Role Profile

Role Details:

Title: Corporate Information Manager

Grade: Special B

Purpose:

The Corporate Information Manager will ensure that the Information Governance Framework is adopted and implemented throughout the Council. This will require extensive liaison and inter departmental co-operation at Corporate Board, Group Director, Elected members, external bodies and all staff levels.

Structure:

Responsible to: Head of Legal and Democratic Services

Responsible for: Principal Records Management Officer SO2, Information Governance Officers X 4 Scale 5-6

Smarter Working Profile: The work style for this role is defined as:

Hybrid: A balance between working from home and from a designated council workplace allocation, attending other workplaces as required.

Circumstances

The post holder may be required to work evenings or weekends as the needs of the service require.

This is role treated as a politically restricted post in accordance with Section 2(3) of the Local Government and Housing Act 1989.

Safeguarding

We are committed to safeguarding and promoting the welfare of children, young people and vulnerable adults and expect all staff to share this commitment.

This post is not subject to a DBS Check.

Main duties and responsibilities

1. Manage and supervise, on a daily basis, the Corporate Information Governance Team, carry out the roles of Data Protection Officer (DPO) and Senior Information Risk Owner (SIRO). Develop and supervise the team to ensure full compliance with legislation.

2. Lead the Information Governance Team on the development of Council policies, strategies, procedures and guidance on: information rights legislation, processes and procedures; information security legislation, processes and procedures; and records/archives management processes and procedures. To develop strategies and policies to overcome implementation problems that arise in the short, medium and long term.

3. Ensure the Council's legislative compliance with the Information Commissioner and that the Council is able to evidence that compliance.

4. Support the Caldicott Guardian in respect of their duties and responsibilities.

5. Present Governance Reports to CLT, Directors, Heads of Service, Chief Officers and all Council teams as appropriate. Make recommendations to CLT, Corporate Directors, Departmental Managements Teams and Senior Officers across the Council advice and guidance on legislation, codes of practice, EU directives, etc, relevant to information rights, information

security and records/archives management and establish/maintain an auditing function to ensure corporate compliance with the same.

6. Lead in the management of the Council's strategic corporate compliance with: Freedom of Information legislation, GDPR, Data Protection (including Data Subject Access Request ("SAR")) legislation, Environmental Information Regulations, Police requests, Re-use of Public Sector Information Regulations; information security legislation and records/archives management and their respective processes and procedures.

7. Lead in the management and maintenance and recall of the Council's archives currently based at the Corporate Archive Facility, promoting efficiency and effectiveness in the use of these information assets and ensuring systems and standards meet care guidelines and quality standards.

8. Lead the Council's legislative compliance with the Information Commissioner and that the Council is able to evidence that compliance.

9. Lead the Information Governance Officers in the development, implementation and maintenance of strategies to enable information sharing with partners, including the health service, private and voluntary sector, and other agencies in accordance with central government requirements,

10. Lead on the Council's annual compliance with the NHS Information Governance Toolkit in order to obtain the accreditation essential to facilitate joint working with partner organisations.

11. Develop long term action plans and strategies that will ensure the overall purpose of the post and the aims and objectives of the Corporate Information Governance Team are met.

12. Establish contacts and working arrangements with relevant national and regional groups and other Local Authorities to ensure corporate policies, procedures and guidance are in line with good practice gathered. Chair relevant Information Governance working groups and other multi-discipline and multi-agency meetings.

13. Supervise and manage via appraisals, shared conversations and one to ones the employment and wellbeing of the Corporate Information Governance Team

14. Lead on the training and development of staff within the Corporate Information Governance Team and, as appropriate, staff in other areas of the Council on information rights, information security and records/archives management (including the development of modules for inclusion in the Council's training packages and guidance for staff) to ensure that individuals achieve their highest contribution.

15. Lead on the training and development on information rights, information security and records/archives management of Members of the Council and, as appropriate and where requested, of Partner Agencies, including the development of modules for inclusion in the Council's training packages and guidance.

16. Investigation and reporting to regulatory body of all data breaches that could result in a penalty of fine.

17. Ensure that Data Protection within the Council is undertaken in a controlled, consistent and legislatively compliant manner.

18. Ensure that any internal reviews or ICO appeals are dealt with and responded to effectively and within legislative timescales to avoid penalties and fines.

19. Ensure that advice and assistance regarding Information Sharing Protocols, agreements and privacy notices are applied correctly and reviewed regularly.

20. Ensure that advice on intellectual property issues, confidentiality, copyright and other associated issues are provided in a timely and accurate manner.

STATUTORY ROLES

General Data Protection Regulations (GDPR)

The Corporate Information Manager is responsible for;

- Maintain an Information Asset Register for both paper and electronic records held by the Council
- Carrying out Privacy Impact Assessments on all new Projects involving personal data and advising on how to complete the project in a legally complaint way
- Undertaking Business Continuity Plans to inform a "Critical Systems" programme for recovery.
- Updating Information Risk Assessments for all Council Systems
- Maintaining an Information map of all Council data processing in order to create a "Record of processing Activity" (ROPA) to map the flow of information into the council and across its lifecycle journey to its destruction upon its expiry and retention period.
- Advising all areas of the Council on data protection to avoid penalties and fines
- Offering mandatory e-learning on existing and new data protection laws.
- Logging, Recording and archiving into the new store all Council paper files in line with Records management retention rules and legislation

The Corporate Information Manager will create and maintain auditable Registers for all

- Data and security breaches,
- Contracts,
- Information Sharing Agreements
- Privacy Notices
- Privacy Impact Assessments
- Re-Use of Public Sector Information Regulations
- INSPIRE Regulations
- Transparency Directive

Under GDPR there is also a statutory requirement for the appointment of a Data Protection Officer (DPO) within public bodies employing in excess of 500 people.

DATA PROTECTION OFFICER (DPO)

Under the GDPR, it is a mandatory designation for all public authorities and bodies to appoint a DPO. The DPO will have the equivalent autonomy and resource as the s.151 officer. *Article 39* entrusts the DPO with the duty to monitor compliance with the GDPR. As part of these duties to monitor compliance, DPOs must, in particular:

1. Collect information to identify and map processing activities

2. Analyse and check the compliance of processing activities inform, advise and issue recommendations to the controller or the processor

3. Carry out data protection impact assessments,

Article 39 states that the DPO should '*cooperate with the supervisory authority*' and '*act as a contact point for the supervisory authority (ICO) on issues relating to processing and data protection issues.* The contact details of the DPO should also be made public on all Privacy Notices so that individuals are aware of the Complaints procedure in terms of data breaches.

The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil his or her tasks.

The DPO will ensure that policies and procedures are kept up to date and plans/schedules data processing audits regularly, monitoring core activities to ensure they are compliant with the EU GDPR.

The DPO will liaise with all members of staff on matters of data protection.

Key tasks of the DPO:

a. Inform and advise Calderdale Council, and its relevant partners and suppliers, on data protection and compliance with the Regulation and UK laws.
b. Inform and advise all members of staff on their obligation to adhere to the EU GDPR and UK law(s) when dealing with personal data.
c. Monitor compliance with the EU GDPR and UK law(s).
d. Contribute to the development and maintenance of all v data protection policies, procedures and processes in relation to the protection of personal data.
e. Allocate responsibilities internally to support ongoing compliance with the EU GDPR and UK law(s).
f. Ensure training and awareness is available and delivered to all members of staff involved in processing operations relating to personal data.
g. Regularly monitor compliance with the EU GDPR and UK data protection law(s) by conducting audits of processes relating to personal data, and report CLT
h. Advise and inform on the data protection impact assessment and monitoring performance against the requirements of the EU GDPR.
i. Liaise and cooperate with the supervisory authority [ICO].
j. Be the point of contact for the supervisory authority on issues relating to processing of personal data, and to consult with the supervisory authority, where necessary, on any other personal data matters.
k. Monitor compliance with the policy throughout Calderdale Council and to develop / advise on procedures for effective security.
l. Advise on the allocation of information security responsibilities.
m. Develop / advise on formal procedures for reporting incidents (EU GDPR and information security related) and investigations.
n. Contribute to the business continuity planning process.
o. Advise on the control and monitoring of copying of proprietary software.
p. Advise on and monitor the safeguarding of organisational records.
q. Ascertain the extent to which personal data is collected, held and/or used in Calderdale Council, and that it is properly controlled and safeguarded from loss of confidentiality, integrity or availability from any cause.

The DPO must have the resources necessary to be able to carry out their tasks.

Depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO:

- active support of the DPO's function by senior management
- sufficient time for DPOs to fulfil their tasks
- adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate
- official communication of the designation of the DPO to all staff
- access to other services within the organisation so that DPOs can receive essential support, input or information from those other services
- continuous training

Several safeguards exist in order to enable the DPO to act in an independent manner:

- no instructions by the Council Management regarding the exercise of the DPO's tasks
- no dismissal or penalty by the Council Management for the performance of the DPO's tasks

The DPO must be allowed to perform tasks in an independent manner and should not receive any instructions regarding the exercise of their tasks. They report to the highest management level in the Council and cannot be dismissed or penalised for doing their job.

The DPO is authorised to have access to all the Councils systems relating to the collection, processing and storage of personal data for the purpose of assessing the use and security of personal data. The Data Protection Officer may expect the cooperation of all staff in carrying out these duties, including access to systems and records.

SENIOR INFORMATION RISK OWNER (SIRO)

The role of the Senior Information Risk Owner (SIRO) was introduced by the Cabinet office resulting from a data handling review in May 2008. This is a statutory post and is required by the Information Governance NHS Toolkit (IGT) to strengthen information assurance controls and applies to all organisations completing the IGT and processing NHS patient information.

The nominated person should be a Senior Manager who is familiar with information risks and the organisation's response to risk. The role of the SIRO is to take strategic Corporate Information Manager ownership of the organisation's information risk policy, act as an advocate for information risk and provide written advice on the content of their organisations annual governance statement in regard to information risk.

The aim is to ensure that the approach to information risk management:

- Takes full advantage of existing authority and responsibility structures where these are fit for this purpose;
- Associates tasks with appropriate management levels;
- Avoids unnecessary impacts on day to day business;
- Ensures that all the necessary activities are discharged in an efficient, effective, accountable and visible manner.

The responsibilities of the SIRO:

1. The Councils Senior Information Risk Owner (SIRO) is responsible for coordinating the development and maintenance of corporate information risk management policies, procedures and standards for the Council.

2. The SIRO is responsible for the ongoing development and day-to-day management of the Council's Risk Management Programme for information privacy and security.

3. The SIRO is responsible for the successful completion of the NHS Information Governance Toolkit submission to ensure adequate legal compliance and security standards are in place to promote the continued access and sharing controls of data between both organisations.

4. The SIRO is responsible for the strategic planning and advising of identified corporate risk from manual and electronic information systems and handling.

5. The SIRO is responsible for signing all Information Sharing Agreements on behalf of the Council between the Council and all third party organisations.
6. The SIRO is responsible for Leading and fostering a culture that values, protects and uses information for the success of the Council and benefit of its customers

7. The SIRO is responsible for owning the Council's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by Information Asset/System Owners

8. The SIRO is responsible for owning the organisation's information incident management framework

9. The SIRO shall advise the Chief Executive, CLT, DMT's and Extended Management team and the Council on information risk management strategies and provide an annual report to CLT.

10. Service Managers/System Owners shall ensure that information Risk Assessments and Privacy Impact Assessments (PIA's) are performed at least once each year on all information assets where they have been assigned 'ownership', following guidance from the SIRO. Service Managers/System Owners shall submit the assessment results and associated mitigation plans to the SIRO for review, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks. The data created by the Service Managers/System Owners will inform and update the Information Governance Risk Register in accordance with the Council's Information Risk Management Policy Statement and Strategic Framework.

11. The SIRO policy is applicable to all areas of the Council and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

Councils are required to ensure their appointed SIRO possesses the necessary knowledge and skills to undertake their role effectively and to provide periodic evidenced statements of information assurance for the annual Statement of Internal Control. The SIRO should undertake information risk management training at least annually to be able to demonstrate their skills and capabilities are up to date and relevant to the needs of the organisation.

This is not a complete statement of all duties and responsibilities of this post. The post holder may be required to carry out any other duties as directed; the responsibility level of any other duties should not exceed those outlined above.

Qualification Criteria

Candidates: Must meet all essential qualification criteria to be evidenced in the application form.

Qualification Criteria	Essential	Desirable	How Identified
Relevant Law Degree or relevant and demonstrable experience in a similar role	X		Application / Interview
Certified GDPR Practitioner Training		X	

Person Specification

Candidates: Evidence how you meet the below requirements in your personal statement.

Shortlisting Criteria (including applied knowledge and experience)			
Expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR	X		Application / Interview
Experience of and understanding of the processing operations carried out	X		
Understanding of information technologies and data security	X		
Knowledge of a large diverse organisations and its statutory duties	X		
Proven experience of promoting a data protection culture within the Organisation	X		
Personal resilience and adept at managing competing deadlines to enable delivery of projects to specification, on time and within budget.	X		
High level of competency in the use of computer systems	X		

Strong communication, negotiation, and analytical skills	X		
Experience of working in accordance with legislation and statutory obligations	X		
Proven ability to use IT packages including standard Microsoft Office software	X		

Role Profile prepared by/author: Ian Hughes Date:24/03/2026
Job title: Head of Legal & Democratic Services

Signed by (Recruitment & Resourcing team member): Date:24/03/2026
Name: Michelle Newman

Job Evaluation Ref: JE285

All staff will be expected to maintain high standards of customer care in the context of the council's Core Values, to uphold the Equality and Diversity Statement and to participate in training activities necessary to their post.

The Health and Safety at Work Act 1974 and associated legislation places responsibilities for health and safety on Calderdale Council, as your employer and you as an employee of the Council. In addition to the Councils overall duties, the post holder has personal responsibility for their own health & safety and that of other employees; additional and more specific responsibilities commensurate with your role are identified in the Council's Corporate H&S policy and in you are required to familiarise yourself with these responsibilities.

Calderdale Council is a NO SMOKING Employer - Smoking will not be permitted on Council premises and grounds, and there will be no provision made for employees who wish to smoke.

All Calderdale staff will operate within the GDPR data protection guidelines.