



Job title	Senior Information Compliance Officer	Job family and level	Administrative, Professional and Managerial Level 5
School/ Department	Registrars Department (Information Security and Compliance)	Location	University Park Campus

Purpose of role

The University continues to strengthen its data protection and information security framework in response to evolving regulatory requirements and digital transformation. The University are enhancing our approach to privacy management, information governance, and regulatory compliance. The Information Compliance function plays a vital role in ensuring the University maintains the highest standards of data protection while enabling innovation and operational excellence. This role supports the delivery of the University's Information Compliance Strategy and promotes a culture of privacy by design.

This role offers an opportunity to develop a career in Information Security and Compliance within the Registrar's department, contributing to the delivery of the University's compliance and governance objectives.

The Senior Information Compliance Officer will work collaboratively across the institution to embed privacy management and information governance practices. They will support departments in meeting their obligations under UK GDPR, DPA 2018, and related legislation while enabling effective data use for education, research, and administration.

	Main responsibilities (Primary accountabilities and responsibilities expected to fulfil the role)	% time per year
1	<p>Privacy and Information Compliance</p> <ul style="list-style-type: none"> ▪ Lead the maintenance and development of the Information Asset Register and Register of Processing Activities (ROPA) ▪ Review and update Privacy Notices to ensure accuracy and transparency ▪ Conduct Privacy Impact Screening and Assessments to support the use of new technology and research projects ▪ Assess legitimate interests and other legal bases for processing ▪ Review supplier due diligence responses and data processing agreements ▪ Support privacy-enhancing technology initiatives ▪ Monitor regulatory changes and update compliance frameworks accordingly ▪ Coordinate with Digital Technology Services on IT Security privacy-related controls and requirements 	45%

	<ul style="list-style-type: none"> ▪ Provide support and guidance to the Information Compliance Officers around information compliance matters such as Freedom of Information Act requests, SARs, and Information Rights Requests ▪ Support and/or deputise for the Data Protection Officer in delivering strategic advice and guidance around information compliance matters 	
2	<p>Information Compliance Advice and Guidance</p> <ul style="list-style-type: none"> ▪ Provide expert guidance on data protection matters to staff at all levels ▪ Support the interpretation of complex privacy requirements ▪ Act as escalation point for challenging compliance queries ▪ Guide departments on privacy by design implementation ▪ Create and maintain privacy procedures and guidance ▪ Develop templates and tools for privacy management supporting compliance reporting and metrics ▪ Document privacy decisions and rationale ▪ Maintain records of privacy advice provided ▪ Undertake privacy audits and assessments 	30%
3	<p>Incident Management</p> <ul style="list-style-type: none"> ▪ Lead on and manage data breach response procedures ▪ Support breach investigations and documentation ▪ Assist with breach notifications when required liaising directly with the Information Commissioner's Office ▪ Maintain the breach register and identify trends 	10%
4	<p>Training and Awareness</p> <ul style="list-style-type: none"> ▪ Deliver targeted privacy awareness sessions in-person and virtually ▪ Develop role-specific training materials ▪ Create practical guidance for common privacy scenarios ▪ Support privacy champions across departments 	10%
5	<p>Professional Development</p> <ul style="list-style-type: none"> ▪ Maintain current knowledge of privacy laws and regulations ▪ Follow developments in privacy technology and practices ▪ Participate in relevant professional networks ▪ Share knowledge with the wider team 	5%

Person specification

	Essential	Desirable
Skills	<ul style="list-style-type: none"> ▪ Excellent interpersonal and communication skills (both oral and written) including report writing, drafting and presentation skills. ▪ Demonstrate ability to take ownership of challenging situations and to function independently as well as part of a team. ▪ Ability to effectively communicate clear and practical advice on data protection and information security related matters/policies with the ability to handle sensitive and confidential issues effectively and to non-technical stakeholders. ▪ Competent analytical and problem solving abilities. ▪ Willingness to be flexible and ability to prioritise and to deliver to targets. ▪ Advanced proficiency in the Microsoft suite and excellent data management. 	<ul style="list-style-type: none"> ▪ Evidence of taking up development opportunities in the work/study environment ▪ Knowledge of security standards including ISO 270001 and Cyber Essentials. ▪ Knowledge of IT Security controls such as : <ul style="list-style-type: none"> ○ Access Control ○ Security Monitoring ○ Vulnerability Mgt ○ Penetration Testing ○ Data Loss Prevention ○ Internet & Email Security
Knowledge and experience	<ul style="list-style-type: none"> ▪ Significant experience of Data Protection gained over several years within large or complex organisations. ▪ Strong demonstrable knowledge of FOIA gained over several years. ▪ Experienced in communicating and influencing senior management in relation to data protection issues and risks. ▪ Demonstrable relationship building and management experience. ▪ Experience of managing large workloads, delivering on time and to a high quality. 	<ul style="list-style-type: none"> ▪ Familiar with or have worked within High Education.

<p>Qualifications, certification and training (relevant to role)</p>	<ul style="list-style-type: none"> ▪ Degree or equivalent qualification or a proven track record of relevant work experience. ▪ Data Protection Qualification 	<ul style="list-style-type: none"> ▪ Freedom of Information Qualification ▪ Certificate in Information Security Management Principles



Expectations and behaviours

The University has developed a clear set of core expectations and behaviours that our people should be demonstrating in their work, and as ambassadors of the University's strategy, vision and values. The following are essential to the role:

- Valuing people** Is always equitable and fair and works with integrity. Proactively looks for ways to develop the team and is comfortable providing clarity by explaining the rationale behind decisions.
- Taking ownership** Is highly self-aware, looking for ways to improve, both taking on board and offering constructive feedback. Inspires others to take accountability for their own areas.
- Forward thinking** Driven to question the status quo and explore new ideas, supporting the team to "lead the way" in terms of know-how and learning.
- Professional pride** Sets the bar high with quality systems and control measures in place. Demands high standards of others identifying and addressing any gaps to enhance the overall performance.
- Always inclusive** Ensures accessibility to the wider community, actively encouraging inclusion and seeking to involve others. Ensures others always consider the wider context when sharing information making full use of networks and connections.

Key relationships with others

This is a Smart Art diagram. Click on the boxes to enter the role holder's job title, line manager's job title and any direct reports (if applicable). If a role does not have any direct reports, remove this box by double clicking on it and pressing Delete.

****Please remove this paragraph of instructions before submitting the role profile****



