ISLE OF ANGLESEY COUNTY COUNCIL	
Report to:	Governance & Audit Committee
Date:	04/12/2025
Subject:	Information Governance – Annual Report of Senior Information Risk Owner (SIRO) for the period 01/04/2024 to 31/03/2025
Head of Service:	Lynn Ball Director of Function (Council Business) / Monitoring Officer / SIRO.
Report Author:	Interim Data Protection Officer
Nature and Reason for Reporting: To provide the Senior Information Risk Owner's view of the main Information Governance (IG) issues for the period 01/04/2024 to 31/03/2025; and current risks.	

1. INTRODUCTION

This Report outlines the view of the Council's SIRO as to the Council's compliance with statutory* requirements in the field of Information Governance (IG).

Additionally, this Report will refer to any Council interaction with regulatory authorities and instances of identified vulnerability and risk. Aside from the information in **Appendix 8** of this Report will not include reference to cyber security, nor the work undertaken during the year in relation to the Cyber Assessment Framework. These are matters for the Chief Digital Officer's Annual Report to this Committee.

Some statistical information regarding the Council's IG performance is presented in the Appendices.

2. RECOMMENDATIONS

2.1 Focused data breach training be delivered to Freedom of Information Act Officers (FOIA Officers) to improve their awareness of what constitutes a data breach, how to report a data breach, and the mitigation measures that need to be taken in the event that a data breach is discovered.

2.2 The Personal Data Security Incidents Policy, and supporting Guidance, be reviewed and updated before being relaunched internally with FOIA Officers. Such relaunch to be accompanied by specific training on the revised Policy and Guidance.

Footnote: *These include compliance with the United Kingdom General Data Protection Regulation (UK GDPR), provisions of the Data Protection Act 2018, stipulations within the Freedom of Information Act 2000, requirements under the Regulation of Investigatory Powers Act 2000 (relating to surveillance activities), alongside associated procedural guidelines.

2.3 Subject to corporate approval, quarterly KPI figures in relation to FOIA requests, as reported to the Executive and Corporate Scrutiny Committee, be amended to include compliance rates across individual services. This is to improve transparency in identifying areas of underperformance with a view to assisting and supporting those areas with targeted improvement measures and training.

2.4 Request that services conduct an assessment of their publication schemes with a view to increasing reliance on s20 and s21 of the FOIA (that is, information which is intended for future publication or information which is already available)

2.5 To provide FOIA training to FOIA Officers to include the appropriate application of exemptions.

3. THE SIRO'S ASSESSMENT

3.1 Data Breaches

The overall figures for reported data breaches remains consistently low, as reported in previous years. However, for the Council to have only experienced seven data breaches in a year **(Appendix 1)** may indicate a lack of awareness of what constitutes a data breach and so matters that should be reported to the Interim Data Protection Officer (IDPO) are being overlooked. To ensure that the Council's practices are robust, training needs to be refreshed in this area. Clearly this will be done in recognition of the fact that the number of data breaches may increase with improved awareness and clarity of the required systems and processes.

The Personal Data Security Incidents Policy was last reviewed in 2020. It was due to be reviewed in 2022, and then in 2024. However, owing to staffing/capacity issues, this work was never undertaken. Similarly, the guidance note to accompany the Policy was also due for review but this work has not been undertaken.

3.2 Freedom of Information Act 2000 (FOIA)

While there are areas of good practice, the headline is that the Council's overall FOIA compliance figures are stubbornly low and always below the required minimum requirement expected by the Information Commissioner (ICO) (target 90%) **(Appendix 4)**.

Of relevance to this issue may be the following considerations:-

- There is an absence of current service related publication schemes. Routine/regular publication of material frequently requested under FOIA and the Environmental Information Regulations (EIR) is an exemption to FOIA/EIR requests and, used effectively, publication schemes can reduce the burden on services.
- It is noted in **Appendix 4** that there was only one request for an internal review during the period of this Report. An internal review is an appeal

against a decision made in response to an FOIA/EIR decision and is required before an applicant may refer an appeal to the ICO.

As a comparison, the report on governmental FOIA compliance indicates that in 2024 (figures released in 2025) that an internal review was initiated in 13% of FOIAs. The Council's low level of requests for internal reviews may be linked to a very limited reliance on statutory exemptions.

The number of reported exemptions relied upon was only 16 in total despite there being 818 FOIA requests, involving 6574 elements. See **Appendix 4**.

Accordingly, the IDPO has arranged for FOIA Officers to receive additional training on FOIA, more generally, including specific training on the application of exemptions. There will also be routine meetings with the IDPO for the FOIA Officers and the application of exemptions will be a standing agenda item. This is intended to refresh awareness and confidence in the application of exemptions.

In particular the IDPO will be working with the FOIA Officers, and their services, to discuss the renewal/implementation of publication schemes. This allows regularly requested items to be published, allowing FOIAs to be responded to in reliance on sections 20 and 21 of the FOIA. That is information intended for future publication, or which is already available. Thoughtful and regularly reviewed publication schemes can lead to improvements in FOIA compliance rates and reduce the workload on services.

It is proposed that the reporting of individual elements is removed from future reports. This information does not provide any meaningful assistance to understanding the workload created by FOIAs and quarterly reporting of performance by individual service areas would provide greater understanding of relevant issues and opportunities for intervention and improvement.

The average compliance figure over preceding years has been provided in **Appendix 4**.

3.3 ENVIRONMENTAL INFORMATION REGULATIONS

FOIA reporting should include reporting on EIR 2004. Over the reporting period requests that should have been treated as EIR requests have been incorrectly logged as FOIA requests and managed, processed and reported as such.

In future reports, EIRs will be included in joint reporting.

It should be noted that the same statutory deadlines for responses exist for EIR. That is, 20 working days.

3.4 SUBJECT ACCESS REQUESTS (SARs)

This is reported in **Appendix 6**

3.5 INDIVIDUAL RIGHTS REQUESTS (IRRs)

2 IRRs were received during the reporting period. These were treated incorrectly as complaints.

In future SIRO reports these will be reported as IRRs made under the Data Protection Act 2018.

3.6 REGULATORY OVERSIGHT

This is reported in **Appendix 7**

3.7 THE RESOLUTION OF THE GOVARNANCE AND AUDIT COMMITTEE 2023/2024

This is reported in **Appendix 8**

3.8 CORPRORATE RECORDS MANAGEMENT (FOIA)

This is reported in **Appendix 9**

Appendix 1. The number of data security incidents recorded by the Council during the year.

Data security incidents (24/25): 7

Level 1 (near miss or confirmed as a data security incident but **no** need to report to ICO/other Regulators) = 7

Level 2 incidents Data security incidents that **must** be reported to the ICO because of the risk presented = 0

Category Level 0 -1	**Number**
Disclosed in error	7
Lost data/ hardware	0
Unauthorised disclosure	0
Lost in transit	0
Other	0
Category 2	**Number**
Disclosed in error	0
Unauthorised disclosure	0
Technical failing	0
Other	0

Appendix 2. Agreed actions following data security incidents.

Action
No formal actions were agreed during the period of this report.

Appendix 3. Data breaches reported to the ICO.

During the period of 01/04/2024 to 31/03/2025, no data breaches required reporting to the ICO.

Appendix 4. Information about Freedom of Information Act 2000 requests and complaints

4.1 Freedom of Information Act 2000 requests

During the reporting period of 01/04/2024 and 31/03/2025 the Council received 818 requests for information.

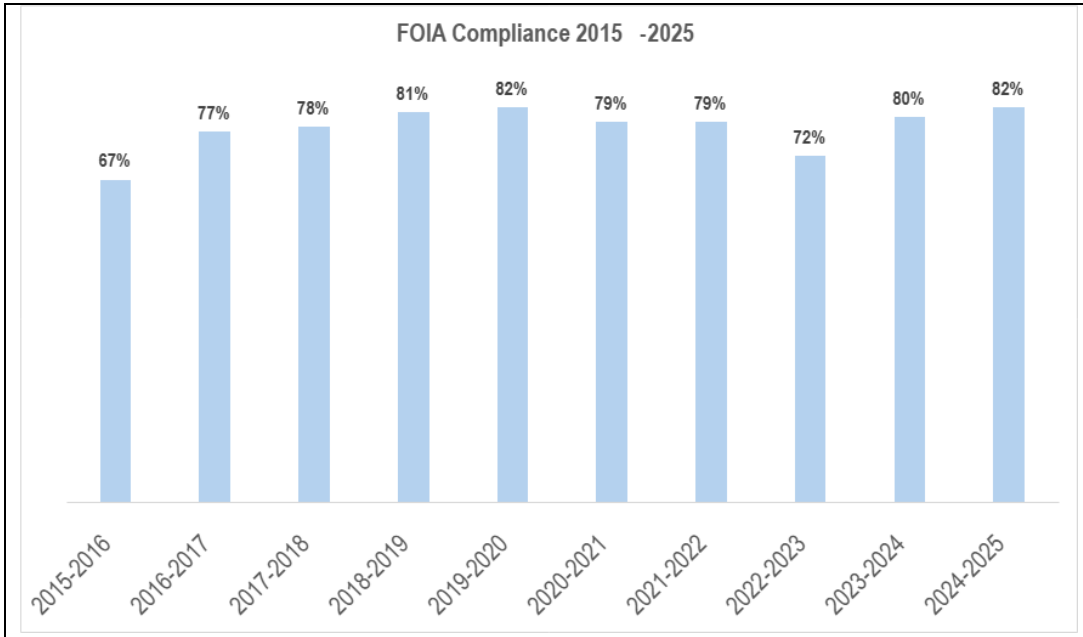
Most requests were made to Planning & Public Protection, Highways, Property & Waste, and Resources.

FOI data in summary for the reporting period:

Total Number of Requests Received	818
Total Number of Elements Received	6574
Percentage of requests responded to within statutory timescale	82% against the ICO target of 90%
Total number of requests for an Internal Review in accordance with the Statutory Code of Practice	1

The ICO advises that public bodies should respond to 90% of FOIA requests within 20 working days.

During the reporting period of 01/04/2024 to 31/03/2025, the Council's corporate average compliance was 82%.
This remains significantly below the ICO's target and suggests training and capacity issues. This pattern of underperformance is longstanding and stagnant. Compliance over time is presented in the graph below.


FOIA Compliance 2015 -2025
67%
77%
78%
81%
82%
79%
79%
72%
80%
82%
2015-2016
2016-2017
2017-2018
2018-2019
2019-2020
2020-2021
2021-2022
2022-2023
2023-2024
2024-2025

4.2 Freedom of Information Act 2000 exemptions used.

During the reporting period of 01/04/2024 to 31/03/2025 the following exemptions were applied:

Exemption	Number of times used
Section 1 S1(3) (request requires clarification)	3
Section 12 (above the appropriate limit of 18 hours)	1
Section 14 (repeated requests)	1
Section 21 (accessible by other means)	4
Section 31 (prejudice to various law enforcement functions)	1
Section 39 (environmental information)	1
Section 40 (personal data)	1
Section 41 (information provided in confidence)	2
Section 42 (legal professional privilege)	2
Total exemptions applied	16

Appendix 5. Information about the number of data protection complaints made to the Council during the year by individuals about its processing of their personal information.

Data protection legislation consolidates the rights of individual data subjects to complain about the way organisations have used, or propose to use, their personal data or otherwise infringe their data subject rights.

Data Protection Act Complaints to the Council (Individual Rights Requests)
2 DPA complaints were received 1 complaint related to a request to **erase personal data** 1 complaint related to an **objection** to the Council's processing of personal data Following investigation by the IDPO, it was found that**:** **1 case was upheld**. The Council's processing had compromised an individual's rights; **1 case was not upheld**. The Council's processing had not compromised the individual's data protection rights.

Appendix 6. Information about the number of data protection Subject Access Requests and the Council's performance.

Subject Access Requests and Compliance
49 SARs were received during the period. Of those received: 39% (19) responses sent within the appropriate statutory deadline, i.e. within 1 month with 1 late response. 59% (29) requests are on hold pending confirmation or clarification regarding the identity of the applicants. Such requests are not categorised as "late". 2% of the responses sent were late.

Appendix 7. Information about Regulatory Oversight

7.1 Data Cymru Ransomware Incident

7.1.1. Summary of Incident

On 03/11/2024 Data Cymru experienced a ransomware attack by a group identified as INC Ransom. The attack was first detected on 04/11/2024 and resulted in unauthorised access to sensitive personal data relating to children's social services across councils in Wales. A further investigation on 26/11/2024 uncovered a second, more extensive dataset, that had also been accessed by the attackers.

The compromised data included sensitive personal information of children in care placements across Wales, dating back to 2012. This information included children's names, dates of birth, placement details, provider information, and setting addresses.
According to analysis, the attack appeared to have been made possible through a legacy test account created during Data Cymru's migration to their outsourced IT provider (OGI/NSUK) in 2012. This account, which Data Cymru was unaware of, provided the attackers with a backdoor into their systems. The primary focus of the attack was a legacy file storage system that was being gradually phased out as part of a migration to SharePoint.

7.1.2. Actions Taken by Isle of Anglesey County Council

This Council responded to the Data Cymru breach with a measured and coordinated approach, focused on protecting affected individuals while maintaining compliance with data protection requirements. Upon notification of the breach in 11/2024, this Council promptly established internal communication channels, designating identified officers as the points of contact for the incident. Information was carefully managed on a need-to-know basis to maintain the confidentiality recommended by the National Cyber Security Centre.

Throughout the incident management process, the Council actively participated in the coordinated national response through the All-Wales Heads of Children's Services (AWHOCS) regional leads meetings and Data Protection Officer networks. The Council adopted the nationally agreed media management protocol and prepared our communications team to handle any press inquiries according to the established guidelines. We also maintained ongoing communication with affected local care providers, offering guidance on their responsibilities as data controllers.

When the BBC published an article in 03/2025 about a data breach affecting vulnerable children, the Council promptly reviewed risk assessments and prepared to manage any resulting FOIA requests according to the recommended exemption approach. Throughout the incident, the Council maintained comprehensive documentation of our decision-making processes, including the risk-based decision not to notify affected individuals. In 04/2025, the Council received confirmation that the ICO had decided not to take regulatory action, validating the approach to managing this complex data breach incident.

7.1.3 Lessons Learned by Isle of Anglesey County Council

The Data Cymru ransomware incident provided this Council with several valuable insights that have strengthened our approach to data protection and incident management. Through our involvement in this complex incident, the Council identified key areas for improvement across our data governance practices, security oversight, and multi-agency collaboration processes.

The Council recognised the need to clarify data controller/processor relationships and review data sharing arrangements with external organisations, particularly where sensitive information about vulnerable children is concerned. These governance considerations have led to more robust documentation of data flows and processing activities for special category data.

Security collaboration emerged as another crucial learning area, with the Council acknowledging the importance of regular verification of security controls implemented by their data processors rather than solely relying on contractual obligations. The fact that unencrypted data extracts were compromised highlighted the need for consistent security standards across all data handling practices. Finally, the Council's participation in the coordinated national response demonstrated the value of multi-agency incident management while also revealing opportunities to develop more robust internal processes for incidents involving external data processors.

7.2 Information Commissioner's Office

The ICO is responsible for enforcing and promoting compliance with the Data Protection Act 2018 and the UK GDPR; the Freedom of Information Act 2000; the Privacy and Electronic Communications Regulations; the Environmental Information Regulations; the Re-use of Public Sector Information Regulations; the INSPIRE Regulations. The ICO has power to assess any organisation's processing of personal data against current standards of 'good practice'.

Information about the number of data protection complaints from individuals about the Council's processing of their personal information which were investigated by the Information Commissioner's Office (ICO) during the period of this report.
Two complaints were investigated by the ICO, with one investigation running beyond the period of this report. In both cases, the ICO required no further action from the Council.

Freedom of Information Act Appeals to the ICO
Two decisions were appealed to the ICO during the period of this report: In one case, the decision of the ICO was that the Council ought to provide a substantive response to the request within 10 working days. The other case required the Council to consider the data protection elements of the FOIA complaint separately, but no further steps were required.

7.3. Surveillance Camera Commissioner

Nothing to report for this period.

Appendix 8. Update on resolution of the Committee from 2023-2024

"It was resolved to accept the report and to approve the recommendation that the SIRO and the Council's senior leaders are provided with regular updates on cyber risks and mitigations so that informed, strategic decisions relating to the constant cyber threat to the integrity and confidentiality of the Council's data assets can be made promptly and effectively."

Current Status

Updates are provided to the Leadership Team where either:

- a vulnerability has been identified/or a proposed mitigation to an identified vulnerability, is likely to cause a material impact to one or more services or

- there is a choice to be made on the balance of risks. In these cases the Leadership Team receives a report from IT requiring a decision to be made to apply a mitigation recognising any impacts thereof. Alternatively, to implement a different mitigation of lesser impact, or to accept the risk of a particular vulnerability.

On 30/09/2025 the Council's Chief Digital Officer presented a report to this Committee in relation to the status of cyber projects including the work ongoing as part of the National Cyber Assessment Framework.

Appendix 9. Corporate Records Management/FOIAs

The recently appointed IDPO has raised concerns that the original specification for the FOIA/CRM system is too restrictive in the level of oversight that it will provide. In essence, the conclusion is that the CRM project which has been pursued was not sufficiently ambitious. The current IDPO has undertaken a holistic review of the Council's Information Governance arrangements and has concluded that it would be of greater benefit to the Council to devise a system that is not just limited to FOIA data but also includes wider information requests (those described in Section 3 of this Report) which should provide for a broader range of accuracy and corporate monitoring of performance.

A model along similar lines already exists in another regional authority but enquiries have established that the existing system in not compatible with this Council's CRM platform so joint working/acquisition is not possible.

In the circumstances the new project will be fully designed in-house and a new CRM specification is being designed together with a new project plan.

In the meantime, although outside the timetable of this Report, the IDPO has implemented some new ways of working and managing FOIAs, along with additional training and regular ongoing meetings which it is hoped will make the present service more efficient. There is now additional monitoring, routine meetings between the IDPO and FOIA officers providing opportunities to address areas of weakness and allowing targeted training and support to those service areas with lower levels of compliance.

Information has also been reported to the Corporate Scrutiny Committee on 18/11/2025 and will be reported to the Executive on 25/11/2025. The relevant Report states the following:-

"*The Council's current Data Protection Officer (DPO) has reviewed the councils FOI policy and procedures. Following this review a new specification will be developed for the establishment of FOIs on the CRM system that will ensure our procedures are compliant with the Information Commissioner's Office (ICO). It is believed that the new online system should make improvements to performance in the long term. Some reduction in capacity within services to deal with FOI tasks also ensures that the target of 90% remains a difficult one."*