

Job Description

IT Compliance Officer

Salary:	Grade 6
Contract:	Full time, ongoing
Location:	Canterbury Campus
Responsible to:	Assistant Director of IT Services (Product & Partnerships)
Job family:	Administrative, professional and managerial

Job purpose

The IT Compliance Officer plays a pivotal role in embedding a culture of compliance, governance, and continuous improvement within the IT Services department at the University of Kent.

The role ensures departmental adherence to institutional, legal, and regulatory obligations—particularly in relation to, but not limited to; IT audit support, policy frameworks, risk management, FOI coordination, and the maintenance of the Information Asset Register. The postholder will work closely with the University's Data Protection Office (DPO) and other stakeholders to ensure IT systems, services and data are appropriately governed, compliant, and risk aware.

A key part of the role is to support departmental data protection practices, including facilitating and contributing to Data Protection Impact Assessments (DPIAs) to identify and mitigate information risks, managing regulatory risk effectively.

Key accountabilities

The following are the main duties for the job. Other duties, commensurate with the grading of the job, may also be assigned from time to time.

- Act as the departmental lead for IT Services compliance activity, ensuring effective monitoring and reporting on regulatory, policy and audit requirements.
- Coordinate departmental responses to internal and external audits, maintaining supporting evidence and tracking audit recommendations to resolution.
- Maintain the IT Services policy framework and catalogue, ensuring timely review, alignment with University governance, and accessibility for stakeholders.
- Serve as the IT Services liaison for FOI requests, supporting data collection, deadline tracking and quality assurance in collaboration with Central Information Compliance.
- Own and maintain the departmental Information Asset Register (IAR), liaising with asset owners and ensuring regular updates in line with data protection obligations.
- Facilitate and contribute to the completion of Data Protection Impact Assessments (DPIAs) for IT Services systems and projects, supporting stakeholders in identifying and addressing data protection risks in collaboration with the University's DPO.
- Champion data protection best practice and support teams in implementing appropriate safeguards for systems and data.
- Manage the departmental risk register, coordinating reviews with owners and supporting the reporting of emerging risks and mitigations to IT Services senior leadership
- Ensure IT Services frameworks (e.g. policy, risk) are implemented, maintained and monitored, working with team leads to embed best practice.

- Produce clear, accessible management reports and dashboards to support governance, audit, planning and risk oversight.
- Support the design, rollout and maintenance of compliance-related training and awareness activities.
- Participate in specialised projects and process improvements, providing expertise in governance, risk and compliance.

Key challenges and decisions

The following provide an overview of the most challenging or complex parts of the role and the degree of autonomy that exists.

- Maintaining a comprehensive view of legal, regulatory and internal compliance needs across a complex and technical service landscape.
- Balancing operational priorities and strategic improvement activities while supporting audit, FOI and data protection compliance.
- Coordinating inputs from diverse stakeholders under tight deadlines (e.g. audit or FOI timescales).
- Translating complex compliance obligations into accessible guidance for IT Services colleagues across a range of disciplines.
- Managing the quality, accuracy and version control of the policy and risk frameworks while championing their consistent use.

Facts & figures

- Supports compliance across a department of c. 100 IT Services staff.
- Coordinates audit and FOI responses on behalf of IT Services, typically involving cross-functional contributions.
- Maintains departmental policies and a live Information Asset Register.
- Manages multiple frameworks and inputs into Institutional risk reporting.

Internal & external relationships

Internal: IT Services Senior Leadership Team, Policy Owners, Project Managers, Team Leads, Central Secretariat, Data Protection Officer, Information Governance, Risk Management, Legal Services, Procurement, HR.

External: Auditors, regulatory bodies, FOI requesters, other Higher Education institutions, UCISA, Gartner and benchmarking networks

Health, safety & wellbeing considerations

This job involves undertaking duties which include the following health, safety and wellbeing considerations:

- Regular use of Screen Display Equipment
- Pressure to meet important deadlines such as might be inherent in high profile projects
- There may be a requirement to work evenings and weekends
- Potential for working in isolation
- Ability to occasionally travel in a timely and efficient manner between campuses

Person specification

The person specification details the necessary skills, qualifications, experience or other attributes needed to carry out the job. Applications will be measured against the criteria published below.

Selection panels will be looking for clear evidence and examples in an application, or cover letter (where applicable), which back-up any assertions made in relation to each criterion.

Essential Criteria:

- Educated to A-Level standard or equivalent experience (A)
- Demonstrable experience supporting audit, governance or compliance frameworks (A, I)
- Strong understanding of data protection principles and experience supporting FOI responses or data governance (A, I)
- Experience supporting or coordinating Data Protection Impact Assessments (DPIAs) or information risk assessments (A, I)
- Proven experience developing or maintaining policy or risk registers in a large organisation (A, I)
- Experience managing data across multiple systems and presenting management information to non-specialist audiences (A, I)
- Excellent verbal and written communication skills and ability to engage with staff at all levels (I)
- High level of accuracy, attention to detail, and ability to manage sensitive information appropriately (I,T)
- Confident in using Microsoft 365 (especially SharePoint, Excel, Teams and Power BI/Lists) (A, I)
- Ability to work independently, manage competing demands, and meet deadlines (I)
- Firm commitment to achieving the University's vision and values, with a passion for a transformative student experience and multidisciplinary, impactful research (I)
- Commitment to deliver equality, diversity and inclusivity in the day to day work of the role (I)

Desirable Criteria:

- Professional certification or training in risk management, audit, data protection, or compliance (A)
- Experience working in a Higher Education or public sector environment (A, I)
- Familiarity with project governance methodologies (A, I)
- Experience supporting Information Asset Registers and GDPR compliance (A, I)

Assessment stage: A - Application; I - Interview; T - Test/presentation at interview stage