East Lothian Council

Members' Library Service Request Form

Date of Document	08/08/25
Originator	Nikki Brennan
Originator's Ref (if any)	
Document Title	Creation of Project Officer - Information Governance

Please indicate if access to the document is to be "unrestricted" or "restricted", with regard to the terms of the Local Government (Access to Information) Act 1985.

Unrestricted	☒	Restricted	☐

If the document is "restricted", please state on what grounds (click on grey area for drop-down menu):

For Publication

Please indicate which committee this document should be recorded into (click on grey area for drop-down menu):

Cabinet

Additional information:

Authorised By	Hayley Barnett
Designation	Head of Corporate Support
Date	09/02/26

For Office Use Only:	
Library Reference	16/26
Date Received	09/02/26
Bulletin	Feb 26

East Lothian Council

STAFFING REPORT – NEW POST

REPORT TO: Members' Library Service

BY: Depute Chief Executive – Resources and Economy

DATE: February 2026

SUBJECT: Staffing Report for the Creation of a Project Officer within Information Governance

---

1 PURPOSE

1.1 To seek Executive Director – Council Resources approval under delegated powers for the creation of an Information Governance Project Officer as a **Temporary** change to the staffing structure.

2 RECOMMENDATIONS

2.1 To agree to the proposed changes to the staffing structure as outlined in the report.

3 BACKGROUND

3.1 This position is proposed to provide additional capacity within the Information Governance team, with the primary objective of addressing the current backlog of outstanding Data Protection Impact Assessments (DPIAs), Data Sharing Agreements (DSAs), and data protection-related complaints.

3.2 The postholder may also be assigned other duties, as required, to support the wider work of the Information Governance function.

4 POLICY IMPLICATIONS

4.1 This proposal supports and reinforces compliance with the Council's Data Protection Policy, Information Security Policy and a range of legislative requirements. By providing additional capacity within the Information Governance team, the post will directly contribute to ensuring that the organisation meets its obligations under the UK General Data Protection

Regulation (UK GDPR), the Data Protection Act 2018, and relevant internal data protection and information governance policies.

4.2 The post will enable more timely completion of DPIAs, DSAs and the resolution of data protection complaints. This, in turn, will strengthen organisational accountability, reduce risk, and ensure consistent adherence to statutory and policy requirements relating to the handling of personal and sensitive data.

4.3 Failure to address these backlogs could result in non-compliance, reputational damage, and potential regulatory action. Therefore, the proposal has clear and positive policy implications by supporting a proactive and compliant approach to information governance.

5 INTEGRATED IMPACT ASSESSMENT

5.1 The subject of this report does not affect the wellbeing of the community or have a significant impact on equality, the environment or economy.

6 DISCLOSURE SCOTLAND REQUIREMENT

6.1 This post will require a **Basic** Disclosure check in order to comply with legislation/PSN Code of Connection.

7 RESOURCE IMPLICATIONS

7.1 Financial – The Council's Finance team has been consulted and the costs (including 30% on-costs) will be £ 77,469.00. Funding will be provided from the Business Transformation budget. The post has been evaluated at a **Grade 8**.

7.2 Personnel – This post has been formally evaluated and will be advertised in accordance with the Council's Recruitment & Selection Policy. As part of the approval process HR and relevant Trades Unions will be consulted.

8. BACKGROUND PAPERS

- Agreed Job Details Form
- Proposed Structure Chart

AUTHOR'S NAME	Nikki Brennan
DESIGNATION	Team Leader – Information Governance
CONTACT INFO	nbrennan@eastlothian.gov.uk
DATE	8 August 2025

East Lothian Council

JOB DETAILS FORM

JOB OUTLINE	
JOB TITLE: Project Officer	**JET CODE:** 8043
DIVISION: Corporate Support	
SERVICE/BUSINESS UNIT: Governance / Information Governance	
REPORTING TO: Team Leader – Information Governance	
RESPONSIBLE FOR: No line management responsibility	

JOB PURPOSE:

To assist in the development and operational delivery of the Council's Information Governance Services, maximising efficiency of service delivery within specific standards and in accordance with the Council's policies and plans with a commitment to achieve best value

MAIN DUTIES:

Reviewing and Assessing Data Protection Impact Assessments (DPIAs)
The Jobholder is responsible for the detailed review and analysis of DPIA submissions from service areas. This includes evaluating the adequacy of information provided, identifying risks to personal data, and ensuring compliance with data protection legislation. This task occupies a significant portion of the role and requires sustained concentration and technical expertise.

Providing Advice, Guidance, and Training on Data Protection Compliance
The Jobholder provides professional advice to service areas on data protection obligations, risk mitigation strategies, and the implementation of appropriate safeguards. This includes interpreting relevant legislation, organisational policies, and best practice standards to support informed decision-making and ensure compliance. In addition to advisory responsibilities, the Jobholder plays a key role in capacity-building across the organisation by developing and delivering training sessions, both virtually via Microsoft Teams and in person, tailored to the needs of different service areas. They are also responsible for creating, reviewing, and updating training materials and guidance documents to reflect current legislative requirements and organisational procedures, thereby promoting a consistent and informed approach to data protection compliance.

Collaborating with Information Security and Other Stakeholders
The role involves working closely with Information Security colleagues and other internal stakeholders to complete DPIA reviews and ensure a coordinated approach to risk management and compliance.

Drafting Formal Reports and Communications
The Jobholder prepares detailed written reports outlining DPIA findings, recommendations, and conditions. They also respond to queries and complaints from service areas regarding DPIA outcomes, requiring clear and professional communication.

Participating in DPIA Meetings and Presentations
The Jobholder attends and contributes to DPIA meetings, both formally and informally, to discuss findings, clarify requirements, and manage expectations. This may involve negotiation and persuasion, particularly when dealing with contentious or complex issues.

Monitoring Implementation of DPIA Conditions
The Jobholder ensures that conditions applied to DPIAs are followed through by service areas, providing follow-up support and advice where necessary to maintain compliance.

Maintaining Records and Ensuring Data Accuracy
Accurate record-keeping of DPIA reviews, decisions, and communications is essential. The Jobholder ensures that all documentation is securely stored and managed in line with organisational and legislative requirements.

Keeping Up to Date with Legislative and Policy Changes
The Jobholder is expected to remain informed about changes to data protection legislation, such as the Data (Use and Access) Act 2025, and assess how these developments may impact DPIA processes and organisational compliance.

Reviewing and Assessing Data Sharing Agreements (DSAs)

The Jobholder undertakes the review and assessment of Data Sharing Agreements to ensure they meet the Council's policy requirements and comply with relevant legislation. This includes identifying risks, recommending mitigations, and supporting service areas in the development of robust and compliant data sharing practices.

Processing and Responding to Data Protection Complaints

The Jobholder manages data protection-related complaints, liaising with service areas to gather necessary information and ensure a thorough investigation. They maintain clear and timely communication with complainants throughout the process, ensuring that concerns are addressed appropriately and in accordance with statutory and organisational standards.

Any other appropriate duties, as requested by Management, commensurate with the grade for the post.

ESSENTIAL REQUIREMENTS FOR THIS ROLE

Qualifications/Experience:

- Relevant degree Level Qualification (e.g. law, information management) and evidence of professional training in data protection compliance and/or be able to demonstrate equivalent knowledge, skills or and competencies gained through previous experience.

Disclosure Scotland:

- This role requires **Level 1 Disclosure Clearance** to allow access to the Public Sector Network. ELC will submit a Police Act Disclosure application on behalf of the preferred candidate and receipt of the subsequent certificate will be **required prior to commencement**.

Scottish Social Services Council: N/A

Politically Restricted Post: N/A

TEAM OBJECTIVES:

Key Responsibilities of the Information Governance Team

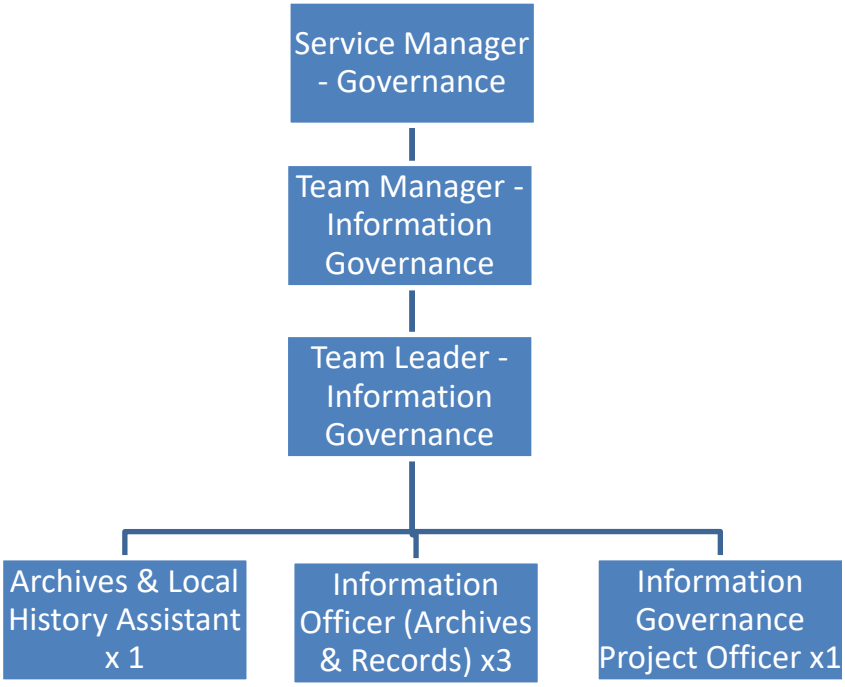
1. **Data Protection & Privacy Compliance**
   - Ensure compliance with data protection laws.
   - Manage data subject rights requests (access, rectification, erasure, etc.).
   - Review data protection impact assessments (DPIAs) for new projects.
2. **Records Management**
   - Develop and enforce policies for the creation, storage, retention, and disposal of records.
   - Maintain records retention schedules aligned with legal and operational needs.
3. **Information Security Collaboration**
   - Work with IT and Information Security teams to safeguard data.
   - Support incident response and data breach investigations.
4. **Policy Development & Training**
   - Create and maintain Information Governance policies, procedures, and guidance.
   - Deliver staff training and awareness programs on data handling and governance.
5. **Risk Management & Auditing**
   - Identify and mitigate risks related to information handling.
   - Conduct audits and reviews to ensure compliance and best practices.
6. **Freedom of Information (FOI) & Subject Access Requests (SARs)**
   - Coordinate responses to FOI requests and SARs in a timely and lawful manner.
7. **Governance Framework & Oversight**
   - Establish governance structures for data ownership and accountability.
   - Monitor and report on IG performance and compliance metrics.

Objectives of the Information Governance Team

- **Protect the Councils information assets.**
- **Ensure legal and regulatory compliance.**
- **Promote transparency and accountability.**

- **Enable safe and effective use of data.**
- **Support organisational resilience and trust.**

ORGANISATIONAL STRUCTURE:


Service Manager - Governance
Team Manager - Information Governance
Team Leader - Information Governance
Archives & Local History Assistant x 1
Information Officer (Archives & Records) x3
Information Governance Project Officer x1

PERSON SPECIFICATION		
Attributes	**Essential**	**Desirable**
Education, Registration & Training	Educated to Degree level in a relevant subject e.g. law, information management or be able to demonstrate equivalent knowledge, skills and competencies by evidencing: Experience of working in a complex environment with competing demands; Knowledge of relevant professional, regulatory and statutory frameworks in relation to data protection Skills and experience of producing professional written documentation for use at a corporate or senior management level; Completed training relating to data protection Evidence of a commitment to Continual Professional Development; This role requires **Level 1 Disclosure Clearance** to allow access to the Public Sector Network. ELC will submit a Police Act Disclosure application on behalf of the preferred candidate and receipt of the subsequent certificate will be **required prior to commencement**.	Completed training relating to: records management, archives administration, and/or digital preservation; Completed training relating to compliance with the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004 Experience of working in a leadership role in a complex environment
Previous Experience (Paid & Voluntary Work)	Experience of interpreting, advising on and applying changes in legislation	Experience of working within a public authority and/or local government

	Experience of change management and supporting corporate services to meet legislative requirements; Experience of working in a multidisciplinary, complex organisation with competing demands Experience of managing services associated with legislation compliance Experience of working to strict and/or statutory deadlines.	Experience of liaising with and responding to external agencies in terms of compliance and scrutiny.
Knowledge/ Skills /Competencies	A clear understanding of relevant professional, regulatory and statutory frameworks in relation to data protection. Ability to use initiative to identify and implement improvements to existing processes.	Knowledge of local authority functions and activities; Detailed knowledge/experience of data protection legislation and regulatory frameworks;
Personal Qualities	The successful candidate should be able to demonstrate the following qualities: Flexibility; Adaptability; Creativeness; Resilience; Self-discipline; Diplomacy; Integrity; Open-Mindedness;	

	Excellent attention to detail; Ability to use independent judgement to manage confidential and/or highly sensitive information with tact, diplomacy and mindfulness of legal requirements; Ability to develop good working relationships with internal and external stakeholders; Excellent initiative and a commitment to continuous improvement.	
Council Behaviours	We are Person Centred We Initiate and Embrace Change We Strive to be the Best we can be We make things Happen We work Together	

FACTOR LEVEL DESCRIPTORS

WORKING ENVIRONMENT:

This is a hybrid role, with the Jobholder working either remotely or within a standard office environment. When working from home, the Jobholder is responsible for ensuring their workstation complies with Display Screen Equipment (DSE) requirements. Office-based work is conducted in a typical office setting, which is clean, safe, and free from physical hazards.

The role does not involve any outdoor working, exposure to adverse weather conditions, or environments such as construction sites, refuse tips, or areas requiring personal protective equipment (PPE). There are no hazardous substances or manual tasks associated with the post.

There is no requirement for lone working in high-risk environments. Any meetings or collaborative tasks are conducted either virtually or in-office, with limited walking required (e.g., moving between meeting rooms).

Overall, the working environment is low-risk and consistent with standard professional office roles.

PHYSICAL CO-ORDINATION:

The role requires a standard level of physical coordination, primarily for the use of a computer and associated office equipment. The Jobholder uses a keyboard and mouse daily to carry out tasks such as reviewing documentation, drafting reports, and managing communications.

The Jobholder is expected to use the Microsoft 365 suite (including Word, Excel, Outlook, and Teams) on a daily basis. These tools are used for:

- Word: drafting formal communications and reports
- Excel: tracking DPIA progress and managing data
- Outlook: managing email correspondence and scheduling
- Teams: participating in virtual meetings and collaborative discussions

No specialist tools or equipment are required for this role, and there is no use of machinery or manual handling tasks.

Driving is not a requirement for this post, and it is not designated as a contracted car user role. All duties can be carried out within office premises or remotely, with meetings typically held virtually or within walking distance if in-office.

PHYSICAL EFFORT:

This role is primarily desk-based and involves prolonged periods of sitting while reviewing documentation, drafting reports, and participating in virtual meetings. The Jobholder is not required to lift, carry, push, or pull any equipment or materials as part of their duties.

There are no tasks that require working in awkward or constrained positions. Physical movement is limited to occasional walking within office premises, such as attending in-person meetings or moving between workstations.

Overall, physical effort is minimal, with approximately 95–100% of the working time spent seated in a standard office environment.

MENTAL SKILLS:

One of the most complex aspects of this role involves the assessment and review of Data Protection Impact Assessments (DPIAs). These require a high level of analytical skill and attention to detail to ensure full compliance with data protection legislation.

The Jobholder is expected to interpret and apply relevant policies, procedures, and legislation—particularly the UK GDPR and Data Protection Act 2018—when reviewing submissions from service areas. This involves working collaboratively with Information Security colleagues to evaluate risks and recommend appropriate mitigations.

Problem-solving in this role draws on a variety of sources, including:

- Internal policy and procedure documents
- Legislative and regulatory frameworks
- Input from service areas
- Guidance from Information Governance and Information Security teams

Analysis is often in-depth, requiring the Jobholder to assess the nature, scope, context, and purposes of data processing activities, and to identify potential risks to individuals' rights and freedoms. The role demands a strong understanding of both technical and organisational measures to ensure compliance.

Planning and scheduling are integral to the role. The Jobholder is responsible for managing their own workload, often scheduling DPIA reviews and related tasks several weeks to months in advance, depending on project timelines. This can cover projects from other services i.e. things like the procurement of a new finance system – assessing the IG documentation to ensure delays do not impact the procurement functions. It can also cover projects to improve and clear the DPIA backlog etc.

They may also contribute to broader strategic planning within the Information Governance function, particularly in relation to data protection compliance and risk management**.** This could involve providing insight on ways to improve processes, or collaboration with other teams to streamline. These plans are generally developed several months in advance as part of the strategic planning cycle, ensuring alignment with compliance objectives and allowing time for collaboration and process improvements.

CONCENTRATION:

The Jobholder is required to maintain sustained periods of concentration throughout the working day, particularly when reviewing and analysing Data Protection Impact Assessments (DPIAs). These tasks demand a high level of attention to detail and accuracy, often requiring uninterrupted focus for periods of one hour or more. There is no set time for a length of period the Jobholder is expected to concentrate for. However, some more complex documents can require a few hours of work to ensure they have been assessed properly. The Jobholder can still take breaks throughout this work which will likely help enhance concentration.

Key duties requiring concentration include:

- Reviewing complex DPIA submissions from service areas, which involves interpreting technical and legislative information
- Drafting detailed reports and formal communications, including recommendations and conditions for compliance. For example: reports for SMT and reports on findings of DPIAs etc for Service areas.
- Participating in DPIA meetings, where the Jobholder must listen actively, respond to queries, and explain findings clearly.

The most significant pressures in the role stem from:

- Frequent interruptions, such as queries from service areas or urgent requests for DPIA reviews. These interruptions are inevitable.
- Switching between tasks, particularly when managing multiple DPIAs at different stages of completion
- Tight deadlines, which may be linked to project timelines or statutory requirements for data protection compliance. Certain deadlines are imposed by Procurement (i.e. standstill and before award issued) If the Jobholder is involved with complaints, then there is an internal deadline of 20 working days. If it is a regulatory request, for example an appeal has been lodged regarding the outcome of a DP complaint, from the ICO/SIC then this is external.

For example, the Jobholder may be reviewing a DPIA involving sensitive personal data while simultaneously responding to queries about another assessment, all under time constraints. This requires the ability to refocus quickly and maintain a high standard of work despite competing demands.

COMMUNICATIONS SKILLS:

Communication is a key aspect of the role and occurs through various channels—verbal, email, telephone, and in-person. These interactions often involve discussing contentious or complex issues, requiring the Jobholder to provide clear, detailed explanations and, at times, engage in negotiation or persuasion to manage expectations and ensure understanding.

The Jobholder plays a key role in capacity-building across the organisation by developing and delivering training sessions, both virtually via Microsoft Teams and in person, tailored to the needs of different service areas. These training sessions will be focussed on data protections matters (subjects include but not limited to – DPIA's, DSA's, information sharing

etc) These will be aimed at all service areas and will include generic 'everyone should know' sessions and also bespoke sessions in cases where a data breach has occurred.

Individuals will all have different levels of familiarity with the training but given the DP mandatory training, they should have at least a basic understanding.
Training may involve presentations however these will be created by the Team Leader – Information Governance. Training is not accredited.

The role involves working closely with Information Security colleagues and other internal stakeholders to complete DPIA reviews and ensure a coordinated approach to risk management and compliance. Discussions will be with regards to data processing activities for which the Services have asked for.

The Jobholder will also respond to queries and complaints from service areas regarding DPIA outcomes, requiring clear and professional communication. The Jobholder would be required to explain why a decision has been made, for example if a DPIA has failed due to inadequate DP procedures, they would explain this and link to the appropriate legislation. If the queries/complaints escalate then these would be picked up by the Team Leader or Team Manager where appropriate.

The Jobholder will hold an advisory role i.e. they can advise and guide others regarding their obligations under the legislation/council policy. In cases where a DPIA is refused, this will be communicated to the Service. If they choose to go ahead anyway, the Jobholder does not have the authority to stop them (only Head of Service does).

While the Jobholder is unlikely to elicit or explain contentious information, the Jobholder would:

In terms of complaints - draft information that could be considered contentious for review and escalation to the DPO.

In terms of DPIAs/DSA – illicit information from suppliers/services which may not immediately be evident and require further investigation. For example, a recent supplier stated no data processing required, further conversations uncovered full system access for data processing/testing. This required further investigation and required contract termination.

It is most likely that the contentious issues are dealt with by the Team Leader and/or Team Manager. It would be irresponsible to say that the Jobholder would never come across this, but it is likely to be less than 20% of the time.

DEALING WITH RELATIONSHIPS:

The Jobholder may be required to engage with external service providers in instances where internal services are unable to supply sufficient information to complete a DPIA.

Additionally, the Jobholder may handle complaints or concerns raised by service areas regarding the outcomes of DPIA reviews, including decisions made or conditions applied.

Furthermore, the Jobholder may handle data protection complaints raised by members of the public who may be dissatisfied or irate. Verbal abuse from customers is unlikely. It is more likely that the customers tone (verbally and in writing) is negative. At times they can also be pushy and belligerent. That is not to say that verbal abuse will never happen, but it is very unlikely.

RESPONSIBILITY FOR EMPLOYEES:

The Jobholder will not be responsible for employees.

RESPONSIBILITY FOR SERVICES TO OTHERS:

Although the role does not involve delivering a traditional front-line service, the Jobholder plays a key role in a front-line capacity by responding to customer complaints as and when necessary. They also provide critical support to corporate functions, specifically within Information Governance and Data Protection. The primary responsibility is to ensure the quality and compliance of Data Protection Impact Assessments (DPIAs) submitted by service areas.

The Jobholder delivers this service to internal departments across the organisation, providing expert guidance and support throughout the DPIA process. This includes assessing the adequacy of information provided, identifying risks, and ensuring that appropriate safeguards are in place in line with data protection legislation.

A key aspect of the role involves applying and monitoring compliance with relevant regulations, particularly the UK GDPR and the Data Protection Act 2018. The Jobholder ensures that conditions applied to DPIAs are adhered to and may be required to follow up with service areas to confirm implementation.

While not directly responsible for designing services, the Jobholder contributes to the management and improvement of service delivery by advising on data protection considerations during project planning and implementation. This ensures that services are designed with privacy and compliance embedded from the outset.

The Jobholder contributes to the assessment, design, and delivery of improvement plans, primarily from a data protection and compliance perspective. Examples include:

- Assessment: Reviewing proposed projects or service changes to identify potential data protection risks and advising on mitigation strategies.
- Design: Providing input to ensure privacy and compliance are embedded in new processes or systems from the outset.
- Delivery: Collaborating with project teams during implementation to validate that agreed data protection measures are applied correctly and effectively.

<u>Monitoring compliance</u>
The Jobholder supports service areas in implementing conditions and recommendations arising from DPIA reviews. This includes:

- Following up to ensure that agreed actions are completed
- Advising on appropriate technical and organisational measures to protect personal data
- Contributing to the development and refinement of internal procedures related to information governance

The Jobholder will escalate to the Team Leader – Information Governance for them to address if services do not comply with the Jobholders implementation of conditions and recommendations.

RESPONSIBILITY FOR FINANCIAL RESOURCES:

The Jobholder does not have any responsibility re. financial resources.

RESPONSIBILITY FOR PHYSICAL AND INFORMATION RESOURCES:

The Jobholder does not have responsibility for physical resources such as plant, equipment, premises, or stock. However, they do have a significant role in relation to information resources, particularly in the context of managing and reviewing Data Protection Impact Assessments (DPIAs).

Primary responsibility: Information systems and records
The Jobholder is responsible for handling sensitive and complex information submitted by service areas as part of the DPIA process. This includes:

- Reviewing and analysing documentation to ensure compliance with data protection legislation
- Maintaining accurate records of DPIA reviews, decisions, and conditions applied
- Ensuring that information is stored and managed securely in line with organisational policies and data protection requirements.

This information is held within the Information Governance folders with controlled access. The Jobholder will use this information to adequately assess the requests to ensure that they meet the appropriate levels of data protection, as set out in the legislation.

While the role does not involve designing or managing IT systems directly, the Jobholder's work is integral to the organisation's overall approach to data protection and information management.

INITIATIVE & INDEPENDENCE:
The Jobholder operates within established organisational policies, procedures, and legislative frameworks, particularly those relating to data protection and information governance. While guidance is available through internal documentation and support from colleagues and managers, the role requires a significant degree of independent decision-making.

Independent decisions include:

- Assessing the adequacy and completeness of DPIA submissions
- Identifying potential risks and recommending appropriate mitigations
- Determining whether further information or clarification is required from service areas
- Advising on compliance with data protection legislation and internal policy.

These decisions are made using professional judgement, supported by training, experience, and reference to relevant legislation (e.g. UK GDPR, Data Protection Act 2018), as well as organisational guidance.

Issues referred to the manager may include:

- Escalation of high-risk or contentious DPIAs
- Situations where there is disagreement with service areas regarding compliance or mitigation measures
- Cases requiring strategic input or cross-departmental coordination.

The Jobholder works with a reasonable level of autonomy and is trusted to manage their own workload and make informed decisions within the scope of their role. While they do not have direct line management responsibility.

The Jobholder will not contribute to working groups or project teams, offering input into policy development and strategic planning related to data protection and information governance.

KNOWLEDGE:

The role requires a strong foundation of technical and specialist knowledge in data protection and information governance. This knowledge is typically acquired through a combination of formal education (such as a relevant degree in law, information management, or a related field) and/or substantial practical experience in a similar role.

To undertake the full duties of the post, the Jobholder must have:

- A thorough understanding of data protection legislation, particularly the UK GDPR and the Data Protection Act 2018
- Practical knowledge of organisational policies and procedures relating to DPIAs and information governance
- Strong investigative and analytical skills to assess complex information and identify compliance risks
- Effective communication skills to explain findings, influence outcomes, and manage expectations across service areas
- The ability to use initiative and exercise sound judgement when reviewing DPIAs and advising on mitigation measures.

Knowledge is acquired and maintained through a combination of:

- On-the-job experience and mentoring
- Formal training and professional development
- Participation in cross-functional teams
- Keeping up to date with legislative changes, regulatory guidance, and sector developments.

The Jobholder must remain aware of proposed changes to data protection legislation (Data (Use and Access) Act 2025 (DUAA) and emerging best practices, as these may directly impact the DPIA process and the organisation's compliance obligations. This awareness is essential to ensure that advice and decisions remain current, accurate, and legally sound.

The Jobholder must have experience of interpreting, advising on and applying changes in legislation.

Experience of change management and supporting corporate services to meet legislative requirements.

Experience of working in a multidisciplinary, complex organisation with competing demands.

Experience of managing services associated with legislation compliance.

AUTHORISATION:

I have read the information contained in this document and confirm that it is an accurate reflection of the duties and responsibilities for this post.

Jobholder* *(only in re-evaluation situations)*

Signed ..... Date .....

Line Manager

Signed .....Nikki Brennan..... Date 17/12/2025

Service Manager

Signed [redacted] Date 17 Dec. 25