Data and Information Governance Policy

Version 1 – 25 September 2020

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.

1	**Privacy**	**Responsible**
1.1	The University will embed a culture of privacy that respects individual's rights.	Chief Operating Officer
1.2	The University will ensure contemporary privacy practices are used to govern the collection, management and use of personal information.	Chief Operating Officer
1.3	The University will ensure that data, which is collected and managed to assist evidence based organisational decision, is only used in ways that respect the privacy of individuals.	Chief Operating Officer
1.4	The University will only share data with partner organisation where it was clear when the information was originally obtained that it could 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.	Chief Operating Officer
1.5	The University will act appropriately and respond diligently if there is a suspected breach of privacy obligations, mitigating against any harm to staff, students and our stakeholders.	Chief Operating Officer
1.6	Disciplinary action may be taken where a privacy breach is found to be intentional.	Chief Operating Officer
1.7	The University may use personal information if it is needed to protect people from material threats to personal safety and wellbeing.	Chief Operating Officer
2	**Cyber security**	
2.1	The University will identify and manage cyber security risk to systems, assets, data, and capabilities.	Chief Operating Officer
2.2	The University will implement appropriate cyber security controls to protect the delivery of critical infrastructure services.	Chief Operating Officer
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.	Chief Operating Officer
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.	Chief Operating Officer
3	**Information, communication and technology 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.	Chief Operating Officer

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.	Chief Operating Officer
3.3	University information, communication and technology services and facilities are only for appropriate, legal and ethical use.	Chief Operating Officer
3.4	The University may, where appropriate, monitor and restrict the use of University's services and facilities.	Chief Operating Officer
3.5	The University will only allow authorised privately owned information, communication and technology devices to connect to University services and facilities.	Chief Operating Officer
3.6	Systems and applications will be designed, deployed, maintained and decommissioned according to their value and their confidentiality, integrity and availability requirements.	Chief Operating Officer
4	**Data and Information management**	
4.1	The University will ensure appropriate governance for management of data and information that is consistent with regulatory, legal, risk, environmental and operational requirements.	Chief Operating Officer
4.2	The University will ensure that data and information, recognised as an asset, is available for use and reuse where appropriate.	Chief Operating Officer
4.3	University staff will ensure that information is created and captured to support all university functions and activities.	Chief Operating Officer
4.4	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.	Chief Operating Officer

---

Definitions and acronyms: Information

25 September 2020 *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.