Appendix 1 – SIRO Report

Contents

Executive Summary

Introduction

Key Roles and Responsibilities

Governance and Monitoring Arrangements

Risk Management and Assurance

Corporate Governance actions

Data Breach Management and Reporting

ICT Security & Cyber Risks

Freedom of Information (FOI), Environmental Information Regulations (EIR) & Data Protection Act (DPA)

Internal Reviews and Referrals to the Information Commissioner's Office (ICO)

Information Governance Policies, Record of Processing Activities and Information Asset Register

Conclusion & Further Information

Executive Summary

This report presents the annual Senior Information Risk Owner (SIRO) report. It aims to demonstrate legislative and regulatory requirements relating to the handling, quality, availability, and management of information.

Wirral Council is committed to effective information governance and strives to ensure robust arrangements are in place at all times. Governance arrangements are monitored 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 recent measures introduced to support the realisation of excellent information governance across the Council.

Cyber security risks pose a real threat to the Council and this update details how the Council manages those risks, including a summary to list actions 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. It also details changes implemented to sustain and maintain improvements in this area. The use of Artificial Intelligence (AI) by many requestors has increased the complexity of the information requests received by the Council. It has also contributed to an increase of requests for Internal reviews, the request itself being AI generated.

The number of data breaches are reported, breaches are reviewed weekly to ensure continuous monitoring takes place.

Building on the work done from final quarter of 2025, a number of actions were implemented to strengthen the governance framework, demonstrating the Council is committed to compliance. These actions included:-

- Appointment to the Information Governance Team (IGT), of a Graduate, employed on a 2 year programme of work.
- Additional Deep Dive exercise on Subject Access Requests, as requested by Operational Performance Group (OPG)..
- Continuation of FOI Surgeries facilitated by IGT.
- Further development of using Civica Icase for recording and reporting information requests and security incidents.
- Updating of the form used for Data Protection Impact Assessments (DPIAs).

1. Introduction

The report reflects on the Council's information governance work undertaken from October 2025 to August 2026, which includes:

- A deep dive exercise to review and report on performance indicators relating to the Council's processing of Subject Access Requests. With a focus on Care Leavers SARS.
- An update on the plans the Council has in place to minimise risk, to provide assurance of ongoing improvement to manage those risks.
- A comprehensive review of the Record Of Processing Activities (ROPA)

- A review and updating of Data Breach reporting form and Data Privacy Impact Assessment form, as required by The Data Use and Access Act 2025 (DUAA)..
- Introduction of a dedicated and separate process for Data Protection complaints as required by the new legislation – DUAA.

2. Key Roles and Responsibilities

SIRO

The Head of Legal Services is the SIRO and is responsible for:

- 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 by the Corporate Governance Group (CGG) and the Information Governance Board (IGB). CGG is a high-level strategic group that seeks to ensure proper arrangements are in place for the oversight of Information Governance within the Council. IGB monitors and promotes Information Governance ensuring that effective information governance / risk management and IT governance arrangements are in place.

4. Risk Management and Assurance

The Council's Corporate Risk Register (CRR) is reviewed on a regular basis by the Council's Senior Leadership Team and reported to the Policy and Resources Committee. It contains a specific risk in relation to Cyber Security; this is one of the Council's highest ranked risks. In addition, there is a risk around the compliance with corporate policies and procedures this risk is mitigated in part by controls in relation to Information Governance/Management policy and supporting procedures. At the last review of the CRR a new risk was identified focusing on the governance and use of Artificial Intelligence (AI) across the Council was added and continues to be developed.

Part of the Council's assurance arrangements includes the undertaking of audit reviews, the findings of which are reported to Audit and Risk Management Committee. There have been 2 audit reviews specifically linked to Information Governance, and these are detailed below.

<u>Audit 1 - Artificial Intelligence Governance Audit</u>

As previously reported to Members, the Council has employed Information Technology (IT) Technical Audit team at Salford Council to provide two Information Technology reviews one of which was on the use of Artificial Intelligence (AI). The AI audit opinion was "**Reasonable**" which is broadly equivalent to the **Moderate** rating at Wirral Council.

The report Executive Summary recognises that the Council has proactively established governance arrangements ahead of widespread AI adoption and is taking a measured approach to managing emerging AI-related risks. Although, the report highlighted that there are opportunities to strengthen AI governance arrangements further, most notably AI Inventory and AI risk management.

The report includes four recommendations of which two are priority 1, which is equivalent to high risk at Wirral Council. The report also includes one Advisory point that implemented should enhance the current control environment.

The priority 1 recommendations are:

- A central inventory of AI-enabled systems, tools and agents, in use across the organisation should be maintained. The inventory should capture key information including the business owner, purpose, AI functionality, data processed, risk classification and approval status. The council should also implement proportionate measures to provide visibility of undeclared potentially high-risk AI usage (shadow AI), e.g. agents created in M365 Copilot.
- Management should establish and maintain a formal documented AI risk management process to ensure AI-related risks are consistently identified, assessed, documented, monitored, and reviewed. The process should provide evidence of risk assessments, risk ownership, mitigating controls, and periodic review activities. Whilst management has demonstrated awareness of a number of key AI risks and has implemented or is considering mitigating actions in several areas, a formal process would help provide assurance that AI risks are being comprehensively and consistently managed across the organisation.

Audit 2 - External Review of Cyber Security

As previously reported, the Council appointed Salford City Council to provide specialist IT audit support following the departure of the Internal Audit team's IT audit resource. An audit of Cyber Security and the Council's response to cyber incidents is currently in the fieldwork stage. The review assesses the adequacy and effectiveness of the Council's cyber security governance, risk management arrangements, technical controls, and incident response processes. Testing and evidence gathering are ongoing in accordance with the agreed audit scope and methodology. Internal Audit continues to maintain regular liaison with the auditor to monitor progress, provide oversight, and ensure the review is completed in accordance with professional standards and agreed timescales

Looking ahead, Risk and Compliance will be completing assurance mapping against the key corporate risks; this will include determining assurance from all lines of defence which will inform audit planning.

5. Corporate Governance Actions

The council is committed to a clear strategy and sustainable framework for Information Governance across the council. Weekly and monthly performance reports are made available to Senior Manager via DASH. This provides opportunity to monitor and comment on any actions required to improve on information issues, risks and cultural behaviour or arrangements around data processing and security.

In summary, the following key actions were delivered from August 2025 to date which have strengthened the Council’s management of information risks.

- The essential on-line training for Adult Social Care and Health to ensure compliance with NHS toolkit was reviewed by the DPO and remains fit for purpose. The target for completion is 95% and this was achieved for the June 2026 deadline.

- The Data Breach internal form has been re-designed to make it simpler to complete.

- The Data Protection Impact Assessment form has been reviewed and updated in line with DUAA..

- All breaches are reviewed weekly by the DPO, Deputy DPO and IGT with referrals to the ICO taking place if they meet the threshold for reporting.

- Introduction of a dedicated reporting procedure for Data Protection complaints as required by DUAA.

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).

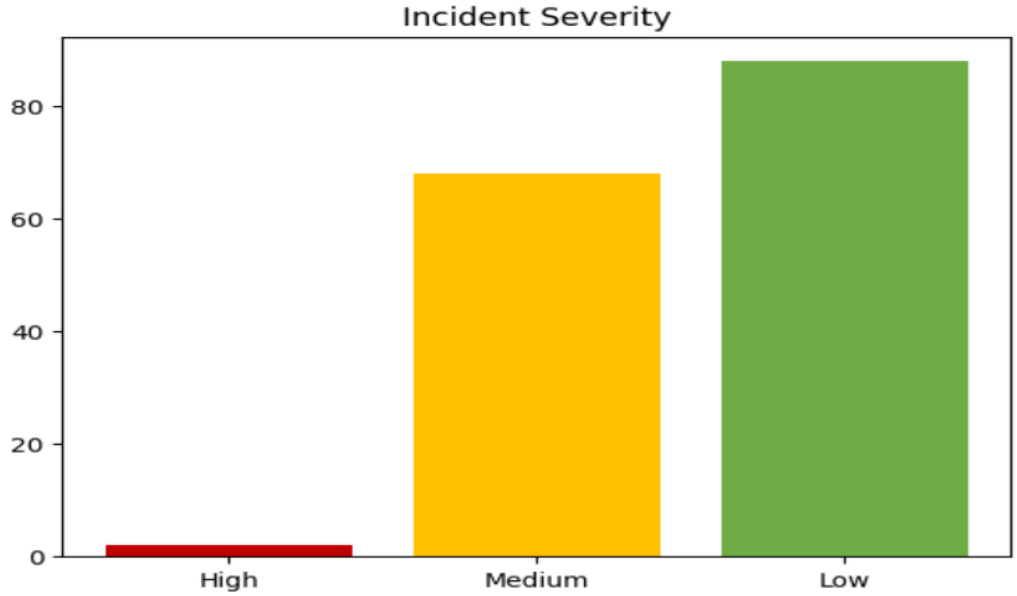
All data breaches are reviewed individually at a weekly meeting to ensure corrective actions can be timely. Common actions are escalation to a senior manager; suggestions for changes to processes or procedures or staff advised to undertake refresher training.

Reporting, containment actions, investigation and learning phases of data breach incidents play a key role in the management of risk and improvement of internal controls.

The table below shows the numbers of incidents recorded and investigated by the Council.

Recording Year	No. of Incidents
1st September 2025 to 31st August 2026	158

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



Severity Impact	1st September 2025 to 31st August 2026
High	2
Medium	68
Low	88
Overall Total	**158**

Department	High	Medium	Low	Total
Adult Care and Health	0	14	19	**33**
Children, Family and Education	0	33	36	**69**
Finance	0	4	9	**13**
Law and Corporate Services	1	11	11	**23**
Neighbourhoods	1	3	7	**11**
Regeneration and Place	0	3	6	**9**
Total	**2**	**68**	**88**	**158**

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 Risk

As the Council continues to increase its reliance on digital technologies and cloud-based services to deliver critical public services, cyber security remains a significant organisational risk. Cyber-attacks continue to represent a Tier 1 national risk and have the potential to disrupt services, compromise sensitive information, create financial losses and damage public confidence.

To address these risks, Wirral Council has continued to strengthen its Cyber Security function within Digital, Data and Technology (DDaT). The Council's approach is aligned with guidance from the National Cyber Security Centre (NCSC) and recognised cyber security frameworks. The Council also works closely with regional and local government cyber security communities to share intelligence, best practice and emerging threats.

During the reporting period, the Council has further enhanced its cyber security capability through investment in people, processes and technology. A dedicated Security Operations Centre (SOC) capability is now operational, providing continuous monitoring, threat detection and incident response support across the Council's digital estate. This capability improves the Council's ability to identify, investigate and respond to cyber security threats in a timely manner, strengthening overall organisational resilience.

The Council has continued to mature its cyber security operating model, including the development of dedicated security governance, security architecture and cyber risk management functions. Cyber risks are actively identified, assessed and monitored

through formal governance arrangements, ensuring that emerging threats and vulnerabilities are managed appropriately and reported through established risk management processes.

Alongside technical controls, the Council continues to invest in staff awareness and organisational resilience. During the year, the Council transitioned its cyber security awareness and phishing simulation platform from Cyber Ninjas to BoxPhish, providing an enhanced training capability and supporting a more proactive approach to cyber security awareness. This is complemented by ongoing awareness campaigns designed to help colleagues identify and report phishing attempts, social engineering attacks and other cyber threats, recognising that employees remain one of the most important lines of defence against cyber incidents. The Council has also refreshed its cyber security training approach to ensure learning remains aligned to current threats and national guidance.

The Council remains committed to achieving Cyber Essentials Plus accreditation and continues to implement the technical, procedural and governance improvements required to meet the standard. This government-backed accreditation provides independent assurance that appropriate cyber security controls are in place to protect systems, devices and data and forms part of the Council's wider cyber security improvement programme.

The Council also continues to benefit from external monitoring and assurance arrangements. Its external digital footprint is monitored through services including the NCSC's Active Cyber Defence programme and Police Cyber Alarm, helping to identify vulnerabilities and emerging threats. Regular cyber incident response planning, testing and review activities are undertaken to ensure the Council is prepared to respond effectively should a cyber security incident occur.

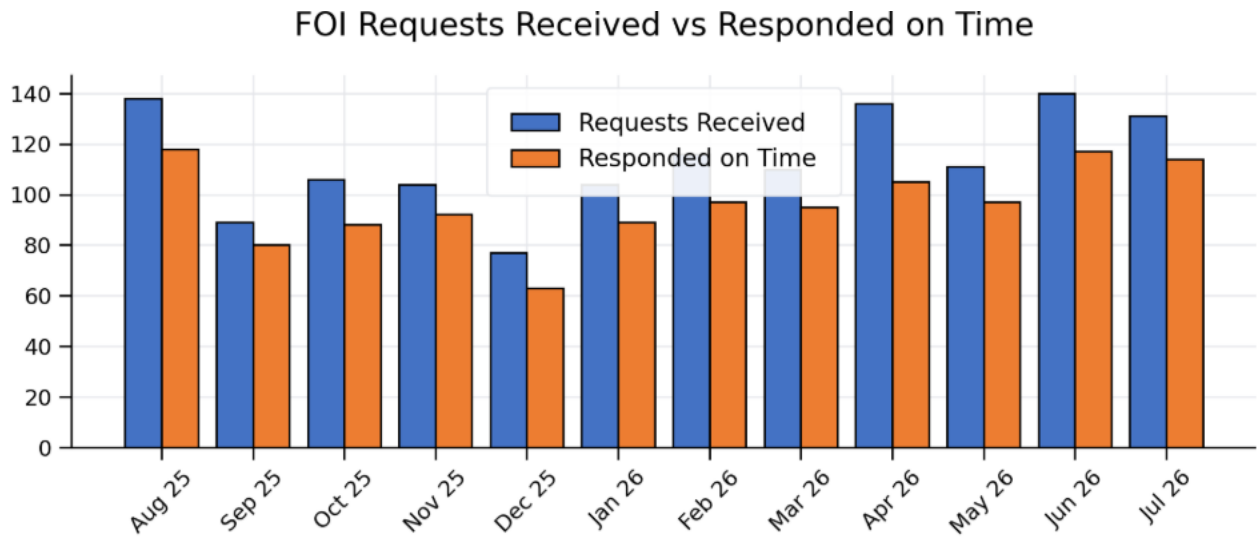
Overall, whilst the cyber threat landscape continues to evolve, the Council has made significant progress in strengthening its cyber resilience. Ongoing investment in cyber security capabilities, governance, monitoring, staff awareness and incident response arrangements is improving the Council's ability to prevent, detect, respond to and recover from cyber security incidents, helping to protect the information, services and residents that depend upon them.

8. Freedom of Information & Environmental Information Regulations

The table below shows a breakdown of compliance rates from August 2025 to July 2026

Month	Requests Received	Responded on Time	Percentage Responded on Time
August 25	138	118	85.5%
September 25	89	80	90%
October 25	106	88	83%
November 25	104	92	88.5%
December 25	77	63	82%
January 26	104	89	86%
February 26	116	97	84%
March 26	110	95	86.5%
April 26	136	105	77%
May 26	111	97	87.5%
June 26	140	117	84%
July 26	131	114	87%
TOTALS	**1362**	**1155**	**85%**

Bar chart and line graph are for the period 01/08/2025 – 31/07/2026



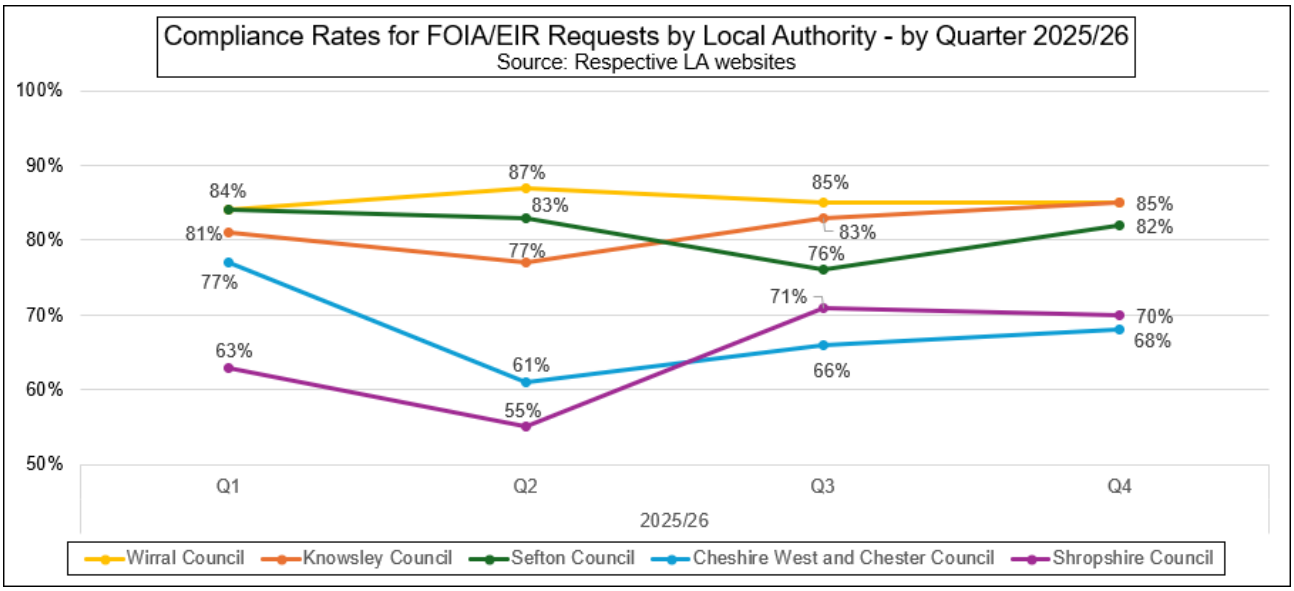
IGT review any themes or emerging patterns so service areas can be alerted. This approach means service areas can make informed decisions regarding the active publishing of topical information. IGT ensure the Council Publication Scheme is up to date, enabling the public to be signposted to publicly available information.
Publication scheme | www.wirral.gov.uk

Numbers of Requests per Directorate and % achieved on Time

Month	Regen and Place	Adult Care and Health	Children Family and Education	Law and Corporate	Finance	Neighbourhood
Aug 25	27 (80%)	2 (68%)	14 (87.5%)	17 (85%)	13 (81%)	45 (92%)
Sept 25	22 (96%)	3 (100%)	8 (80%)	11 (100%)	17 (81%)	19 (90.5%)
Oct 25	16 (84%)	4 (57%)	17 (85%)	10 (72%)	14 (82.5%)	27 (93%)
Nov 25	18 (82%)	8 (90%)	15 (100%)	8 (100%)	16 (76%)	27 (93%)
Dec 25	9 (82%)	5 (100%)	14 (68%)	6 (75%)	7 (78%)	22 (96%)
Jan 26	12 (92%)	9 (90%)	8 (57%)	10 (100%)	13 (72%)	37 (95%)
Feb 26	17 (81%)	5 (100%)	15 (75%)	8 (67%)	16 (94%)	36 (88%)
March 26	14 (87.5%)	7 (87.5%)	15 (75%)	7 (70%)	18 (90%)	34 (95%)
April 26	17 (90%)	1 (33%)	13 (52%)	10 (91%)	27 (82%)	37 (82%)
May 26	16 (94%)	4 (100%)	16 (73%)	8 (90%)	22 (88%)	31 (91%)
June 26	17 (81%)	4 (100%)	15 (83%)	15 (94%)	29 (76%)	37 (86%)
July 26	19 (86%)	9 (75%)	18 (86%)	7 (70%)	18 (95%)	43 (91.5%)
Total	**204 (86%)**	**61 (83.5%)**	**168 (76%)**	**117 (84%)**	**210 (83%)**	**395 (91%)**

Comparison Figures

The table below shows some comparison figures from neighbouring authorities.



9. Data Protection Act (DPA) 2018

Subject Access Requests are reported with a four-month delay as we can extend a SAR by 2 months if they are complex in nature. The requestor also have to supply valid ID which can also extend the time taken.

Table 1 details the Corporate SARS – These are all SARS except for Adult Social Care (ASC) and Children, Family and Education (CFE) - these are depicted in Table 2 and 3 below.

Table 1 – Corporate SARS

Month	Number Received	Responded on Time	Percentage Responded on Time
Aug 25	43	39	91%
Sept 25	39	34	87%
Oct 25	42	38	90.5%
Nov 25	36	33	92%
Dec 25	36	30	83%
Jan 26	47	38	80%
Feb 26	64	53	83%
March 26	51	45	88%
April 26	32	29	91%
TOTALS	**390**	**339**	**87%**

Table 2 – ASC SARS

Month	SARs Received	Responded to on time	Performance Rate
Aug 25	4	3	75%
Sept 25	6	5	83%
Oct 25	12	11	92%
Nov 25	25	25	100%
Dec 25	4	4	100%
Jan 26	7	5	71%
Feb 26	17	14	82%
March 26	7	7	100%
April 26	4	4	100%
TOTAL	**86**	**78**	**91%**

Table 3 – CFE SARS

Month	SARs Received	Responded to on time	Performance Rate
Aug 25	25	24	96%
Sept 25	24	22	92%
Oct 25	23	31	91%
Nov 25	3	2	67%
Dec 25	20	18	90%
Jan 26	28	26	93%
Feb 26	33	29	88%
March 26	26	24	92%
April 26	16	16	100%
TOTAL	**198**	**192**	**97%**

10. Internal Reviews and ICO Referrals

Taking figures from Civica from 1st August 25 to 31st July 26, 99 FOI/EIR Internal reviews. Where the figures show not upheld or partially upheld this means the Council was either completely correct or partially correct in its initial decision.

FOI/EIR Internal Review % by department

Department	Upheld	Not upheld	Partially Upheld	% not upheld
Law and corporate	5	6	1	58%
Children, family and education	3	6	1	70%
Finance	2	14	2	90%
Adult health and care	1	3	0	75%
Neighbourhoods	8	15	5	71%
Regeneration and place	4	12	3	79%

*These percentages are using Partially upheld as not upheld.

The Table below shows the reasons why an Internal Review was requested.

Reasons for Internal Review

Escalation Reason	Number of Cases	Percentage
Disagree with decision not to release requested information	53	53.5%
Disagree with decision for any other reason	30	30.3%
Other complaint about handling of request	11	11.1%
No escalation reason recorded	4	4.0%
Delay in handling of request	1	1.0%
Total	**99**	

.

During the period 1st August 2025 – 31st July 2026 **2 FOI/EIR and 3 SAR ICO referrals** were made. **1 FOI/EIR complaint was upheld,** and **3 SAR ICO referrals were not upheld.** Applicants can complain to the ICO after they have received an Internal Review decision and remain dissatisfied.

The 2 FOI/EIR ICO referrals directorates: 1 x Regeneration and Place **Upheld**
1 x Finance **Not upheld**

% Successful ICO Referrals

	Partially Upheld	Upheld	Not Upheld
FOI/EIR	0	1	1
		% Successful	50%

*That is taking Partially upheld as not upheld.

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

A continued review of Information Governance policies is required to ensure they are current and fit for purpose. The Graduate member of IGT completed a complete review of the ROPA. There is an ICO requirement that Public Bodies maintain and can produce a ROPA for inspection upon request. The ROPA demonstrates compliance with the requirements of Data Protection Legislation, it is an organic document and is reviewed and updated on an ongoing basis. The ROPA is combined with the Information Asset Register to ensure it is a comprehensive document. Additional columns will need to be added to this document to take account of AI technology within existing systems and software.

12. Conclusions

In summary, work continues into the final quarter of 2026, and further work is planned for 2027 to help the council sustain and improve in all areas of information governance, highlights include:-

- Information Governance remains on the Corporate Risk register
- Retention of FOI Champions and continuation of FOI surgeries.
- Inclusion of a Graduate in IGT.
- Review of IG policies and procedures
- Review of IG templates and Forms

- Establishing a closer working relationship with the Cyber Security Team
- Review and update of the combined ROPA and Information Asset Register.

For further information and guidance please contact:

SIRO – Vickishaw@wirral.gov.uk

DEPUTY SIRO – Petemoulton@wirral.gov.uk

DPO – Janecorrin@wirral.gov.uk

Deputy DPO –Jonathanmorley1@wirral.gov.uk

Head of Digital Ops and Cyber Security – Jimfessey@wirral.gov.uk

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

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