Job Description – Senior Manager Information Rights

About the Role

The Senior Manager – Data Breaches and Issues, Information Rights is responsible for managing the processes and activities needed to ensure that the university fulfils its obligations under the Data Protection Act 2018 and the Freedom of Information Act 2000. This includes ensuring that statutory deadlines are met, high standards are maintained and thorough records kept. The role covers both operational activities and strategic developments to support the continuous improvement of Information Rights compliance in the university.

Key Responsibilities

1. Assessment and management of Data Protection breaches in collaboration with other members of the Information Rights Management Team and in collaboration with other units as needed. Escalation of breaches to the Head of Information Rights and the Data Protection Officer or Chief Information Security Officer as appropriate, reporting them to the Information Commissioner’s Office as required within statutory deadlines.

2. Management of the Information Rights Issue Log prioritising issues according to risk, acting as the lead in their resolution and coordinating activities with other units as required. Recording new issues as they arise, documenting issue resolutions and reporting progress at regular team meetings.

3. Engage with and advise on initiatives to improve breach and incident management.

4. Arranging and running bespoke training sessions for teams across the university in order to promote understanding of Information Rights and of individuals' responsibilities in relation to the relevant Acts.

5. Supporting other members of the Information Rights Management Team to ensure that comprehensive and appropriate responses are provided to requests made under either the Data Protection Act 2018 (DPA) or the Freedom of Information Act 2000 (FOIA) within the statutory deadlines.

6. Line managing other members of the team as needed, supporting their personal development while maintaining high standards.

7. Contributing to relevant projects as needed, working collaboratively with the project team and with related teams in the university, including Information Security, Data Governance and IT.
Skills and Experience

• Strong knowledge of the Data Protection Act 2018 and working knowledge of the Freedom of Information Act 2000, including a good understanding of the relationship between the two Acts and experience of the practical application of both. Ideally holding qualifications in both subjects to at least Practitioner level.

• A good understanding of Information Security and of the relationship between Information Security and Data Protection, including the use of technical measures to support privacy of personal information.

• Good communication and interpersonal skills, demonstrating the ability to build rapport with team members and stakeholders, and to clearly articulate data protection requirements and the benefits of compliance to stakeholders across the business.

• Able to work collaboratively and flexibly within a team to enable the whole team to deliver against its objectives.

• Able to build collaborative relationships with other units of the university and to use these effectively to help units improve their data protection compliance.

• Good organisational skills, able to demonstrate a structured and systematic approach to process management and case management.