

Senior Manager, Information Governance & Privacy

HEP Level 9

POSITION NUMBER	954523
ORGANISATIONAL UNIT	Business Intelligence
POSITION REPORTS TO	Executive Director Business Intelligence
OVERALL PURPOSE	<p>The Information Governance and Privacy Officer is a key member of the Business Intelligence team, providing expert guidance and strategic support across the University to strengthen privacy awareness, compliance, and best practices in Information and Data Governance—including Indigenous Data Sovereignty.</p> <p>This role champions the implementation and continuous improvement of enterprise-wide governance and privacy frameworks, ensuring policies and procedures under the VU Information and Data Governance Framework are effectively embedded and operational. As the designated Privacy Officer, the role responds to privacy-related enquiries, complaints, and incidents with accuracy and efficiency, while proactively driving improvements in privacy practices across the University</p>
ORGANISATIONAL CONTEXT AND RELATIONSHIPS	<p>Within the University the position:</p> <ul style="list-style-type: none"> ◆ Works closely with the General Counsel and Legal Services, CFO Portfolio, and Digital and Campus Services to enact governance principles. ◆ Works collaboratively across the University's academic and professional units to embed a culture of information and data governance excellence in University operations. ◆ Works closely with VU's Indigenous Academic Unit, Moondani Balluk, to align Information, Data, and Privacy policies and operations with Indigenous Data Sovereignty best practice. <p>Outside the University the position liaises with:</p> <ul style="list-style-type: none"> ◆ The Indigenous Data Network (IDN), National Indigenous Australians Agency (NIAA), National Aboriginal Community Controlled Health Organisation (NACCHO), and any other relevant peak bodies. ◆ Office of the Victorian Information Commissioner and Office of the Australian Information Commissioner, Australian Cyber Security Centre, and other external regulators as required.
LOCATION/CAMPUS	The position is currently located at the Footscray Park Campus of the University. The position and incumbent may be relocated to any other existing or future University work locations where it conducts its operations.

People and Culture use only

KEY CAPABILITIES

Victoria University is committed to building core capability across VU through investment in our staff, our systems and our processes. We will develop the capabilities of our staff to:

Deliver – Excellence Results-driven, accountability, problem solving focus.

Engage – Customer service mind-set internally, externally and particularly for students.

Collaborate and Partner – Build successful relationships, communicate effectively, influence and negotiate.

Innovate – Entrepreneurship, growth, continuous improvement, digital transformation.

Lead – Inspire direction, lead change, manage and develop people.

OUR ORGANISATION

Victoria University (VU) is a dual sector (higher education and TAFE) tertiary institution based in Melbourne, Australia. VU has academic colleges, each covering a broad discipline of study, and several research institutes and research centres. The University has campuses in Melbourne's CBD and western region, and a campus in Sydney and Brisbane. It also offers courses at partner institutions throughout Asia. Over 40,000 students, including around 14,000 international students, study VU courses worldwide. In 2016, VU celebrated its 25th anniversary as a university, which also marked its 100 years as an educational institution.

ORGANISATIONAL UNIT

Business Intelligence is part of the Portfolio of the Chief Financial Officer. The portfolio leads and manages financial and information services across the university, providing advice and services to deliver VU's strategy and optimise operations, including Data Governance and Insights, Finance, Legal Services, Procurement & Business Operations and Risk.

Business Intelligence is VU's trusted advisor for data and analytics and is responsible for ensuring VU's data assets maintain a high level of integrity and relevance. It encompasses:

- ◆ Business Intelligence Solutions Team, responsible for collecting, managing and governing the university's data assets, data warehouse and platforming, collaborating closely with Digital and Campus Services, Performance Business Partners, Data Insights and Surveys Team to ensure data assets are fit for purpose;
- ◆ Data Insights and Surveys Team, responsible for research, analytics and reporting; collecting, analysing and reporting student feedback, including external QILT surveys; and collaborating with BIS to develop and govern VU's data assets.
- ◆ Performance Business Partners Team, responsible for working with VU leaders to understand their business challenges, opportunities and priorities to improve performance and undertake load and fee planning functions.

By providing enterprise-wide data analysis, forecasting, market data, student surveys, predictive analytics, data visualisation, reports, presentations and recommendations, the Business Intelligence team deliver strategic level, critical information that helps the University succeed in a competitive environment. It is accountable for producing fit-for-purpose user-friendly reports that create insights to support senior

stakeholders to make informed, timely management decisions.

The teams possess a deep understanding of the ways information is collected, organised, governed and displayed to maximise strategic insights for decision-makers, and to ensure data privacy and data security, deliver on VU's Data Principles.

MAJOR TASKS AND ACCOUNTABILITIES

- ◆ Provide authoritative and forward-looking advice on domestic and international privacy and data protection legislation, ensuring the University meets its compliance and regulatory obligations.
- ◆ Lead the finalisation, implementation, and continuous improvement of Victoria University's Information and Data Governance Framework, ensuring it reflects best practice and includes principles of Indigenous Data Sovereignty.
- ◆ Drive the effectiveness of the Data Governance Committee by implementing robust oversight mechanisms that monitor key data practices, assess risks, and ensure strategic alignment across the University.
- ◆ Lead the development and execution of a privacy program working collaboratively across the University to implement a comprehensive privacy framework that defines responsibilities, safeguards personal information, ensures compliance, and actively reduces the risk of privacy breaches.
- ◆ Serve as the primary contact for all internal and external privacy enquiries, complaints, and requests for access to personal information, ensuring timely, accurate, and compliant responses in alignment with legislative and policy requirements.
- ◆ Develop and implement mitigation and incident management plans to address the broader strategic, reputational, and operational risks associated with privacy and data protection, using influence and persuasion in the provision of expert advice to senior University staff, to achieve outcomes in the best interest.
- ◆ Lead with innovation in the design, development and management of a Privacy Impact Assessment (PIA) process and related policies, to assist VU staff who are undertaking a PIA for new projects involving personal information.
- ◆ Ensure VU's compliance with privacy and data policies and procedures, and other relevant legislative and policy requirements applicable within the tertiary education system.
- ◆ Design and deliver targeted resources and training programs that empower University leaders to confidently manage privacy and data responsibilities within their areas, building capability and embedding a culture of accountability and best practice.
- ◆ Manage privacy breaches, risks, controls, and initiatives, ensuring regular reporting to senior leadership and the governance team.
- ◆ Work with other information management areas to identify gaps in accountability or capability and provide expert, strategic advice to address them—driving coordinated action with stakeholders to mitigate risks and strengthen governance.
- ◆ Adhere to and cooperate with all OH&S policies and procedures of the University.

TYPICAL/MAJOR CHALLENGES

- ◆ Cultivating consistent privacy awareness and data stewardship across diverse university departments, each with varying levels of capability and engagement, requires persistent leadership and tailored capability-building strategies.
- ◆ Coordination and implementation of competing priorities with digital, legal, academic, and administrative units to implement governance frameworks and privacy initiatives..
- ◆ Interpreting and advising on privacy and data governance principles, while enabling academic and administrative units to operate efficiently.

LEVEL OF SUPERVISION

Operates under broad direction from the Executive Director Business Intelligence and will be required to manage other administrative, technical and/or professional staff.

PROFESSIONAL AND ORGANISATIONAL KNOWLEDGE

- ◆ Information Management and Governance – Demonstrated understanding of data stewardship, quality, metadata, and lifecycle management within a university context.
- ◆ Demonstrates expert knowledge of privacy legislation and compliance obligations, applying this understanding to shape policy and guide institutional practice.
- ◆ Applies strategic insight into enterprise systems and data architecture to embed governance principles and ensure consistent, organisation-wide implementation of privacy and data frameworks.

KEY SELECTION CRITERIA

1. Knowledge or Training equivalent to: Postgraduate qualifications and extensive relevant experience; or extensive management experience and proven management expertise; or an equivalent combination of relevant experience and/or education/training.
2. Demonstrated capacity to conceptualise, develop, implement and review the application of significant frameworks and policies as related to Information and Data Governance, and Privacy.
3. Good understanding of and experience in the application of domestic and international data and privacy policies and procedures, and other relevant legislative and policy requirements applicable to tertiary education.
4. Demonstrated knowledge of Aboriginal and Torres Strait Islander communities and histories, and proven experience working respectfully and effectively with Aboriginal and Torres Strait Islander peoples, organisations or peak bodies, and with applied Indigenous Data Sovereignty Frameworks.
5. High-level management, administrative, organisational skills and experience in managing enquiries, complaints and supporting committees.
6. Excellent relationship management and consulting skills with demonstrated ability to develop effective strategic relationships with key stakeholders and colleagues, including the ability to influence at senior levels.
7. Demonstrated ability to integrate knowledge of internal and external regulatory requirements with

operational requirements and objectives of a large organisation with a diverse range of functions.

8. Demonstrated ability to design and deliver enterprise-wide change and capability improvement.
9. Sound understanding of and demonstrated experience in the implementation of evidence-based targets and measures, and ability to meet relevant legislative and policy requirements as needed.
10. Demonstrated capacity to understand and comply with employer policy and practices in all aspects of work and conduct, including OH&S and Anti-Discrimination responsibilities and complete/attend relevant training.

Desirable

1. Strong understanding of the tertiary education sector, including its regulatory environment, operational structures, and strategic priorities.
2. Experience in implementing enterprise-wide data governance or privacy initiatives within a complex organisational environment.

Organisational Chart

