I would like to make a Freedom of Information Act request for the following information:

1. Name, title and contact details of the Councils Senior Information Risk Owner	Paul McKevitt Deputy Chief Executive & Director of Resources, P.McKevitt@wigan.gov.uk
2. A Copy of the 2020/21 and 2021/22 Annual SIRO report – this may be a standalone report or part of another report e.g. Annual Governance Statement, if so please provided a copy of the AGS for 2020/21 and 2021/22.	The SIRO does not produce an annual report. However, the Council's Annual Governance Statement covers the areas that a SIRO would report on. The Annual Governance Statements for 2020/21 and 2021/22 are available at:- Governance (wigan.gov.uk)
3. A copy of the Councils current Information Risk Policy.	The Council does not have a document called Information Risk Policy. The Council's Information Governance Framework is attached.

Information Governance Framework

Author: [redacted]
Date: 30th September 2022
Version 4.0

Version Control		
Document Title	Information Governance Framework	
Purpose	To provide an accountability framework for information governance at Wigan Council	
Date of Approval	28th September 2022	
Valid Until	28th September 2024	
Owner	Data Protection Officer	
Approver	Information Governance Operational Group (Chair – SIRO)	
Distribution Method and Responsibility	Intranet and Internal Comms Update (tbc) [redacted]	
Version	**Date**	**Comments**
1.0	Approved by ISWG 20th May 2011	Issued by NetConsent 13th October 2011
2.0	September 2019	
3.0	December 2019	Consistency with other policies
4.1	June 2022	Stakeholder consultation
4.2	August 2022	Review after stakeholder consultation
4.3	September 2022	To IGOG
4.0	September 2022	Approved by IGOG

1. Purpose

To provide an accountability framework for information governance at Wigan Council.

2. Scope

Information is a vital asset for the provision of services to the public and for the efficient management of Council services and resources. As well as rights to access public and personal information, it plays a key part in governance, service planning and delivery and performance management.

Governance is about how the Council ensures it is doing the right things, in the right way, for the right people, in a timely, inclusive, open and accountable manner.

CIPFA consider that *"Good governance leads to good management, good performance, good stewardship of public money, good public engagement and ultimately good outcomes for citizens and service users".*

Information governance is concerned with how information is held, obtained, recorded, used and shared by the organisation. Information Governance, including physical, personal, and information security assets is an essential enabler to ensure that the Council and its partners operate legitimately, efficiently, and effectively. All associated security risks must be managed effectively, collectively, and proportionately, to ensure core regulatory and Council standards are achieved and Council actions demonstrate public accountability and confidence.

It is essential that the Council has a robust information governance framework, to ensure that information is effectively managed with accountability structures, governance processes, documented policies and procedures, staff training and adequate resources.

Ultimate responsibility for all aspects of Information Governance lies with the Cabinet and Senior Management Team. However, all officers have a responsibility to ensure that through their decisions and actions Council information assets (physical, personal, and information security) are protected in a proportionate manner.

The Council's Information Governance Framework consists of specific policy documents (detailed below) covering all aspects of information security and risks, data handing, acceptable use, and reporting protocols allied to other generic Council policies and codes.

3. Roles and Responsibilities

Cabinet and Portfolio Holder

The Cabinet, also known as the Executive, is the main policy-making body of the Council and carries out Council functions that are not the responsibility of any other part of the Council, whether by law or under the constitution.

The Cabinet has overall responsibility for the strategic management and effective governance of all Council services including the strategic context in which organisational process documents are approved and establishing a scheme of governance for the formal review and approval of such documents.

The Cabinet consists of eight senior Councillors who are each 'Portfolio Holders' for a major area of responsibility and seven Lead Members who have designated responsibility. The Portfolio Holder for Resources, Finance, and Transformation has responsibilities including information, data protection and IT.

Chief Executive and Strategic Management Team

The Chief Executive is the Head of Paid Service who leads the Council's staff and advises on policies, staffing, service delivery and the effective use of resources. The Chief Executive and Directors form the Council's Corporate Board, known as the Strategic Management Team, ensuring delivery of an effective Council-wide information management approach.

Senior Information Risk Owner

The Council's Senior Information Risk Owner (SIRO) is the Deputy Chief Executive and Director of Resources who has overall responsibility for managing information risk in the Council. This includes ensuring:-

- that an overall culture exists that values and protects information within the Council
- that information governance compliance with legislation and Council policies
- the provision of a focal point for managing information risks and incidents
- the Chief Executive is advised of any information risk aspects and reporting annually within the Council's Annual Governance Statement

The SIRO chairs the Council's Strategic Information Governance Oversight Group and Information Governance Operational Group.

Caldicott Guardian

The Council's Caldicott Guardian is the Director – Adult Social Care and Health and is responsible for ensuring that all personal/patient identifiable information handled by social care and public health services, are compliant with existing law and standards and they act to safeguard the rights of service users. The Caldicott Guardian ensures that appropriate information governance policies are in place for their services and they are adhered to by all staff and external care providers in their service areas.

Data Protection Officer (DPO)

The Council's Data Protection Officer is the Strategic Lawyer – Resources (Deputy Monitoring Officer). The Data Protection Officer is a statutory role required for all public authorities by the Data Protection Act 2018 and the DPO must report to the highest management level within the Council. The DPO is required to be independent, monitor internal compliance, inform and advise on the Council's data protection obligations, approve and provide advice regarding Data Protection Impact Assessments (DPIAs)

and act as a contact point for data subjects and the regulatory authority, the Information Commissioner.

Information Asset Owners (IAOs)

Each Assistant Director is an Information Asset Owner who is accountable to their Director for information systems and information assets within their service area to ensure ownership, access, usage and transfer to ensure business is transacted within an acceptable level of risk.

They are able to understand how information is held, used and shared and address risks to the information. They are also required to provide an annual assurance statement covering a wide range of information governance issues including any issues of concern during the year and how they were addressed. Each assurance statement is then submitted to the responsible Director to support their own Directors Assurance Statement that in turn informs the Council's Annual Governance Statement.

Information Asset Managers (IAMs)

The ultimate responsibility for information governance sits with the Information Asset Owner (and the Director) but the Information Asset Manager can undertake the agreed processes delegated by the IAO. It is up to the IAO to determine the appropriate seniority of the IAMs in their area, but they should normally be managers who have the authority to ensure compliance by more junior staff.

Service Manager ICT Service Delivery

To work with Information Governance and others to ensure the development, integration and implementation of ICT projects is managed and delivered effectively meeting the needs of technical and business stakeholders whilst managing stakeholders' expectations. To provide a productive line of communication between IG and the various ICT teams, including but not limited to security, bring into service and applications.

Line Managers

All managers with line management responsibility must ensure their staff comply with all Council Information Governance policies. Staff should refer personal data breaches to them for onward reporting to the responsible Assistant Director and the Data Protection Officer.

All Staff

All staff must be aware of and comply with relevant Information Governance policies and procedures. Staff is understood to include all employees, secondees, volunteers, agency staff, work experience students and any other individuals working for the Council on a contractual basis. Elected members (Councillors) are also covered by the policy.

4. Corporate Information Governance Bodies

To ensure that the Council continues to maintain effective governance arrangements and related procedures across all of its activities and priorities ensuring compliance with the Data Protection Act 2018 and other privacy and information legislation, an Information Governance Operational Group (IGOG), chaired by the SIRO, has been established and meets every two months. A more strategic group – the Strategic Information Governance Oversight Group, also chaired by the SIRO – meets as required to consider any matters referred to it by IGOG.

Strategic Information Governance Oversight Group (SIGOG) Responsibilities

- To meet as required, at the request of IGOG or the SIRO to

  - consider negative performance trends requiring a corporate focus.
  - be advocates for and promote compliance with data protection policies across the Council.
  - support and promote the completion and maintenance of the Record of Processing Activities and Information Asset Registers in each directorate.
  - consider the implications of serious data breaches or other data incidents when there are corporate lessons to be learnt
  - review and recommend onward reporting to Strategic Management Team and/or Members.

Information Governance Operational Group (IGOG) Responsibilities

- To ensure that the Record of Processing Activities is maintained as the definitive record of all personal data processed by the Council and the Information Asset Register for non-personal data.
- To review, maintain and approve IG and data protection policies and procedures.
- To consider data breach, subject access and FOI notifications to the ICO, ensuring any recommendations made by the ICO are implemented.
- To take an overview of training requirements and provision in data protection and information governance matters.
- To receive performance data reports on personal data breaches, freedom of information requests and subject access requests.
- To identify trends and areas of concern for referral to SIGOG and/or SMT.

Audit, Governance and Standards Committee

Article 9.06 of the Council's Constitution establishes an Audit, Governance and Standards Committee. Inter alia, this committee provides independent assurance of the governance arrangements of the Council and its services which includes Information Governance. Accordingly, a report is made each year detailing the structures and processes in place to ensure compliance with data protection legislation and providing an overview of performance and key themes in personal data breaches, freedom of information and subject access requests.

This committee also receives the Directors' Annual Assurance Statement, including the Information Asset Owners' Assurance Statements confirming that the following responsibilities were followed throughout the particular financial year:-

- Managing security, compliance and risks associated with their information assets
- Carrying out an annual assessment of 'information risk'
- Maintaining Information Asset Register and Record of Processing Activities
- Ensuring that appropriate data sharing and data processing agreements are operating and DPIAs are evident in respect of new projects/contracts
- Ensuring that data is transferred securely
- Ensuring that user access rights to systems are regularly reviewed
- Ensuring that all staff have accepted all Council related policies and have completed the Council's mandatory E-learning, Cyber Security Awareness and other related courses,
- Ensuring that information security incidents are reported promptly and appropriate actions are taken to remedy data breaches and incidents
- Reviewing service specific document/information retention and disposal schedules.
- Ensuring that Freedom of Information and Subject Access requests are processed effectively
- Ensuring that business continuity management system restore priorities are managed effectively

5. Key policies

The key policies in the framework are the:

- Data Protection Policy – *aimed at all staff to enable those working with information to have an effective understanding of their obligations regarding confidentiality and data security.*
- Information Rights Policy – *aimed at the public to outline how the Council and its staff deal with the public's information rights*.
- Information Compliance Policy – *aimed at all staff to demonstrate the policies and processes that the Council and its staff will follow with regards to information compliance, including protecting personal data*.
- Information Security Policy – *aimed at staff to protect the Council from cyber security issues that may have an adverse impact on the Council.*

6. Information Governance Resources

The Information Governance Team provides expert advice and guidance to all staff on all elements of Information Governance, viz.-

- Developing the Information Governance Framework and all associated policies, standards and procedures, including integrating government and Information Commissioner specific information governance guidance, policies and codes of practice into Council policy.

- Ensuring compliance with Data Protection, Freedom of Information, Records Management, Information Security and other information related legislation.
- Processing of Freedom of Information and Subject Access Requests in accordance with legislative requirements, providing advice to services, as required
- Facilitation of the investigation of all reported data breaches to ensure Council policy is followed consistently and reporting periodically to the Information Governance Operational Group and other Governance Bodies as appropriate.
- Providing advice and guidance on all aspects of information governance and data protection to all staff.
- Supporting the Information Asset Owners and Information Asset Managers to maintain and review the Record of Processing Activities
- Providing support and guidance to all staff on data sharing and data processing agreements, data protection impact assessments and data protection contractual clauses
- Working with Council information groups and directorate teams to establish protocols and agreements on how information is to be used and shared.
- Developing information and data protection awareness and providing training sessions for staff.
- Providing support to the Council's information governance lead officers, viz.
  a. Senior Information Risk Owner
  b. Data Protection Officer
  c. Caldicott Guardian
- Producing an Annual Information Governance report to Members via the Audit Governance & Standards Committee and providing other reports to Council committees on Information Governance, as required

The Chief Technology & Information Officer is responsible for the technical and cyber security management of the infrastructure and also all technical security advice.

7 Guidance and Associated Training

Information Governance training for all staff will be mandatory as part of induction and delivered through the Core Learning offer.

This training will comprise two elements - (i) Data Protection and Information Governance and (ii) Cyber Security. Both will be required to be refreshed annually through the Core Learning offer.

Other training and awareness sessions on any aspect of information governance may be given to staff as required, at team meetings or other sessions provided by Directorate Management or the Information Governance Team.

Regular reminders on information governance topics are made through Team Time, corporate and local team briefings, MyTime sessions, staff news, other web-based information and/or specific emails.

8. Review

This policy will be reviewed two years after approval date unless legislative, regulatory or case law changes require an earlier review.