

CYNGOR SIR YNYS MON / ISLE OF ANGLESEY COUNTY COUNCIL	
MEETING:	Governance & Audit Committee
DATE:	21st September 2021
TITLE OF REPORT:	INFORMATION GOVERNANCE – SENIOR INFORMATION RISK OWNER’S ANNUAL REPORT FOR 1ST APRIL 2020– 31ST MARCH 2021
PURPOSE OF THE REPORT:	To Inform Members as to the Level of Compliance and Risk
REPORT BY:	SIRO/Monitoring Officer Ext. 2586 lbxcs@ynysmon.gov.uk
CONTACT OFFICER:	SIRO/Monitoring Officer Ext. 2586 lbxcs@ynysmon.gov.uk

Purpose of this report

To provide the Audit and Governance Committee with the Senior Information Risk Owner’s analysis of the key Information Governance (IG) issues for the period 1 April 2020 to 31 March 2021 and to summarise current priorities.

Introduction

This report provides the Senior Information Risk Owner’s statement and overview of the Council’s compliance with legal requirements in handling corporate information, including compliance with the United Kingdom General Data Protection Regulation (UK GDPR); Data Protection Act 2018; Freedom of Information Act 2000; Regulation of Investigatory Powers Act 2000 (Surveillance) and relevant codes of practice.

The report provides information about the Council’s contact with external regulators and gives information about security incidents, breaches of confidentiality, or “near misses”, during the period.

Key data about the Council’s information governance is given below in Appendices 1-7.

Senior Information Risk Owner’s Statement

As discussed in the report for 2019-2020, the Council’s data protection governance arrangements have achieved a sufficient degree of maturity and cultural embedding to be able to identify necessary change and improvement organically and without the stimulus of external regulatory intervention as drivers for change.

The Council has mechanisms and process in place to ensure that key intelligence about information governance compliance is captured, analysed and enabling prompt response and operational change and targeted development. Oversight by senior leaders of the Council is supported by the way that data protection is embedded into the culture of Services.

During this year, data protection training sessions have been delivered to staff based on their need for general or specialist role training. Training on the Regulation of Investigatory Powers

Act (RIPA) was provided for RIPA Authorising Officers, the RIPA Senior Responsible Owner and the RIPA Coordinator. Further information about training is provided below (see Appendix 7).

The Council's processes for compliance with the Regulation of Investigatory Powers Act were inspected by the Investigatory Powers Commissioner during the period of this report. Prior to the inspection, the Council's **new RIPA Social Media Guidance** had been produced and circulated to relevant services and the Council's Policy document had been revised. The inspection was favourable and no formal recommendations were made by the IPCO.

During the period of this report the **Council's Data Protection Agreement / Contract** was completely revised in order to accommodate Post- Brexit requirements. The new template is now being used by Services. The **Data Protection Impact Assessment template** and process was also completely revised and re-issued. All non-current data protection content was removed from the Council's intranet site shifting the focus towards the Policy Portal as a resource for data protection resources.

At the September 2020 meeting of the Audit & Governance Committee there was discussion about the possibility that the Council could make more information available in order to better **manage the impact of FOIA requests on Services**. The benefits of routine publication of information are set out in the Act: when a request for information is received for information that is readily available on the Council's website it engages an exemption, which can simplify the response.

In order to assess whether the Council's routine publication of information is currently an effective factor in minimising the impact of FOIA requests, a self-assessment tool was prepared and circulated to the Council's Services. Conclusions are provided in Appendix 8.

It is clear that, owing to demand for operational advice, the Council's information governance capacity is being invested on providing direct support to clients in accordance with the key obligations of data protection legislation. Consequently, there is no longer capacity for any non-essential strategic and corporate initiatives.

Therefore, I propose that rather than reporting on the progress of Services with action plans, future attention will shift to seeking assurance from the Heads of Service, as Information Asset Owners, on key compliance areas, which will be reported to this Committee.

As SIRO, I consider that there is significant documented evidence to demonstrate that the Council's data protection and information governance arrangements are good. I base my assessment on the information governance systems, processes, policies, and training that the Council has in place. I consider that information governance is embedded within the operational culture of the Council. Additional information about key information governance elements is provided in the appendices to my report.

Recommendations

As SIRO, I make the following recommendations to the Committee, that:

- i. the SIRO's statement is accepted;
- ii. the Learning Service ensures that adequate resources are allocated to ensure that the long outstanding consent audit is completed and that it reports upon its completion to this Committee independently ;
- iii. the Council's development of its GDPR Article 30 Record of Processing Activities is supported by the Learning Service;
- iv. my future reports to this Committee report on assurances received by me from the Heads of Service as Information Asset Owners.

Appendix 1 Information about Regulatory Oversight

1.1. The Investigatory Powers Commissioners Office

The Investigatory Powers Commissioners Office (IPCO) oversees the conduct of covert surveillance and covert human intelligence sources by public authorities in accordance with the Police Act 1997 and the Regulation of Investigatory Powers Act 2000 (RIPA). The RIPA regime aims to ensure that directed surveillance is carried out in a way that is compliant with human rights. This is achieved through a system of self-authorisation by senior officers who have to be satisfied that the surveillance is necessary and proportionate; the self-authorisation must then be judicially approved.

As the Council's SIRO, I am also the Senior Responsible Officer (SRO) for the Council's compliance with RIPA procedures.

The Council's processes and practices were inspected by the IPCO during the period of this report. The inspection was favourable and no formal recommendations were made. Although it is acknowledged that the Council makes responsible but limited use of RIPA, the relevant roles, policies, procedures and training are necessary and must be in place.

1.2 Information Commissioner

The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 2018 and the 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 Information Commissioner 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.

The ICO contacted the Council in respect of 2 DPA complaints. Whereas the matters were not, ultimately, investigated by the ICO, the Council was asked to review its responses to the complainants and take any appropriate steps to ensure that the complaint were dealt with fully. The complaints have been reviewed and the matters are concluded.

Freedom of Information Act Appeals to the ICO

One appeal was lodged with the ICO in this period.

The appeal related to the refusal to disclose a report and due to the time lapse since the original response, it was deemed appropriate to disclose the report in full to the complainant

1.3. Surveillance Camera Commissioner

The office of Surveillance Camera Commissioner (OSCC) oversees compliance with the Surveillance Camera Code of Practice. The office of the Commissioner was created under the Protection of Freedoms Act 2012 to further regulate CCTV.

The Council has been using **the Surveillance Camera Commissioner's CCTV specific Data Protection Impact Assessment (DPIA)** since 2019-2020 and it is now used by the Council whenever a new CCTV system is proposed.

A CCTV Single Point of Contact was appointed during 2019 - 2020 at the suggestion of the SCC to local Authorities. The Data Protection Officer reviewed the Council's CCTV processes and resources during the period of the last report; this resulted in the **creation of a register of CCTV of systems, managers and operators**. Importantly, the review identified the governance gaps surrounding historic CCTV systems which existed before the introduction of the SCC Code. A **new CCTV resource** was also developed on the Council's IT Portal. The resource contains the CCTV Data Protection Impact Assessment Template, as well as Guidance. A further audit of CCTV systems is tabled to recommence outside of the period of this report.

During the period of this report, CCTV users and managers were trained in the data protection elements of using CCTV.

Appendix 2. The number of data security incidents recorded by the Council during the year.

Data security incidents (20/21): 30 incidents

Level 0 – Level 1 (near miss or confirmed as a data security incident but **no** need to report to ICO and other regulators) = 28

Level 2 incidents (data security incident that **must** be reported to the ICO because of the risk presented by the incident = 2

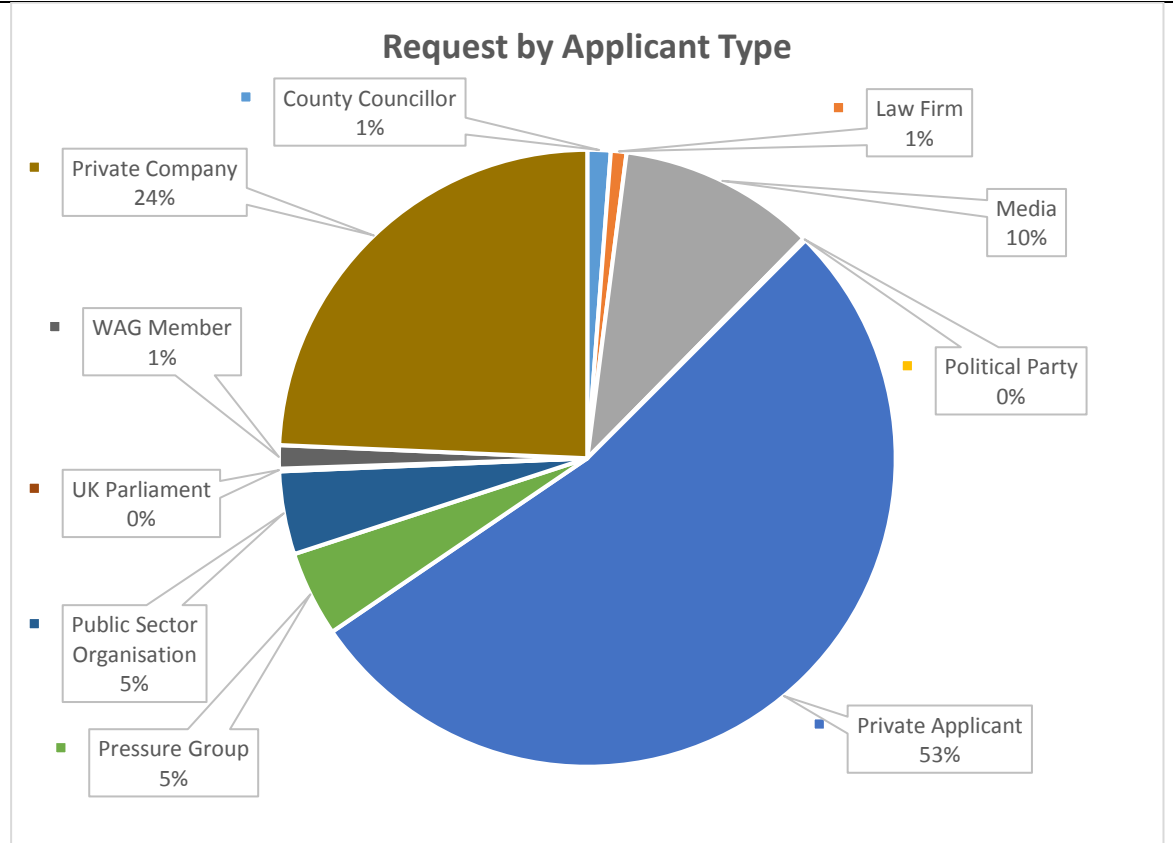
Category Level 0 -1	Number
Disclosed in error	26
Lost data/ hardware	1
Technical	1
Category 2	Number
Unauthorised disclosure	1
Other	1

Appendix 3. Information about Freedom of Information Act 2000 requests and complaints

3.1 Freedom of Information Act 2000 requests and Internal Reviews

During 1 April 2020 and 31 March 2021 the Council received 736 requests for information, comprising in total 5397 individual questions.
The Requests are broken down by applicant type, below.

Total Number of Requests Received	736
Total Number of Questions Received	5397
Requests Per Service	
Corporate (Authority wide) = Requiring a co-ordinated response.	134 requests (1214 questions)
Democratic Services	2 requests (20 questions)
Economic Development	5 requests (16 questions)
Elections	3 requests (8 questions)
Health & Safety	2 requests (40 questions)
Highways	76 requests (558 questions)
Housing	33 requests (290 questions)
HR	28 requests (129 questions)
ICT	31 requests (330 questions)
Learning	33 requests (411 questions)
Libraries etc	2 requests (30 questions)
Leisure	5 requests (28 questions)
Legal	8 requests (58 questions)
Maritime	2 requests (18 questions)
Planning	35 requests (232 questions)
Property	11 requests (75 questions)
Public Protection	82 requests (605 questions)
Resources	118 requests (635 questions)
Registration Service	1 requests (3 questions)
Social Services	91 requests (449 questions)
Transformation	1 requests (10 questions)
Waste	33 requests (238 questions)



3.2 Requests for Internal reviews

Of the 736 requests, 5 resulted in an Internal Review of the responses made by the Council. The outcomes are as follows:

- In 2 cases the original decision was upheld;
- In 2 cases, the original decision was upheld but the Internal Review required the disclosure of additional information.
- In 1 case, the original decision was overturned. A new response was sent and the requested data disclosed.

Appendix 4. 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 infringed their data subjects rights.

Data Protection Act Complaints to the Council

5 DPA complaints were received, of which 4 were investigated:

- 1 related to requests for **erasure** of personal data;
- 2 related to requests for **rectification** of personal data
- 2 complaints related to an **objection** to the Council's processing of personal data

Following investigation by the Data Protection Officer, it was found that the 4 complaints were not upheld. The Council's processing was considered to be lawful and the data subject rights were not compromised.

The remaining complaint could not be investigated as the individual failed to provide adequate proof of their identity at the request of the DPO.

Appendix 5. Information about the number of data protection Subject Access Requests and the Council's compliance.

Subject Access Requests and compliance

25 SARs were received – of the 22 SAR's responded to, 78% responses sent within the appropriate deadline.

2 SARs are on hold and cannot be progressed as the necessary evidence has not been received and 1 was received at the end of the reporting period and was therefore not due a response within the period of this report.

Appendix 6. Data Protection Work plan

The work plan for data protection, which was developed in the months following the implementation of the new data protection legislation in 2018, has been reported to the Committee previously.

The work plan is owned by the Council's Senior Leadership Team and this establishes data protection at the core of the Council's operations. The purpose of the work plan was to provide greater assurance regarding the Council's compliance. The various elements of the work plan were accompanied by *training*, *guidance notes* and *templates* to assist the Service's staff to complete the stages. All aspects of that work plan have long since been completed save for the information below.

The outstanding elements of the current work plan (to March 2021) and the Services which have not completed the actions are shown below:

Action		Non-compliant Service
1.	To review the use of consent as a lawful ground for processing and to review consent recording processes in order to challenge the reliance on consent as a lawful basis by partners.	Learning Service
2.	To develop and monitor the Council's Article 30 ROPA by including links to Privacy Notices, Sharing Protocols, major Contracts or Data Processing Agreements	Learning Service

Appendix 7. Information Governance training

Subject	Category of Staff	Frequency of Training	Compliance Status
Data Protection/ Freedom of Information	New staff - ALL	On joining	Training delivered
Data Protection Policy Acceptance	ALL staff - mandatory	On joining, thereafter every 2 years	
Data Protection Training	ALL staff - mandatory ALL Members & Co- opted Members.	Every 2 years	Training delivered
Freedom of Information / Environmental Information Regulations	Current DP / FOI Service Co-ordinators (also Information Asset Administrators)	1 hour update sessions every 2 years – to be replaced by e- learning modules.	Training delivered
Subject Access Requests	Current DP / FOI Service Co-ordinators	As required	Services identify requirements and arrange training.
Information Governance	Senior Information Risk Owner (SIRO)	Bi-annual	Not required during the reporting period
Data Protection / Freedom of Information	IAO's (Heads of Service)	Every 2 years	Not required during the reporting period
RIPA	RIPA SRO RIPA Authorising Officers RIPA Coordinating Officer	Every 2 years	Training delivered
CCTV	CCTV system administrators	Every 2 years or as required	Training delivered

Appendix 8. Survey of Council Publication Scheme

1. At the September 2020 meeting of the Governance and Audit Committee there was discussion about the possibility that the Council could make more information available in order to better manage the impact of FOIA requests on Services.
2. The benefits of routine publication of information are set out in the Act: when a request for information is received for information that is readily available on the Council's website it engages an exemption, which can simplify the response.
3. In order to assess whether the Council's routine publication of information is currently an effective factor in minimising the impact of FOIA requests, a self-assessment tool was prepared and circulated to the Council's Services. All Services except for Resources participated in the self assessment.
4. Over 15 years ago, the Information Commissioner proposed a single cohesive publication scheme as the most suitable solution. However, the trend in website development has been to move away from this; compliance with the FOIA's publication requirements is achieved by means of the search-box facility on the website.
5. In terms of the findings of the survey, Services were able to demonstrate that they publish proactively in accordance with the Publication Scheme. However, as far as reducing the impact or burden on the Services of responding to FOIA requests is concerned, it is unlikely that the publication of information reduces the number of requests. FOIA applicants want to know the *why* as well as the *what*. Routine publication of documents rarely provides the context that FOIA applicants require. There is also evidence to suggest that published information results in additional requests.