

Job Description



Position Title	Privacy Officer	Level	C
Reports to (role)	Chief Operating Officer	Career Stream	Professional
Team	COO team		
Location	The Kids Research Institute Australia, Perth Children's Hospital, 15 Hospital Ave, Nedlands		

PURPOSE OF POSITION

The Privacy Officer is responsible for establishing, implementing and continuously improving The Kids' enterprise privacy framework, ensuring the Institute manages all sensitive personal, health, child and research participant, partner, donor and commercial information lawfully, ethically and responsibly across research, clinical, education and corporate activities.

The role provides expert privacy advice, develops governance frameworks and practical guidance, leads privacy risk assessment and incident management and privacy by design practices, and works collaboratively across the Institute to support research, innovation, AI adoption, data sharing and information management while maintaining compliance with privacy, research governance and regulatory obligations.

The role acts as the Institute's primary privacy subject matter expert and works closely with Research Governance, Legal, Data Governance, Cyber Security and Executive stakeholders to promote responsible information stewardship and privacy maturity across the organisation.

KEY RESPONSIBILITIES

Key Responsibilities	Tasks required to achieve Key Responsibilities	Measures
Privacy, Governance & Compliance	- Develop and maintain the Institute's privacy management framework, policies and procedures. - Monitor compliance with privacy legislation and organisational obligations. - Provide reporting and recommendations to Executive on privacy risks and emerging issues.	- Privacy governance framework, policies and procedures are in place. - Legislative and organisational privacy obligations are met. - Timely reporting on privacy risks, compliance and emerging issues.
Advisory & Risk Management	Provide expert privacy advice across research, corporate and operational activities.	Practical, timely and risk-based privacy

	• Lead Privacy Impact Assessments for new projects, systems and initiatives. • Coordinate privacy complaints, privacy enquiries, access requests and correction requests. • Support interactions with regulatory bodies where privacy issues arise. • Lead privacy breach assessment processes including recommendations regarding notification obligations. • Develop and maintain privacy incident response procedures and playbooks.	advice is provided across the Institute. • Privacy Impact Assessments are completed for initiatives. • Privacy incidents are managed in accordance with legislative and organisational requirements.
Research & Information Governance	• Provide privacy advice regarding human research, including consent, waiver of consent, secondary use of data, data linkage activities, registries, genomics, biobanks and clinical research activities. • Advise on privacy requirements throughout the research data lifecycle including collection, storage, access, sharing, retention, archival, disposal, de-identification and re-identification risk management. • Support privacy governance relating to cross-institutional collaborations, research partnerships and international data sharing arrangements. • Provide guidance on privacy risks associated with the use of AI, machine learning, large language models, digital health technologies and emerging research platforms. • Maintain a high-level register of personal information across the Institute.	• Privacy principles are embedded into research and operational activities. • Impact assessments are completed for applicable initiatives. • Incidents are managed in accordance with legislative and organisational requirements.
Stakeholder Engagement & Capability	• Build strong relationships across the Institute to embed good privacy practices. • Develop training, guidance and practical tools to improve organisational capability. • Promote a culture of responsible information management.	• Privacy awareness and capability is strengthened across the Institute • Training materials are developed and maintained.
Continuous Improvement & Strategic Leadership	• Monitor legislative and regulatory changes and recommend improvements. • Identify emerging privacy risks and opportunities. • Lead continuous improvement initiatives that strengthen the Institute's privacy maturity and governance framework. • Maintain awareness of WA Health privacy requirements, PRIS reforms, data linkage requirements and relevant public-sector information-sharing frameworks. • Provide advice to Executive on the organisational implications of emerging privacy, data governance and AI regulation.	• Emerging risks, legislative changes and industry trends are monitored and addressed. • The Institute maintains appropriate awareness of external privacy developments. • Continuous improvements are implemented to strengthen privacy maturity.

	Identify opportunities to enhance organisational privacy maturity and capability	
Workplace Safety	- Take reasonable care for your own safety and health and avoid harming the safety and health of others through any act or omission at work. - Identify and assess workplace hazards and apply hazard controls. - Report every workplace injury, illness or near miss, no matter how insignificant they seem. - Abide by Institute policies and procedures.	- Responsibilities are embedded in work practices. - Hazards are effectively managed or reported. - Accidents and incidents are reported in a timely manner. - All applicable safety policies and procedures are sought.

ESSENTIAL CRITERIA

Qualifications:	Bachelor's degree in law, Business, Information Management, Health Information Management, Governance, Risk or another relevant discipline, or an equivalent combination of qualifications and experience.
Essential Skills, Knowledge & Experience:	- Demonstrated experience in privacy, governance, risk or information management with an understanding of privacy obligations within research, health, higher education or similarly regulated environments. - Demonstrated experience advising on health information, sensitive information, research participant information or regulated data environments - Strong knowledge of the Privacy Act, Australian Privacy Principles and privacy governance. - Experience developing organisational policies, frameworks and governance processes. - Experience conducting Privacy Impact Assessments and privacy risk assessments. - Demonstrated ability to provide strategic advice to senior leaders and stakeholders. - Excellent written communication skills, including policy development and reporting. - Strong stakeholder engagement and influencing skills with ability to work effectively across Research Governance, Data Governance, Legal, Cyber Security and operational teams. - Ability to interpret legislation and translate it into practical organisational guidance.
Desirable Skills, Knowledge & Experience:	- Knowledge of WA Health privacy frameworks, data linkage environments and PRIS reforms. - Experience with Aboriginal and Torres Strait Islander data governance or Indigenous Data Sovereignty frameworks. - Familiarity with AI governance, machine learning, digital health platforms or advanced research data environments. - Privacy certification such as CIPP/E, CIPM or equivalent - Experience in health, research, higher education or government. - Knowledge of research governance, ethics or clinical research. - Knowledge of AI governance and information management.

DIRECT REPORTS	0
-----------------------	---

Approved by:	Chief Operating Officer
Date approved:	15 July 2026
Reviewed by P&C:	15 July 2026