RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

ROLE OF THE INFORMATION ASSET OWNER (IAO) - GUIDANCE FOR HEADS OF SERVICE

Version: FINAL V2

1. Introduction

Information is one of the Council's most valuable assets. Managing it effectively is essential for delivering high-quality services, maintaining public trust, and complying with legal and regulatory requirements such as the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Freedom of Information Act.

This guidance explains the role and responsibilities of Information Asset Owners (IAOs) within the Council. IAOs are senior officers, typically Heads of Service, who have ultimate accountability for the information assets within their service area. Their role is critical to ensuring that information is:

- **Identified and valued** as an asset
- **Protected and used lawfully, fairly, and securely**
- **Managed throughout its lifecycle**, from creation to disposal
- **Shared responsibly** to support service delivery and public good

By following this guidance, IAOs will help the Council meet its statutory obligations, reduce risk, and foster a culture that values and safeguards information.

2. Why Do We Need Information Asset Owners?

Information Asset Owners play a vital role in ensuring that the Council manages its information responsibly and securely. The role was introduced following the Cabinet Office's Data Handling Review and remains essential today for several reasons:

- **Legal Compliance**
  IAOs help the Council meet its obligations under UK GDPR, the Data Protection Act 2018, and the Freedom of Information Act. These laws require clear accountability for how information is collected, stored, shared, and disposed of.
- **Risk Management**
  Information is a critical asset, and poor handling can lead to data breaches, reputational damage, financial penalties, and loss of public trust. IAOs provide assurance that risks are identified and managed effectively.
- **Accountability and Governance**
  IAOs ensure that information assets have a named owner who understands their value, sensitivity, and associated risks. This supports transparency and strengthens governance across the Council.
- **Public Trust and Service Delivery**
  By safeguarding information and using it appropriately, IAOs help maintain confidence in council services and ensure that information is used for public good.

3. Who Are the Council's Information Asset Owners?

Information Asset Owners are senior officers within the Council who have ultimate accountability for the information assets in their service area. This responsibility is typically assigned to **Heads of Service** or above, as they have the authority to make decisions about how information is managed, shared, and protected.

IAOs work closely with:

- **Senior Information Risk Owner (SIRO)** – Provides overall leadership on information risk and assurance.
- **System Administrators and Business Application Leads –** Manage key business systems and ensure that access controls and configurations align with security and governance requirements.
- **ICT Information Security Team** – Advises on technical and organisational measures to protect information and supports compliance with security standards.
- **Information Management Team** – Offers guidance, tools, and oversight to ensure compliance with council policies and legal requirements.

By assigning IAOs at this level, the Council ensures that information governance is embedded in service delivery and that accountability for information risk sits with those who understand the operational context.

4. The Role of an Information Asset Owner

Information Asset Owners provide leadership and accountability for the Council's information assets. Their role is strategic and ensures that information is treated as a valuable resource, managed in line with legal requirements and organisational policies.

Key aspects of the role include:

- **Ownership and Accountability**
  IAOs are the named individuals responsible for the information assets within their service area. They make decisions about how information is collected, stored, shared, and disposed of.
- **Assurance and Risk Management**
  IAOs provide assurance that information risks are identified, assessed, and managed effectively. This includes supporting governance processes and contributing to annual assurance statements.
- **Compliance and Ethical Use**
  IAOs ensure that information is used lawfully, fairly, and transparently, in line with UK GDPR, the Data Protection Act 2018, and other relevant legislation. They also promote ethical use of information for public good.

- **Collaboration**
  IAOs work with the ICT Information Security Team, system administrators, and the Information Management Team to implement appropriate controls and maintain compliance.

By fulfilling these responsibilities, IAOs help the Council protect its information, reduce risk, and maintain public trust.

5. Core Responsibilities of an Information Asset Owner

IAOs have a critical role in ensuring that information assets are managed securely, lawfully, and effectively. The main responsibilities include:

1. Identify and Document Information Assets

- Maintain an accurate **Data Protection Register** for each processing activity.
- Record details such as processing activity, lawful basis, personal data categories, retention period etc.

2. Manage Risks and Ensure Compliance

- Assess risks associated with each asset and apply appropriate controls.
- Ensure compliance with UK GDPR principles and other legal requirements.
- Implement technical and organisational measures to protect confidentiality, integrity, and availability.

3. Report Incidents Promptly

- Report any suspected data breach, loss of information, or security incident immediately in line with Council procedures.
- Support investigations and remedial actions.

4. Control Access

- Define and manage user access permissions based on business need and sensitivity.
- Ensure physical and system security measures are in place.

5. Oversee Information Sharing

- Ensure any sharing of personal or sensitive information is lawful and documented.
- Use formal Information Sharing Agreements aligned with WASPI (Wales Accord on Sharing Personal Information).

6. Apply Retention and Disposal Rules

- Follow the Council's Retention and Disposal Policy.
- Ensure secure destruction of records when no longer required.

7. Promote Awareness and Training

- Ensure staff accessing information assets complete mandatory Information Management and Security training.
- Promote compliance with Council policies and acceptable use standards.

8. Support Digital Continuity

- Plan for system changes or migrations to ensure information remains accessible and usable over time.

6. Governance and Reporting

Strong governance ensures that information risks are managed consistently across the Council. Information Asset Owners play a key role in this framework by providing assurance and escalating issues where necessary.

Escalation of Risks and Incidents

- Significant risks or breaches must be escalated promptly to the Information Management and Information Security Teams.
- IAOs should ensure that incidents are logged and investigated in line with Council procedures.

Regular Reviews

- IAOs should review their Information Asset Register regularly and update it whenever new systems or processes are introduced.
- Risk assessments should be refreshed regularly to reflect changes in technology, legislation, or service delivery.

Audit and Assurance

- IAOs may be asked to provide evidence of compliance during internal audits or external inspections.
- Maintaining accurate records and demonstrating adherence to policies is essential for assurance.

7. Supporting Resources

To help Information Asset Owners fulfil their responsibilities, the following resources and tools are available:

Templates and Registers

- **Data Protection Register Template**
  A standard template for recording details of each processing activity.
- **Retention and Disposal Policy & Toolkit**
  Guidance on how long records should be kept and the approved methods for secure disposal.

Council Policy Framework

The Council has a comprehensive policy framework in place to support IAOs in managing information securely and lawfully. This includes, but is not limited to:

- Information Security Policy
- Data Protection Policy
- Data Protection Impact Assessment (DPIA) Policy
- Information Sharing Protocols
- Acceptable Use Policies

These policies set out clear standards and procedures for handling information assets throughout their lifecycle.

Internal Advice and Support

IAOs are supported by specialist teams and officers who provide guidance and expertise:

- **Information Management Team /** Data Protection Officer (DPO)
  Provides advice on information governance, information sharing, and compliance with UK GDPR and other data protection legislation.

- **Information Security Team / Information Security Officer**
  Offers guidance on technical and organisational security measures, risk assessments, and incident response to ensure information assets are protected against threats.

External Guidance

- ICO Accountability Framework – Information Asset Register
- Cabinet Office – Data Handling Procedures in Government
- National Archives – Digital Continuity and IAO Guidance