

## Job Description

<b>Information Governance Officer</b>	
<b>Grade</b>	7
<b>Department</b>	Information Governance
<b>Overall Purpose</b>	
<p>The position of Information Governance Officer (IGO) is a business and technology focused role which requires ambition &amp; focus to drive through the transformation required by an evolving institution against a background of increasing competition, globalisation and rapidly evolving threat horizon, especially in the Information Security space.</p> <p>The Information Governance Officer (Technical) plays a critical role in supporting the delivery of strategic digital transformation programmes across the University, with a particular focus on initiatives such as Future Foundations combined Finance and HR system and Identity and Access Management (IAM).</p> <p>This fixed-term role provides dedicated technical information risk governance capacity for high-priority programmes, ensuring that information security, data protection and records management requirements are embedded into system design, implementation, and operation.</p> <p>Operating at the intersection of information security, data protection, and digital services, the role focuses on assessing and mitigating risks associated with large-scale system change, identity services, and complex data processing environments.</p> <p>The postholder will provide assurance through the assessment of Information Governance Risk Reviews (Screening, Decommissioning, Technical reviews, information Security contract reviews), the provision of system-level guidance to enable secure, compliant, and scalable digital solutions.</p> <p>The role contributes to the development and application of the University's Information and Privacy Assurance Frameworks, ensuring that governance controls are proportionate, risk-based, and aligned with regulatory, contractual and institutional requirements.</p> <p>The role focuses on risk-based decision-making, system-level assurance, and the creation of clear, defensible governance outputs that support audit and regulatory requirements Using a combination of professional expertise and advanced digital tools, including Microsoft Copilot and governance platforms such as OneTrust and The role will also focus on supporting wider Information Governance work with expert support, guidance and training to Faculty, Professional Services &amp; Cultural institutes leadership.</p>	
<b>About the Team</b>	
<p>The Information Governance Officer (Technical) role sits within the Information Governance Office, part of the Directorate of Compliance and Risk, and works closely with IT Services and Research Governance to deliver effective Information Governance assurance across systems and programmes.</p> <p>Key relationships</p>	

## Job Description

- Head of Information Security
- Head of Information and Privacy Assurance
- Head of Data Protection
- Data Protection Officer (DPO)
- IT Services (including CISO function; Security Architecture, Identity and Access Management, Security Operations, Digital & Data Hub teams and Enterprise and Business Architecture team)
- Strategic Programme and Project Leads (e.g. Future Foundations, IAM)
- Research Governance, Ethics and Integrity

### How the team works

The Information Governance Officer team operates within the Information Governance Office team, working collaboratively with IT Services, including the CISO function and Security Architecture, to ensure that Information and Privacy Assurance Frameworks are applied effectively across system design, implementation, and programme delivery.

### Key Accountabilities

#### Strategic programme support and technical assurance

- Provide dedicated information governance support to strategic programmes, including Future Foundations and Identity and Access Management (IAM).
- Contribute to programme governance by identifying, assessing, and mitigating risks associated with data processing, identity systems, and digital transformation.
- Ensure that Records Management and Information and Privacy Assurance are assessed within project initiation, design, delivery, and change processes.
- Collaborate with programme teams and IT Services (including Security Architecture and the CISO function) to ensure governance, security, and architectural requirements are integrated and delivered cohesively.

#### Technical assurance, systems, and risk management

Provide ongoing support to all leadership and project managers to ensure that each project is risk assessed in accordance with the Information Governance “project gating” process.

Lead and deliver Information Governance Risk Reviews (IGRRs) for systems and services within programme scope.

- Assess system architectures, identity models, access controls, and data flows, identifying risks and recommending proportionate mitigations.
- Provide expert input into IAM solutions, identity lifecycle management, and access governance, ensuring alignment with Information Security and Records Management policy, legislation, and assurance frameworks.
- Work closely with IT Services, including the CISO function and Security Architecture, to ensure that

## Job Description

information governance requirements are aligned with system design and security principles.

- Provide input into system and security design decisions, ensuring that privacy, data protection, and governance controls are embedded proportionately.
- Ensure alignment between Information and Privacy Assurance Frameworks and IT Services security and architecture standards, supporting a coherent and risk-based approach to system assurance.
- Support the development, application, and continuous improvement of the University's Information Governance across strategic initiatives.

### Data governance, classification, and lifecycle management

- Advise on implementation of data classification, retention, and sensitivity labelling, particularly within M365 (Purview), Faculty, School and Professional Services and Teaching and Learning and related activities.
- Ensure that data security, minimisation, retention, and lawful processing principles are embedded into new and evolving systems.
- Support programme teams to design solutions that align with data governance policies, standards, and assurance frameworks.

### Decision-making, analysis, and digital tooling

- Apply expert, risk-based judgement in complex technical scenarios involving identity systems, large datasets, and new technologies.
- Use digital tools, including Microsoft Copilot, to support analysis of system documentation, processing activities, and governance artefacts.
- Critically assess and validate outputs from digital tools, ensuring that decisions remain accountable and evidence-based.
- Produce structured, defensible documentation to support programme governance, audit, and regulatory compliance.

### Advice, collaboration, and continuous improvement

- Provide clear, practical advice to programme teams and stakeholders on data protection, information security, and data governance requirements to support compliant system design and delivery.
- Work collaboratively with IT Services, including Security Architecture and CISO-led functions, to ensure governance controls are effectively implemented.
- Contribute to the development of tools, templates, and guidance to improve the consistency, efficiency, and auditability of technical assurance activities.
- Ability to assess existing processes, suggest improvements, and work with others to enhance operational effectiveness to support the wider University.

### Person Specification

Knowledge

**Application of data protection and information governance principles in**

## Job Description

	<p>system and programme contexts; and core concepts of identity, access, and data lifecycle management.</p>
Experience	<p><b>Experience of applying data protection and information governance principles in technical or system-based environments</b></p> <p><b>Experience of supporting or delivering DPIAs, risk assessments, or assurance activities</b></p> <p><b>Experience of working with digital transformation programmes, IT systems, or identity/access services</b></p> <p><b>Experience of working in a regulated environment with complex priorities</b></p>
Skills	<p><b>Strong analytical skills in relation to system design, identity management, and data flows</b></p> <p><b>Ability to interpret legislation and apply it in technical and programme delivery contexts</b></p> <p><b>Ability to produce clear, structured, and defensible governance outputs</b></p> <p><b>Ability to engage effectively with IT Services, including Security Architecture and CISO-led functions, translating governance requirements into practical system considerations</b></p> <p><b>Strong stakeholder engagement skills across IT and programme environments</b></p> <p><b>Ability to use digital tools, including Microsoft Copilot, to support analysis while retaining accountability</b></p> <p><b>ComTIA in networking, computing, AI or similar certificate or equivalent experience</b></p>
Education	<p><b>ComTIA in networking, computing, AI or similar certificate or equivalent experience.</b></p>
Other	<p><b>Advanced knowledge of Information and Privacy Assurance Frameworks-</b></p> <p><b>Practical experience in IAM, M365 governance, and enterprise data platforms</b></p> <p><b>Knowledge of data protection or freedom of information legislation gained through experience, training, or qualifications such as the BCS Data Protection Certificate, IAPP CIPP/E, or equivalent</b></p>
<p><b>Key Behaviours</b></p>	
<p><b>One University:</b> A ‘One University’ approach, whereby we break down silos and work collaboratively towards furthering the University’s strategic goals, vision and values.</p> <p><b>Freedom of Speech and Academic Freedom:</b> Support the University’s commitment to securing and actively promoting the importance of free speech and academic freedom within our community.</p>	

## Job Description

**Service Excellence:** Committed to prioritising service excellence and high performance to deliver great people-centred experiences.

**Agility:** Demonstrate a commitment to agility and continuous improvement by embracing change, championing innovation, and being flexible and forward thinking to adapt.

**Sustainability:** A sustainable approach that safeguards the University of the future by championing environmental practices, advancing digital capability, and supporting financial stability and philanthropic initiatives.

**Inclusion:** Support the University's ambition to create an inclusive place to work where every person matters, demonstrating a commitment to non-discriminatory conduct and respect for others, and fostering a University where people feel deeply connected to each other, to Manchester, and to the wider world.

**Social Responsibility:** Promote and champion the University's social responsibility ambitions to advance social inclusion, prosperous communities, better health, and cultural engagement.