history](#)

All University community members must comply with all relevant laws and regulations, University By-Laws, ordinances, policies and procedures.