BE BOLD, MAKE A DIFFERENCE, SHOW YOU CARE

JOB ROLE PROFILE AND PERSON SPECIFICATION

Post Title and Number: Data Protection Officer

Present Grade: MM1 Dept: Law and Governance

Service/Section/Team: Legal Services

Reports to (title): Head of Legal Practice and Compliance, with dotted line to Director and Law and Governance

Purpose of the Role:

The Data Protection Officer and the Data Protection Team are part of the Law and Governance Service within the Legal Practice and Compliance Team.

Under the Data Protection Act 2018 the Data Protection Officer must operate independently to fulfil their role as an unbiased body guiding the organisation to meet the 7 Principles of GDPR. Reporting to the Head of Legal Practice and Compliance the Data Protection Officer is accountable for safeguarding personal data to ensure it is used responsibly, securely and in compliance with legal and regulatory requirements. The role is responsible to ensure that the Council and schools are advised correctly in all aspects of protecting individuals' privacy, preventing unauthorised access, and ensuring that data is processed transparently and lawfully.

The Data Protection Officer will:

- Have responsibility for delivery of the legally mandated role of Data Protection Officer for the Council and schools. The postholder will be required to register as the Data Protection Officer with the Information Commissioners Office on behalf of the Council.
- Be technically proficient as they will give advice which has legally binding consequences. The post holder must have clear expertise and ongoing professional development in data management and will be expected to hold one or more technical qualifications in data protection.
- Have accountability for the data policies within the Council and Schools, ensuring that they are reviewed at least annually or where legislation or operational changes occur.
- Have the day-to-day authority and responsibility for advising the Council and schools on compliance with the data protection laws in order that they to carry out their duties lawfully.
- Lead personally or via delegation investigation into all reported data breaches as soon as notified through to conclusion and where appropriate implement measures to prevent or mitigate reoccurrence.
- Be expected to effectively communicate, influence, and engage across all levels in the organisation ranging from the council's most senior leadership, Directors and Assistant Director and groups of staff to the Leader and Deputy Leader, Councillors and with school governors, headteachers and school staff.
- Be the data protection contact point of liaison with regulators, third parties such as police, press, suppliers, and the public.

- Have an overarching responsibility for fostering a data protection culture within the council and schools and maintain the highest standards of integrity and professional ethics.
- Maintain the corporate Data Protection and Information Governance Risk Register and ensure that risk mitigation actions are prioritised in the Data Protection Team workplan.
- Produce regular reports on data protection compliance and issues for the highest management level of both the council and schools.

The postholder must be able to independently analyse and evaluate situations, creating what-if scenarios, reasoning based on the information, experience and knowledge to arrive at one or more options, and draw effective conclusions, upon which to provide decisions at an operational and mid-term strategic level. They will be required to participate regularly in meetings of senior or middle management where decisions with data protection implications are taken.

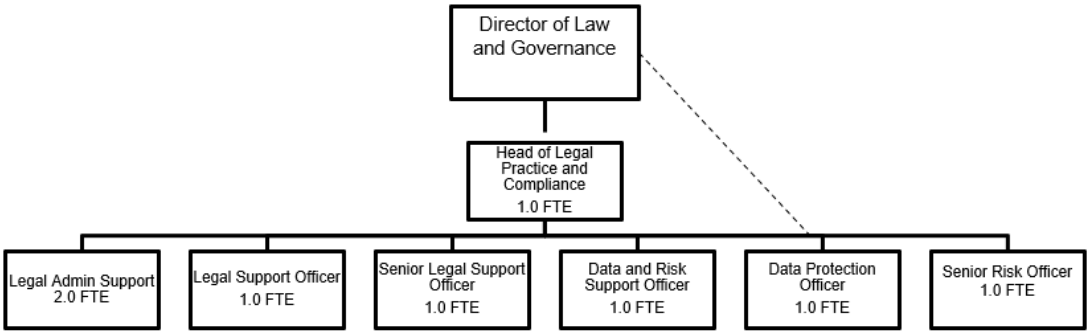
The demands of this role involve regularly managing a number of competing activities, at times with demanding deadlines and public/press/regulator involvement, on an on-going basis, with a range of complexities, from very complex to tactical, including key decisions that could result in legislative action against the council, impact the delivery of the service to the whole Council and beyond, to partner organisations.

This role is required to act alongside the Head of Legal Practice and Compliance as the communication channel to/from all data users with internal and external stakeholders, especially in the case of a major data breach. As such, there may be times when the post holder is required to be available out of hours, including weekends. Accountability for reporting and managing data breaches remains with the data owner.

Dimensions including Structure Chart:

1. Annual budgetary amounts with which the role is either directly or indirectly concerned:
   Responsible for ensuring effective and high quality delivery of the DPO service to schools and thus protecting the income of providing that service. Advice and guidance provided in the role protects the Council from potential fines from the ICO.

2. Structure Chart: The postholder will be part of the Legal Practice and Compliance Team.



3. Number of direct reports: No direct reports. The posts holder will be supported by a Legal Practice and Data Protection Paralegal. According to work volumes administration support from the wider Legal Practice and Compliance Team will be made available.

4. Nature of reporting relationship between post holder and line manager: Reporting to the Head of Head of Legal Practice and Compliance with a dotted line to the Director of Law and Governance the post holder has complete autonomy of decision making and is required to do so by law. The post holder is responsible for managing their own workload. The post holder will have a key enabling role across the organisation wherever personal data is processed. The role is free of procedural control. It supports the development of the data protection culture, including guiding the direction on a mid-term, annual and multi-year basis.

5. Any other relevant statistics: See Purpose of the Role and Key Accountabilities sections for details.

Key Accountabilities:

Accountabilities
1. Prepare and keep up to date by at least annual review all data protection policies and associated documentation which will include but not limited to; Privacy Notices, Data Processing Agreements, consent forms, Data Privacy Impact Assessments, legitimate interest assessments, Police disclosure requests.
2. Monitoring changes to the law and the data protection environment making recommendations to the Data Protection, Information and Security Strategic Governance Board when appropriate.
3. Maintain a deep understanding of the Council and school compliance with data protection laws and regulations by completing self-assessments and data protection audit.
4. Liaise directly with all areas of the business and develop influential relationships, to guarantee that the data protection culture is maintained and continuously improved.
5. Developing data protection training programs for the Council and schools with responsibility for ensuring these are implemented.
6. Collaborating with the Information Governance and Digital Security functions to raise employee awareness of information governance, data protection and security issues, and providing training on the subject matter.
7. Developing strategies and initiatives to ensure engagement with key internal and external stakeholders, this may include actions such as data protection surgeries, intranet articles, staff communication emails.
8. Accountable to ensure that each Council directorate and school have a robust Record of Processing Activity (ROPA) that is regularly reviewed and updated considering changes.
9. Take accountability for the agreed retention periods of both hard copy and digital data assets.

10. Collaborating with the Information Governance function who will maintain the Information Asset Register and are responsible for ensuring adherence to retention periods.
11. Collaborating with property services to ensure safe a secure physical document storage is available. Owners of the physical data are within the Directorates. The DPO is accountable with the Directors to ensure that data owners adhere to retention policies.
12. Deal with all reported security breaches (confirmed and near misses) by investigation, risk assessments, escalation where necessary, reporting to the regulator within timescales, notifying data subjects where necessary, providing advice and guidance to officers and training to prevent a reoccurrence where required.
13. Complete annual data protection reports, analysing trends and providing strategic advice for implementing improvements.
14. Active involvement in the end-to-end workflow process for DPIAs and sign off of all DPIA's.
15. As the subject matter expert oversee and facilitate Data Sharing Agreements, Data Processing Agreements, MOU and others ensuring compliance with regulations.
16. Accountability for a process of Police Disclosure Requests and responsibility to ensure these are completed to the highest standard. This involves working with services to ensure they provide the necessary information and that it approved before disclosure.
17. Respond to FOI, complaints or claims relating to data protection in the set timescales.
18. Collaboration with the SARs team, offering advice and guidance on specific complex SAR requests.
19. General advice to schools on subject access requests (SARs), FOIs.
20. Monitor compliance with the regulations [Article 39 (1)(b)]. This will include:
    a. collecting information to identify processing activities,
    b. analysing and checking the compliance of processing activities, and
    c. informing, advising and issuing recommendations to the organisations.
21. Ensure that they are easily accessible to all parts of the council, schools, the regulator and the data subject. [GDPR Article 37(2)]
22. Ensure they liaise with the data controllers to maintain appropriate methods and teams to meet the requirements of all the bodies they are representing, and ensure that the controller(s) are kept informed of issues with this requirement [GDPR Article 37(3)]
23. Ensure that they maintain the secrecy and privacy required for the role in handling of personal data [GDPR Article 38(5)]

24. Ensure that the contact details for the Data Protection Officer are published and available to the regulator, the public and the data subjects [GDPR Article 37(7)]
25. Provide advice in a proper and timely manner to the organisations on all issues which relate to the protection of personal data [GDPR Article 38(1)], and participate in the assessment of issues as requested by the controller [GDPR Article 35(1), 35(2), 39 (1)(c)]
26. Have due regard in providing advice for the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing [GDPR Article 39(2)]
27. Ensure that they maintain independence of their role and inform the controller of any attempts to interfere that may impact this [GDPR Article 39]
28. Maintain their knowledge and expertise in data protection law and practice commensurate with the organisational requirements of the council and schools [GDPR Article 37(5)]
29. Any other duties reasonably requested by management
30. Carry out all accountabilities in compliance with the Council's Policies and Procedures.

Key Relationships (Internal and External):

Internal

1. Councillors
2. Chief Executive
3. Directors
4. Directorate Management Teams
5. Oversight and Scrutiny Committees
6. Audit and Risk Boards
7. SIRO and Caldicott Guardian
8. Information Governance Manager and Digital Security Manager
6. Heads of Service and Business Owners
7. Officers and Service Users
8. Operational and Project Boards
9. Service Hubs and Other Council Departments
10. team members

External

1. Area forums
2. Community groups and charities
3. Digital Services partners, third-party providers and external agencies
4. Media
5. Councillors of public government/volunteer sector working groups
6. National and regional collaborative working groups
7. Partner organisations, such as Public Health, CCG, Police
8. Peer groups
9. Residents and users of Enfield council services
10. Schools
11. Service user focus groups

The post holder will be the deputy chair of the Data Protection, Information and Security Strategic Governance Board. Other members include the SIRO (chair), Caldicott Guardian, Information Governance Manager, Digital Security Manager, Head of Legal Practice and Compliance. The board remit covers assurance, decision making and escalation of issues relating to the data protection, information governance and cyber security functions.

Equality and Diversity:

The Council has a strong commitment to achieving equality in its service to the community and the employment of people and expects all employees to understand, comply with and promote its policies in their own work.

Health and Safety:

The post holder shall ensure that the duties of the post are undertaken with due regard to the Council's Health and Safety Policy and to their personal responsibilities under the provisions of the Health and Safety at work Act 1974 and all other relevant subordinate legislation.

For a more detailed definition of these responsibilities, refer to the current versions of the Corporate Health & Safety Policy, Group Safety Policy and employee information leaflet entitled "Health & Safety Policy; Guidance on Staff Health & Safety Responsibilities".

Corporate Health and Safety Responsibilities

All employees have personal responsibilities to take reasonable care for the health and safety of themselves and others. This means:

1. Understanding the hazards in the work they undertake;
2. Following safety rules and procedures;
3. Using work equipment, personal protective equipment, substances, and safety devices correctly; and
4. Working in accordance with the training provided and only undertaking tasks where appropriate training has been received.

Employees shall co-operate with the Council by allowing it to comply with its duties towards them. This requires employees to:

- take part in safety training and risk assessments and suggest ways of reducing risks; and
- take part in emergency evacuation exercises.

Employees shall report all accidents, 'near miss' incidents and work related ill health conditions to their manager/supervisor/team leader.

Employees shall read the Corporate Health & Safety – Organisation Part B Policy to ascertain and understand their responsibilities as an employee, line manager, Assistant Director or Director of the Council.

Information Security:

In order to protect the confidentiality, integrity and availability of Council information, including information provided by customers, partner organisations, and other third parties, where applicable, employees will comply with the Council's Information Security Policy.

Statement of Commitment to Safeguarding of Children and Vulnerable Adults through safer employment practice:

Enfield Council is committed to safeguarding and promoting the welfare of children and vulnerable adults. Safe recruitment of staff is central to this commitment, and the Council will ensure that its recruitment policies and practices are robust, and that selection procedures prevent unsuitable people from gaining access to children, young people and vulnerable adults. All staff employed to work with or on behalf of children and young people in the Council must be competent.

All staff working with Children & Vulnerable Adults should be aware of, and share the commitment to safeguarding and promoting the welfare of children, young people and vulnerable adults when applying for posts at Enfield Council.

PERSON SPECIFICATION

Job Title: Data Protection Officer

Grade: MM??

Department: Resources / Digital Services

Team: Service Management and Governance

KNOWLEDGE, SKILLS & ABILIES	HOW TESTED Application – A Test – T Interview – I
Job Specifics – Skills, Experience, Knowledge, Behaviours **Essential:** 1. Qualification in data protection or information security or law or equivalent training and/or certification. 2. Experience (at least 3 years) of delivering data protection services which will include drafting and updating policies and procedures, assessment of DPIA's, Data Sharing Agreements, Data Processing Agreements, dealing with disclosure requests, dealing with data breaches. 3. Demonstrable experience of providing advice and guidance at the highest levels of organisations within the business context of local government and education. 4. Experience in developing data protection training, and delivery of training. 5. Ability to engage, coach and motivate teams and set clear targets and expectations. 6. Evidence of high levels of customer service and satisfaction. 7. Experience of successfully managing performance and providing clear constructive feedback. 8. Experience of successfully implementing plans and projects to time and budget. 9. Demonstrates a good understanding of the political structure and role of elected members. 10. Ability to work collaboratively both with own service and across other services. 11. Stakeholder management. 12. Good working knowledge of using MS-365 software (Word, Excel, Outlook). 13. Exceptional English literacy (written, and verbal for customer facing roles) and numeracy skills. **Desirable:** **1.** Membership with certified ongoing professional development of a professional organisation related to data protection e.g., IAPP, NADPO, BCS, ISACA, (ISC)2	**A/I/T**

Behaviours Appropriate behaviours are key to the delivery of our vision for Enfield. We want staff who will work collaboratively, flexibly and constructively, and exhibit this ethos in all their dealings with residents, colleagues and partners. Our leaders will be exemplars of the following behaviours and encourage them in staff at all levels; **Takes Responsibility** We want staff who are willing to make decisions and be accountable for them. Staff should have a positive can-do attitude where they see problems as challenges which can be overcome. They should accept responsibility for service delivery, be clear about their service offer and deliver what they promise. **Is Open, Honest and Respectful** We want staff who are comfortable and confident to acknowledge the difficulties and the barriers they face. They should also be able to constructively challenge the way things are done where there is evidence that it impedes service delivery. Challenge should be conducted in a professional, courteous manner with the aim of reaching a mutually agreeable resolution. **Actively Listening and Learning** We want staff who are prepared to actively listen and reflect on customer concerns with a view to understanding the customer's point of view. Staff should be able to receive constructive criticism and be prepared to adapt the way they operate and deliver services where appropriate. **Working Together to find solutions** We want staff who can work collaboratively with other departments and partners, freely sharing their knowledge and skills to identify solutions to address customer concerns. **Candidates: Please ensure you address these behaviours in your responses to the essential and desirable (if applicable) criteria above.**	**A/I/T**
Competencies: **Candidates: Please ensure you address these competencies in your responses to the essential and desirable (if applicable criteria above).** 1. Provide leadership / customer focus 2. Build relationships 3. Political Awareness 4. Communicate and Influence	

5. Empower Individuals 6. Deliver Results	
Qualifications & Professional registration criteria **Candidates: Please ensure you address these qualifications in your responses to the essential criteria, you will be expected to meet these requirements of the role and they will be explored with you at interview.** 1. Higher education / college or equivalent 2. At least 1 recognised data protection qualification which may be (ISC)2 CISSP-ISSMP ISACA CISM ISACA CGEIT CESG Certified Professional in one of the data governance areas IAPP CIPP/E and CIPM	**A/I**
Special requirements **Candidates: Please note you will be expected to meet these requirements of the role and they will be explored with you at interview.** 1. Availability to work out of hours, including weekends 2. Availability to provide on call service	**A/I**