Appendix 1 – Annual SIRO Report

Contents

Executive Summary

This report presents the annual Senior Information Risk Owner (SIRO) report. This type of report is seen nationally as good practice to inform Senior Leaders and Elected Members of information governance challenges and to satisfy regulatory requirements.

The report has been produced to demonstrate legislative and regulatory requirements relating to the handling, quality, availability, and management of information.

This report details the responsibilities of the Senior Information Risk Owner (SIRO), this role is occupied by The Director of Law and Corporate Services. The Deputy SIRO is Assistant Director Digital, Data and Technology. The report details activity and performance related to information governance, providing assurances that information risks are being effectively managed; details current activity and explains where improvements are required.

Wirral Council is committed to effective information governance and strives to ensure robust arrangements are in place to ensure the council complies with legislation and adopts best practice. Governance arrangements are monitored and reviewed to ensure systems, policies and procedures are fit for purpose and emulate best practice. The Council is equally committed to ensuring all Officers and Elected Members understand the importance of information governance.

The report details the creation and maintenance of an up-to-date redesigned Record Of Processing Activities (ROPA), which incorporates the Council Information Asset register (IAR).

Cyber security risks remain high on the agenda and pose a real threat to the Council. This report details how the Council manages those risks, including a summary to list action already undertaken and further activities planned.

Performance in relation to information requests processed under Freedom of Information (FOI), Environmental Information Regulations (EIR) and Data Protection legislation is summarised in this report. The report also provides an update on changes implemented in this area to strengthen the resources available to meet the high demand for requests, information and advice/support.

The number of data breaches reported for the time periods January 2023 to June 2024 are included in this report. Breaches are discussed at weekly meetings of the Information Management Team, to ensure continuous monitoring takes place to identify learning or process changes that may be required to reduce the risk of further breaches occurring.

Building on the work done in 2023/24, a number of actions were implemented to ensure the governance framework remains robust and the Council is able to demonstrate its commitment to compliance. These actions include:

- Change of Directorate for IMT into Law and Corporate Services.
- Additional resources for IMT of 1 x full time Officer and 1 x 12 months fixed term Officer.
- Review of all Council Privacy Notices.
- Update and maintenance of the redesigned ROPA, which includes the IAR.
- Responsibility of DSPT to remain as a shared responsibility between Health and Social Care & Law and Corporate Services.

- Introduction of Civica Icase for recording and reporting information requests and security incidents.
- Cessation of the traded service for DPO
- Establishment of new governance arrangements amongst the officer core to separate out consideration of the strategic information management issues and operational information management issues.

1. Introduction

The SIRO Report reflects on the Council's information governance work undertaken during 2023/24 which includes:

- an overview of key performance indicators relating to the Council's processing of information requests
- an update on the plans the Council has in place to minimise risk
- providing assurance of ongoing improvement to manage information risks
- information on organisational compliance with, and performance against, the legislative and regulatory requirements relating to the handling and processing of information in respect of:

  - Data Protection Act 2018 including the requirements of UK GDPR
  - Freedom of Information Act 2000
  - Environmental Information Regulations 2004
  - NHS Data Protection Toolkit DSPT
  - Any Security Incidents requiring notification to the regulator – Information Commissioners Office (ICO)

2. Key Roles and Responsibilities

SIRO
The Director of Law and Corporate Services is the SIRO and is responsible for:

- Leadership and overall ownership of the Council's Corporate Governance Action Plan, acting as corporate champion for information governance
- Providing a focus for the management of information governance at a senior level
- Providing advice and reports in respect of information incidents and risks, including the content of the Council's Annual Governance Statement
- Owning the management of information governance and risk assessment processes within the Council
- Understanding how the strategic priorities of the Council may be impacted by information governance risks, and how these risks need to be managed including the adequacy of resources and levels of independent scrutiny.

Deputy SIRO
The Deputy SIRO is the Assistant Director of Digital Data & Technology and supports the work of the SIRO.

DPO
The Governance and Compliance Manager is the DPO and is responsible for:

- Ensuring the Council's implementation of policies, standards and procedures for Information Governance ensures reduced risk of legal action from either individuals

or regulators.

- Creating and maintaining the Council's statutory records of data processing activities and information asset register to ensure the Council is not acting outside of its powers.

- Acting as the prime contact with the ICO and individuals in the investigation of data protection complaints and breaches to reduce the risk of monetary penalty, legal enforcement, and reputational risk.

- Identifying key control failings / weaknesses and provide support to senior managers to adopt new practices and procedures to improve operational performance and reduce risk.

The DPO, SIRO and Deputy SIRO meet on a regular basis to ensure any existing or potential issues relating to Information Governance are discussed and appropriate actions put in place.

Information Asset Owners and Administrators

The Councils information assets are defined as a body of information, defined and managed as a single unit, so that it can be understood, shared, protected and exploited effectively. An asset can be a single significant document or a set of related data, documents or files; it can be shared or be confined to a specific purpose or organisational unit.

An Information Asset Owner (IAO) is a senior member of staff who is the nominated owner for one or more identified information assets. It is a core Information Governance (IG) objective that all Information Assets of the organisation are identified and that the business importance of those assets is established.
IAOs will work closely together to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities. This is especially important where information assets are shared by multiple parts of the organisation.
IAOs will support the organisation's SIRO in their overall information risk management function as defined in the council's Information Risk Policy.
The IAO is expected to understand the overall business goals of the organisation and how the information assets they own contribute to and affect these goals. The IAO will therefore document, understand and monitor:

- What information assets are held, and for what purposes.
- How information is created, amended, or added to over time.
- Who has access to the information and why.
- Understand and address the risk to the asset, providing assurance to the SIRO.

The Information Asset Administrator's (IAA) primary role is to support the IAO to fulfil their responsibilities. IAAs will ensure that policies and procedures are followed, recognize actual or potential security incidents, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date.

3. Governance and Monitoring Arrangements

The SIRO is supported via two key groups: the Corporate Governance Group (CGG) and the Information Governance Board (IGB). The CGG is a high-level strategic group that seeks to ensure proper arrangements are in place for the oversight of Information

Governance matters within the Council. This includes receiving updates on key issues from the IGB.

The IGB monitors Information Governance performance and promotes Information Governance across the Council.

More specifically the responsibilities of the IGB are:

- Ensure that effective information governance / risk management and IT governance arrangements are in place.
- Ensure that the Council complies with statutory information governance provisions and that these are being applied across the Council.
- Embed a culture of information ownership and accountability.
- Ensure that the Council adopts industry best practice and aligns its work programme to the Council's strategic objectives.
- Share intelligence, identify opportunities for joint working and support management teams to identify baselines for improvement.

4. Risk Management and Assurance

The Council's Corporate Risk Register (CRR) contains a specific risk in relation to Cyber Security, as well as a general risk around the compliance with corporate policies and procedures. This second risk includes controls in relation to Information Governance/Management policy. The CRR is reviewed on a regular basis by the Council's Senior Leadership Team and reported to the Audit and Risk Management Committee.

Part of the assurance of the Council's arrangements is carried out by the Internal Audit Team, which has a dedicated IT Programme Auditor. Recent audit reviews during 2022/23 have included: -
Merseyside Pension Fund Cyber Assurance
CCTV Control Room
Liquidlogic – (Children's)Access Controls
Electoral System Access Controls
Payroll System Access Control Review

5. Corporate Governance Actions

The council is committed to a clear strategy and sustainable framework for Information Governance across the council. Performance reports are made available via Dashboards to the Senior Leadership Team to enable continuous monitoring of the actions required to manage information issues, risks and cultural behaviour to improve the Council's arrangements around data handling, processing and security.

In summary, the following key actions were delivered 2023/24 which have strengthened the Council's management of information risks.

- Staff in Wirral's Adult Care and Health are required to complete essential training called 'NCSC Staying Safe Online' on an annual basis. The target for completion is 95% of staff and this was achieved in both 2023 and 2024.

- The NHS requirement is for an annual submission to be provided by the authority to show compliance with their Data Security & Protection Toolkit (DSPT). Wirral provided its submission on time in June 2024.

- The DPO chairs a weekly meeting to consider all data breaches reported and advises on whether a self-referral of the incident to the Information Commissioner's Office(ICO) is appropriate.

6. Data Breach Management and Reporting

Any concerns relating to potential data breaches are promptly investigated and assessed against the ICO guidance of numbers of people affected, sensitivity, nature of breach and likely impact. Dependent on the assessment, the incident may need escalation to the SIRO and may be self-referred to the Information Commissioner's Office (ICO). The reporting, containment actions, investigation and learning outcomes of data breach incidents play a key role in the management of risk and improvement of internal controls. Data breach statistics are reported each month to Wirral Intelligence Service for inclusion on the DMT Insight App.

All breaches and near misses are reported to the DPO on a weekly basis. The table below shows the numbers of incidents recorded and investigated by the Council.

Recording Year	**Incidents**
1st January 2023 to 31st December 2023	138
1st January 2024 to 30th June 2024	68

All incidents have a severity level assigned to them at the Security Incident Review Meetings. A breakdown of severity classification is shown below.

Severity	**2023**	**2024**
Severe	1	1
Moderate	27	10
Low	103	52
Informational	2	2
Undefined	0	0
Non-incident	5	3
Total	**138**	**68**

Learning from breaches:
As part of the investigation of an incident, learning actions will be captured to identify opportunities to reduce the chances of a similar breach occurring in the future.

Learning is shared across the organisation via either specific service area training or as corporate messages being issued to staff to remind them of good practice in avoiding breaches occurring.

7. ICT Security & Cyber Risks

There is an ever-increasing dependency on digital information and networks to facilitate council services and cyber security continues to be a tier 1 risk to national security. Cyber risks include theft of sensitive corporate or personal data, destruction

or tampering to data, monetary losses, denial of service and disruption systems.

A successful cyber-attack against the council would be significant and have a considerable impact across all Council Services. Recognising how significant the impact of an attack would be, the Council has strengthened information security controls and has formed a dedicated Cyber Security team. It has also invested extra funding on cyber security technologies and services. The cyber security team and the council as a whole follows NCSC guidance closely and is a member of the NW WARP (Northwest Warning, Advice, and Reporting Point).

Wirral Council is working towards achieving Cyber Essentials Plus accreditation which provides a simple, good practice framework against which risks, controls and progress can be tracked, and an independent assessment of the Council's security.

The Council's presence on the external, public internet is registered and monitored by the NCSC. Alerts are provided to the Council to identify where weak configuration controls are identified which could be exploited.

8. Freedom of Information & Environmental Information Regulations

The table below details the requests received between January 2023 to June 2024 under Freedom of Information and Environmental Information Regulations.

Year	Number of Requests	Compliance Rate
2022/23	1398	82%
2023/24	1726	75%

IMT records and ensures fulfilment of these requests, proactively reviewing any themes to ascertain if any key or repeated themes are emerging; if this is the case then service areas can be alerted. Being alerted can mean service areas can make informed decisions regarding the publishing of topical information on the Council web site.

IMT ensure that the Council Publication Scheme is up to date, enabling the public to be signposted to publicly available information.
Publication scheme | www.wirral.gov.uk

As a comparison and a benchmarking exercise the table below shows other authorities' statistics, local to us and their FOI requests and compliance rates.

1st April 2023 to 31st March 2024	**Number of FOIS**	**Compliance Rate**
Knowsley	1180	80%
Sefton	1032	80%
Wirral	1726	75%

9. Data Protection Act (DPA) 2018

The table below shows the number of Subject Access Requests made under the Data Protection Act 2018 in the past 18 months. It also details our performance against the target to process 85% within a calendar month.

	2023 Jan to Dec	**2024 Jan to June**

Requests Received	316	161
Actioned within 1 Month(Number)*	254	133
Within 1 Month (%)*	80%	82.6%

The Information Management Team (IMT) receives and records all requests for data in relation to all service areas. In relation to SARs, Children's and Adults Social Care are responsible for collating and providing the responses directly. They have access to the data held in Liquid Logic and have the specialist knowledge and expertise required to identify what data should be/already has been shared.

10. Internal Reviews

Customers who submit a FOI, EIR or SAR can request an internal review if they are not satisfied with the response provided. Statistics on Internal Reviews are below:

Internal Review Type:	**2023**	**2024 Jan to June**
FOI/EIR	64	99

11. Referrals to ICO

Applicants can complain to the ICO after they have had an Internal Review and statistics are shown below:

Referral Type to ICO	**2023**	**2024**
Freedom of Information	6	16
Environmental Information	2	6

12. Information Governance Policies and Procedures Review and Creation of Record of Processing Activities

A comprehensive review of all Information Governance policies began in 2021, with over 100 documents being identified, this led to a web review of content. A further review of policies is planned for 2024/2025.

The Council is required to have an up-to-date comprehensive ROPA to give assurance to the ICO that they were complying with the requirements of Data Protection Legislation. The current ROPA is a fit for purpose document which includes the Information Asset Register. This enables the Council to have adequate insight into the main areas of risk in relation to data / information assets.

13. Conclusions

In summary, ambitious work was undertaken over the last 18 months with key actions taken to strengthen the Council's approach to effectively manage information risks and ensure a robust approach to information governance. Key highlights include:-

Establishing a Cyber Security Architect Post within the Management Team of Digital Data & Technology.
Information Governance continuing to be highlighted within the Corporate Risk register.
Move of Directorate for IMT for closer contact between the SIRO and DPO.
Addition of 2 x new posts within IMT
Corporate IMT strengthening communication with services areas to share knowledge and offer support in relation to information management requests.

Maintenance of a combined ROPA and Information Asset Register.

For further information and guidance please contact:

SIRO – Jilltravers@wirral.gov.uk

DEPUTY SIRO – Petemoulton@wirral.gov.uk

DPO – Janecorrin@wirral.gov.uk

Deputy DPO –Jonathanmorley1@wirral.gov.uk

Cyber Security Architect – Deylanbailey@wirral.gov.uk

Information Commissioners Office website https://ico.org.uk/

Information Commissioners Office Contacts https://ico.org.uk/global/contact-us/