Post Title:	Head of IT Compliance
Grade:	9

2. Job Description

2.1. Purpose

The Head of IT Compliance will take responsibility for ensuring that IT products, services, contracts and systems are compliant with relevant legislation, licence requirements and Group policies and procedures.

They will carry out risk assessments and internal audits of all IT products and services both in IT services and also across the Group to ensure the efficacy of internal controls and the efficiency of governance mechanisms.

They will also actively promote compliance through training, campaigns and engagement.

They will take the lead in co-ordinating and responding to formal information access requests and complaints within the sphere of IT products and services.

The role will also be pivotal in enabling the delivery and continuous improvement of all information security management activities related to the University Group's tactical and strategic projects, services and systems with an IT component. The role will direct project stakeholders on how to be compliant with the required due diligence activities, and will ensure information security work packages are completed to a both a General Data Protection Regulation (GDPR) compliant standard, and as required by the Group's Information Protection Unit (IPU).

The post holder will have an excellent understanding of relevant standards (eg ISO 27001-2013), legislation (eg GDPR), licensing models and compliance and audit best practice. They will apply this insight to enable the business to operate safely and efficiently.

The post will be line-managed by the Chief Digital Information Officer and will work closely with all areas of Group IT provision in order to build effective and compliant solutions for the University Group.

2.2. Main Duties and Responsibilities

1. Take ownership of the review of all IT products, services and systems and engage with all suppliers, internal project teams and business system owners to assess, document, identify compliance issues and audit end to end data management across systems, data bases and communications channels to ensure the correct security accreditation and measures are in place by all parties to safe-guard data in line with group, DPA and GDPR policies and standards.

2. Sets out and defines a strategic management model for IT and digital information compliance based on business objectives, adopted standards or regulatory requirements.

3. Drafts and maintains the policy, standards and procedures for compliance with relevant legislation. Understands the implications of information, both internal and external, that can be mined from business systems and elsewhere. Reviews proposals for new digital initiatives and provides specialist advice on the management of information-related risk. Creates and maintains an inventory of information assets, which are subject to relevant legislation. Prepares, reviews and submits periodic notification of registration details to the relevant regulatory authorities. Ensures that formal information access requests and complaints are dealt with according to approved procedures.

4. Conduct vendor management at the level required to conduct compliance reviews whilst ensuring handoff of information relevant to progressing services into delivery with business sponsors, delivery managers, IPU and legal. May include supplier pre-engagement (eg ITT's) and/or due diligence reviews along with remediation recommendations or advice to suppliers.

5. Owning and maintaining the portfolio view of both University Group IT service/s systems and their current compliance status against externally recognised IT compliance regulations; and also of the compliance status of IT related transitional projects against the requirements.

6. Champions and actively promotes compliance through training, campaigns and engagement.

7. Interprets information assurance and security policies and applies these in order to manage risks. Provides advice, guidance and solution recommendations to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines. Uses testing to support information assurance. Contributes to the development of policies, standards and guidelines for information assurance.

8. Carries out risk assessments for IT products and services. Uses consistent processes for identifying potential risk events. Quantifies and documents the probability of occurrence and the impact on the business. Refers to domain experts for guidance on specialised areas of risk, such as architecture and environment. Co-ordinates the development of countermeasures and contingency plans. Also conducts periodic reviews and audits of all live products and services to ensure no change to compliance requirements, keeping a database for group wide access.

9. Manages and maintains the compliance of all IT and service assets with respect to licensing requirements. Carries this out in line with business and regulatory requirements involving knowledge of financial and technical processes, tools and techniques. Identifies, assesses and communicates associated risks. Ensures asset controllers, infrastructure teams and the business co-ordinate and optimise value, maintain control and maintain appropriate legal compliance.

10. Plans formal reviews of activities, processes, products or services. Evaluates and independently appraises the internal control of automated business processes, based on investigative evidence and assessments undertaken by self or team. Ensures that independent appraisals follow agreed procedure and advises others on the review process. Provides advice to management on ways of improving the effectiveness and efficiency of their control mechanisms. Identifies and evaluates associated risks and how they can be reduced.

11. Supports contractual compliance where appropriate.

12. Responsible and accountable and drives process performance improvements in relevant compliance areas (eg PIA etc)

13. Supports project teams, information protection and security teams on advice, guidance and training where appropriate.

14. Deputises for the Chief Digital Information Officer on compliance issues as required.

AND such other duties as are within the scope of the spirit of the job purpose, the title of the post and its grading.

2.3. Supervision Received

Line management is from the Chief Digital Information Officer.

The post-holder will have a second reporting line to the CTO and Deputy CDIO's.

2.4. Supervision Given

None.

2.5. Contacts

- IT Services staff, including Executive Team.
- University Group Leadership Team.
- Staff and students in other Schools / Support Areas of the University Group.
- External Suppliers and other education institutions.

3. Person Specification

ATTRIBUTES	ESSENTIAL	ADVANTAGEOUS
Education Qualifications	• Educated to degree level in a relevant discipline with a chartered professional qualification or substantial experience in related field in lieu of the above.	• Postgraduate or professional qualification in a relevant discipline. • CISA (Certified Information Systems Auditor).
Knowledge & Experience	• Substantial experience of IT compliance management in a large, complex organisation. • Leadership / Management • Influencing experience • IT regulatatoty requirements • Strategic Execution • IT Security management • Understanding global / local business differentiation.	• Understanding of business organisation, politics and culture. • Ability to understand related industries. • Higher Education experience.
Interpersonal Skills	• Results orientation. • Collaboration / teamwork. • Resolving conflicts and problems. • Adaptability. • Openness to learning. • Decisiveness. • Accountability. • Communication, listening information gathering. • Creative and innovative thinking. • Influencing and persuading. • Excellent oral and written communication skills. • Ability to organise workloads to ensure simultaneous execution of tasks and activities. • Ability to work effectively under pressure. • Ability to own and see tasks through to completion. • Ability to work as part of a team. • Ability to use own initiative.	• Conceptual thinking. • Strategic thinking. • Leading, inspiring and building trust.

	• Influencing and negotiating skills (internal & external to organisation	
• Job-related Skills, Abilities & Competencies	• Excellent analytical, strategic conceptual thinking, strategic planning and execution skills. • Exceptional leadership skills with the ability to develop and communicate a compliance vision, and inspire, motivate and develop staff. • Takes accountability and has strong sense of ownership. • Results orientated and a commitment to a high quality customer service • A distinctive blend of business, IT, compliance, financial and communication skills. • Understanding business organisation, politics and culture. • Ability to build and maintain broad network of business relationships. • Knowledge of customer behaviours, needs and expectations. • Ability to lead a team/discipline to quickly resolve complex problems in the provision of IT services. • Good understanding of current and emerging technologies and how other enterprises are employing them to drive digital business support. • Auditing information systems. • Risk management and risk-based assessment. • Knowledge of relevant legislation and processes (GDPR; FOIA; DSAR etc.). • Knowledge of relevant software & hardware licensing models and ability to interpret, advise and apply.	• Governance and management of IT. • Knowledge of procurement approaches and frameworks. • Supplier management.

ATTRIBUTES	ESSENTIAL	ADVANTAGEOUS

Other Requirements	• A flexible approach to working hours and location, including a willingness to travel, locally, nationally or overseas, as required. • An appreciation of other cultures; the global reach of the University and its international agenda. • A mature, professional and self-motivated approach to tasks. • Ability to represent IT Services in formal and informal settings. • Able to work under pressure. • Ability to work flexibly and extended hours by agreement to meet tight, fixed deadlines or as required by service imperatives. • Health & Safety Awareness.	