Job description

Job title Data Protection Lead (Core)

- Grade: PO4
- Reports to: Data Protection Service Manager
- Direct reports: 0
- Your team: Information and Digital Governance/Data Protection and Records Management
- Service area: Digital Services
- Directorate: Resources

Special requirements of the post

Workstyle: Desk-based worker (Lower presence, one day a week minimum)

- Colleagues who are not usually client or customer-facing and can mostly work anywhere with the right technology. Regular on-site activities are required such as team events and collaboration that are more productive face to face

This post requires a DBS check at the appropriate level (Basic)

This post is subject to the council's declaration of interest procedure

Our mission

Islington is a place rich with diversity and culture. As a council our sense of purpose couldn't be clearer: we serve. It's in the logo. We are committed to challenging inequality in the borough and as one of the largest employers we know that to look after the place and the planet, we have to look after our people. **Together we can change the future**.

To do this, everyone who works at Islington Council lives by a set of values which guide us in everything that we do: collaborative, ambitious, resourceful, and empowering. They spell out 'CARE', which is what we think public service is all about.

Overview of the role

Working as part of the Information and Digital Governance team supporting the Data Protection Officer (DPO) to embed the highest standards of data protection within the council, ensuring the council complies with data protection legislations.

The postholder will serve as the council's primary advisor on day-to-day data protection matters, resolving queries from staff and management across all directorates. Exercise judgement to provide accurate, pragmatic advice and only escalate to the DPO for particularly high-risk or precedent-setting matters.

Key responsibilities

Please list each key responsibility of the role:

- As a subject matter expert serve as the lead advisor on day-to-day data protection matters providing specialist advice that is tailored to specific departmental requirements.
- Plan and undertake data protection audits across the council. Develop audit criteria and checklists ensuring that these are aligned with legislation and council policies. Provide audit feedback via comprehensive reports to Corporate Directors and Information Asset Owners (IAO) highlighting compliance gaps and recommending improvements.
- Design and deliver the council's data protection training programme in collaboration with the Information and Digital Governance team. Regularly update and tailor content for different audiences and deliver sessions (including bespoke workshops). Implement a system to monitor training completion and effectiveness (e.g. quizzes, feedback) and use communication channels (intranet, newsletters, awareness campaigns) to keep data protection top-of-mind. Ensure that training and communications reflect the latest legislative developments and emerging risks (e.g. incorporate lessons from recent breaches or new ICO guidance).
- Support the council's management of data breaches by acting as the incident coordinator. Engage relevant parties to support the investigation and provide advice on containment as required. Prepare reports that include lessons learned and corrective actions and present these to the DPO and SIRO. Ensure that any follow up actions are implemented to reduce recurrence of issue.
- Own the data protection policies and guidance. Draft, review and update key documents (e.g. Data Protection Policy, Privacy Notices etc) in line with new laws or best practice. Ensure that policies are regularly reviewed (at least annually) and remain fit for purpose. By doing so, uphold the Council's accountability (UK GDPR Art.5(2)) – demonstrating that policies are not only in place but actively maintained and enforced. Produce practical guidance materials and tools for staff and partners (e.g. DPIA templates, breach response checklists, "quick guides" on handling personal data correctly).
- Manage the DPIA process as part of embedding privacy by design. Advise project teams early on about when a DPIA is needed; provide templates and guidance. Review completed DPIAs, identifying any privacy risks. If risks are identified, ensure they have mitigating actions, and follow the project through its lifecycle to verify those actions are completed. Maintain a log of all DPIAs and their risk outcomes. Make decisions on moderate risk DPIAs (sign-off or require further measures) and escalate high residual risks to the DPO for formal sign-off. Continuously improve the DPIA process (e.g. introduce tooling or integrate with project management checkpoints) to strengthen the council's proactive risk management.
- Maintain and enforce the Council's Information Sharing Protocol and process. Act as the gatekeeper for data sharing: ensure a standard template and approval process exists for

Data Sharing Agreements (DSAs) and that all new DSAs are logged in a central repository with review dates. Work with services to advise on completing DSAs, verifying lawful bases and sufficiency of safeguards for each data share. Present high-risk or novel sharing proposals to the Data Protection Service Manager and the DPO for scrutiny. Maintain a record of all active sharing arrangements and periodically prompt data owners to review and update them.

- Working with Strategic Procurement and Legal Services support the Data Protection Service Manager to identify all contracts that involve data processors, advising on contract clauses, due diligence and monitoring in line with data protection legislative requirements.
- Attend and be an active participant in the council's Information Governance Review Panel providing expert advice on the application of exemptions.
- To respond to information complaints and conduct internal reviews in line with the corporate policy, liaising with data subjects, directorates and the ICO where required. Provide clear, written resolutions to complainants by re-evaluating decisions impartially and explaining the outcome in plain language.
- Any additional duties consistent with the grade and level of responsibility of this position, for which the holder possesses the required experience and/or training.

Compliance

Ensure adherence to legal, regulatory, and policy requirements under UK GDPR, Health and Safety, Employee Code of Conduct and in your area of expertise by identifying opportunities and risks, and escalating issues as necessary.

Person specification

Your application form needs to demonstrate how you fulfil the role's requirements. It is essential to address the criteria, as this will be used to evaluate your suitability for the position.

Essential and desirable criteria

Essential: the basic requirements that must be met for someone to be considered for a particular job. These criteria are mandatory and cannot be negotiated. Essential criteria directly impact the core qualifications or skills necessary to perform the job effectively.

Desirable: the additional qualities, skills, or qualifications that would be advantageous for a candidate to possess but are not mandatory. Not meeting them does not automatically disqualify someone from consideration for the job. This also allows candidates who do not possess certain desirable criteria the opportunity to explain how their other knowledge, experience and skills relate to these and what they may be in the process of doing or willing to do to achieve these.

Knowledge, experience, and skills

Point	Criteria description	Essential/desirable
1	Significant experience in a data protection role, providing advice and guidance in a large complex organisation, preferably public sector.	Essential
2	Thorough understanding of, and practical experience of meeting legal compliance requirements around Data Protection.	Essential
3	Practical experience of developing and delivering corporate training programmes, providing training and guidance about data protection to all levels of staff in a variety of formats.	Essential
4	Experience of developing, reviewing and embedding information governance policies, process and guidance.	Essential
5	Experience of managing and responding to data breaches and working alongside key stakeholders including IT, legal and the ICO.	Essential
6	Experience of working with highly confidential information, including sensitive data about service users and staff and investigative information which impacts the privacy of staff.	Essential

Point	Criteria description	Essential/desirable
7	Excellent communication and interpersonal skills. Able to communicate clearly, effectively and sensitively in both written and oral presentation.	Essential
8	Ability to liaise and negotiate wit staff at all levels, including the Chief Executive and elected members and to develop and maintain good interpersonal networks.	Essential
9	Ability to deal constructively with staff and members of the public where requests or matters can't be complied with for legal or security reasons.	Essential
10	Ability to be tenacious in advice and support even where this may conflict with the organisations priorities.	Essential
11	Good influencing skills with the ability to lead and motivate employees without direct authority over a team, providing clear direction and securing commitment to continuous improvement.	Essential
12	Strong organisational and time management skills to work effectively under pressure to balance own and team's priorities so that objectives are achieved to deadline and cost.	Essential

Our accreditations

Our accreditations include: The Mayor's Good Work Standard, Disability Confident Employer, London Living Wage Employer, Stonewall Diversity Champion, and Employer with Heart.