CYNGOR SIR YNYS MON / ISLE OF ANGLESEY COUNTY COUNCIL	
MEETING:	**AUDIT & GOVERNANCE COMMITTEE**
DATE:	**3 September 2019**
TITLE OF REPORT:	**INFORMATION GOVERNANCE – SENIOR INFORMATION RISK OWNER'S ANNUAL REPORT FOR 1ST APRIL 2018– 31ST MARCH 2019**
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 2018 to 31 March 2019 and to summarise current priorities.

Introduction

This report provides an overview of the Council's compliance with legal requirements in handling corporate information, including compliance with the General Data Protection Regulation; Data Protection Act 2018; Freedom of Information Act 2000; Regulation of Investigatory Powers Act 2000 (Surveillance) and relevant codes of practice.

The report also includes assurance of on-going improvement in managing risks to information during 1 April 2018 to 31 March 2019. It reports on the Council's contact with external regulators and provides information about security incidents, breaches of confidentiality, or "near misses", during the relevant period.

Background

For the purpose of this report, Information Governance (IG) is defined as how the Council manages and uses personal information; that is information about people, be they service users or employees.

The Council collects, stores, processes, shares and disposes of a vast amount of information. Specifically, though, holding and using information about people includes inherent risk of loss, damage or inadvertent disclosure. Personal data is also expensive to gather, use and hold, and, when things go wrong, it is expensive to replace. It follows that it should be managed as efficiently as all other valuable Council assets, like people, business processes and infrastructure.

The Council must meet its statutory responsibilities effectively and protect the personal information it holds throughout its life cycle; from creation, through storage, use, retention, archiving and deletion.

Significant breaches of data protection legislation may result in monetary penalties. Additionally, if data about individuals is wrongly shared or disclosed, thereby causing them harm (distress and/or tangible damage) they are entitled to compensation.

Information Governance at the Council

It is considered good practice to have a SIRO to provide information governance direction and leadership at a senior level. This role is undertaken here by the Head of Function (Council Business) and Monitoring Officer.

The SIRO receives regular updates on how well each Service is performing in key information management areas. The SIRO escalates information governance risk to the other members of the Council's Senior Leadership Team and recommends mitigations to the relevant Heads of Service.

Other IG roles within the Council include:

- **Data Protection Officer** – the role is created by the GDPR and Data Protection Act 2018
- **Corporate Information and Complaints Officer**
- **Information Asset Owners** - Heads of Service who '*own'* the assets and are responsible for making sure their information assets properly support the business, and that risks and opportunities connected with it are monitored and acted upon (included within current job descriptions);
- **Information Asset Administrators** – nominated officers who ensure that policies and procedures are followed, recognise actual or potential

security incidents, and maintain the information asset registers (included within current job descriptions);

- **Internal Audit**

The number of data security incidents recorded by the Council during the period 1 April 2018 to 31 March 2019

Data security incidents (18/19): 29 incidents

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

26

Level 2 incidents (data security incident that **must** be reported to the ICO and other regulators (as appropriate).

3

Category Level 0 -1	**Number**
Disclosed in error	19
Lost data/ hardware	5
Technical security failure	1
Other – misplaced hardware	1
Category 2	**Number**
Lost data Disclosed in error	1 2

For the purposes of comparison, the number of **Data security incidents (17/18): 20 incidents**

Freedom of Information Act 2000 requests and complaints

Freedom of Information Act requests
During 1 April 2018 to 31 March 2019, the Council received **1052** requests under the Freedom of Information Act 2000 which contained **7532** questions in total.

Freedom of Information Act Internal Reviews
During the period of the report, there were 20 requests for an Internal Review of an FOIA response. In 9 cases, the review upheld the original responses. One case was not upheld and a new Section 1 response was sent. I request was refused as a response has been sent prior to receipt of the request for an internal review.

Freedom of Information Act Appeals to the ICO
6 appeals were lodged with the ICO in this period, 4 cases – the Council were asked to send responses 1 case was withdrawn 1 case – the Council's response was upheld

Information about the number of data protection complaints made to the Council during 1 April 2018 to 31 March 2019 by individuals about its processing of their personal information.

Data Protection Act Complaints to the Council
8 DPA complaints were made and investigated 2 pre and 6 post GPR

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 1 April 2018 to 31 March 2019.

Data Protection Act Complaint Investigations by the ICO
No DPA complaints were investigated by the ICO

Information about the number of data protection Subject Access Requests and the Council's compliance during 1 April 2018 to 31 March 2019.

Subject Access Requests and compliance
46 SARs were received
81 % responses sent within the statutory deadline for SARs and complex SARs.

Regulatory Oversight

Oversight of aspects of IG is provided by a number of regulators, reflecting the legislation and codes of practice which relate to it. The Council is required to routinely report to the regulators on a number of issues and, where required to do so, on an ad-hoc basis, in respect of certain matters. The regulators are listed below.

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. These are legislation that impact the way the Council uses information and, when the legislation creates an access to information regime, the way the Council ought to respond to requests.

The Information Commissioner has power to assess any organisation's processing of personal data against current standards of 'good practice'. This can result in enforcement action, as is the case with Freedom of Information Act requests, or enforcement action and fines, as is the case with data protection.

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 which 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.

The Council makes very little use of covert surveillance and covert human intelligence sources; please see Appendix 1.

The Council's processes and practices were inspected by the IPCO during September 2018.

The Investigatory Powers Commissioner stated in his report that the Council

> "*demonstrated a level of compliance that removes, for the present, the requirement for a physical inspection….*
>
> *Your Council was found to have a good policy and guidance document and has provided training for authorising officers and applicants* [since the last inspection]".

The Commissioner required that the Council:

- **Undertake a review of its extant CHIS authorisation**
  This was done on 3 October 2018

- **Minor amendments to the Council's Policy documents**
  These were made in October 2018

- **Provide refresher training for authorising officers and applicants**
  The training was placed on the Data Protection Action Plan (the 'Plan', see Appendix 2) and will be delivered outside the period of this report as other areas were deemed to be a priority

Office of Surveillance Camera Commissioner

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

In February 2019, the Surveillance Camera Commissioner wrote to the Council and all local authorities to recommend that the Data Protection Officers of each authority be designated as Senior Responsible Owners (SRO) for CCTV and Surveillance Cameras. This step was intended to strengthen the connection between the Code and data protection governance within local authorities. It is likely that this step will lead to further developmental work.

However, the corporate work-plan for data protection includes elements which are intended to improve the Council's governance of its CCTV and Surveillance Camera systems in order to demonstrate compliance with the

legislation and the Code. This work is in progress outside the period of the report.

Data Protection Action Plan

Following on from the initial period of GDPR implementation, analysis of the Council's data protection assurance documents suggested key areas for further development and investigation. These elements were incorporated into a plan for the year. The Plan (see Appendix 2), which was endorsed in November 2019 by the Council's Senior Leadership Team, is intended to provide evidence of compliance on a detailed operational level and to introduce necessary improvements in areas of higher risk. Implementation of GDPR/DPA 2018 was not an event, but a process of continuous improvement.

The Plan seeks to address issues which present the highest risks to the Council within the Services which are deemed themselves to be high risk because of the nature of the personal data processing that occurs within those Services. This is why particular attention is given to *Children and Families Services*, *Adult Services*, *Learning* (which includes the Local Education Authority) and *Housing*.

Progress Against the Action Plan during the period of the report

<u>Training</u>

1. Data Protection training

The importance of training as a safeguard of data protection compliance is clear. Whereas the Council has trained on data protection matters since 2013, the introduction of the new data protection legislation in 2018 required fresh training across the board.

1.1 E-Learning

In May 2018, a mandatory e-learning module was introduced for all staff to provide a foundational level of knowledge about the requirements of the GDPR.

During the period covered by this report, the participation of staff within the Council's Services with the e-learning is shown below:

Adults	59%
Children and Families	98%
Transformation	88%
Council Business	100%
Highways, Waste and Property	32%
Housing	82%
Learning	40%
Regulation and Economic Development	54%
Resources	89%

The e-learning module was also made available to County Councillors and Co-Opted Members of the Council. Completion of the e-learning module (or attendance at the trainer-led sessions) was mandatory.

During the period of this report the participation of Members with the data protection training is shown below:

Member participation with data protection training
Elected Members' participation: 64%
Co-opted Member's participation: 19%

However, the e-learning module highlighted the need for further training to encourage responsibility and ownership for personal data within services by Council officers.

Other methods of training were therefore delivered during the period of the report as discussed below.

1.2 Trainer led learning

In order to be effective, training has to be relevant to practical work situations; this is known to be an effective way to develop a culture of awareness and personal responsibility.

A training module was developed which was intended for staff roles which the Council's record of data security incidents demonstrate to have a key role to play in ensuring data security and compliance with the legislation.

The training was delivered to frontline staff and middle managers, roles which are important to ensuring data security and ensuring that the Council procures services and develops its business activities in a compliant way that incorporates *Privacy by Design and Default*. (i.e. systems and processes).

A series of trainer led sessions was held for staff in the key roles identified by their Head of Service. The training was attended by 61% of those required to attend. The sessions were well received by attendees and a further round of sessions has been arranged to "mop up" those who did not attend the first session.

Attendance by Services is shown below and includes only those nominated for attendance by the Heads of Service

Adults / Oedolion	59%
Children and Families / Plant a Theuluoedd	57%
Transformation / Trawsnewid	100%
Council Business / Busnes y Cyngor	100%
Learning / Dysgu	62%
Regulation and Economic Development Rheoleiddio ac Datblygu Economaidd	53%
Resources / Adnoddau	66%

A trainer led session was also held for Members. The attendance of Co-opted Members was not mandatory.

A Data Protection Basics training book was developed in draft during the period of this report, in order that managers could deliver effective training to staff who do not have access to the Council's network or email accounts. The training is paper based and incorporates a testing element. The initial draft was considered too technical during testing, and a new draft was prepared. The Council is seeking the views of the Information Commissioner on the content.

Two training sessions on Data Subject Access Requests were held for key staff with specialist roles and responsibilities for subject access requests undertaking this role within their respective Services. Attendance of relevant staff was 100%.

2. Freedom of Information Act 2000 Training

Access to information law is complex and it is important that the Council arranges regular training for staff with responsibility to respond to access to information requests. The number of requests received is increasing year on year; as discussed above, the Council received 7532 questions during the year. This places a considerable burden on a limited resource particularly when the compliance officers responsible for issuing responses to requests have other duties within their respective services. As the risks of non-compliance with a fast changing legal framework are increasing, the importance of training is amplified.

During the period of the report a review of the key contacts for Freedom of Information Act 2000 requests (and other access to information regimes) was undertaken. The number of contact officers has been increased to include deputies, which will improve compliance rates during times of annual leave or sickness absence.

Training was not delivered during the period of the report, but has now been arranged for delivery in Autumn 2019.

3. RIPA Training

Following on from the recommendations of the Investigatory Powers Commissioner, a review of the training needs of the Council's Authorising Officers was arranged. This was prompted by a comment made by the inspector that for a Council that makes limited use of RIPA, fewer Authorising Officers could be better than training a larger number of Authorising Officers.

The SIRO decided to pause the review in order to focus on other elements of the Data Protection Action-Plan, because of its low use and judicial oversight made it a low risk to the Council. The review and delivery of the training is due to take place during 2019-20.

Consent Audit

Aside from training, the most important key element of the Work-Plan was to audit the reliance of the Council's Services on consent as a basis for processing personal data. The risks of making inappropriate uses of consent as a basis for processing personal information are high. Similarly, using appropriate consent incorrectly can result in regulatory action.

Consent has been used inappropriately throughout the public sector for a number of years. It was seen as being convenient and more inclusive of people's interests than relying on the statutory powers which drive the Council's functions.

The new legislation places a duty on the Council to review its uses of consent and take remedial action if consent is not the appropriate legal basis for processing personal data.

During the period of the report, a survey was developed and undertaken in order to provide an objective means of analysing each interface the participating Services have with the public, be this paper forms or web-based forms. Undertaking the survey has been time intensive, because it was often not apparent to the Services themselves that reliance on consent was being utilised and that it was often inappropriate. A common feature was that, as part of trawling for points of contact with the public, additional forms came to light. The audit has resulted in increased intelligence about the Services' processes.

The Council's **Social Services** (Children and Families, and Adults) made excellent progress during the period of the report. Quality assurance of the survey results by the Data Protection Officer has commenced. The quality assurance work will be completed by the end of August 2019.

The Council's **Housing Service** also made excellent progress with the audit, nearing its completion by the end of the period covered by this report. It is anticipated that the quality assurance element will be completed by December 2019.

The Council's **Learning Service** however made little progress with the audit. Some work has been undertaken by managers but the audit lagged behind schedule. It is possible that other factors exhausted the Services' capacity during the period, including complex subject access requests.

Work to quality assure the audit continues after the period of this report.

CCTV Assurance

The Surveillance camera elements of the Work-Plan were developed in anticipation of the Surveillance Camera Commissioner's renewed interest in local authorities. The legislative framework for surveillance camera systems

is complex, which places greater responsibilities on the Council to audit its use of CCTV.

During the period of the report, a draft Council policy was developed in accordance with the Data Protection Action-Plan and an audit, which captures all the relevant elements of the SCC's *Code,* was developed in draft. The audit is a foundational step in the creation of a new corporate asset register.

The use of the SCC's Data Protection Impact Assessment for Surveillance Camera Systems was adopted by the Data Protection Officer.

Assurance will be reported in next year's report.

The Council is not responsible for the compliance of schools with the legislation or the Code.

Recommendations

The SIRO makes recommendations to the Committee that:

i. all Members who have yet to undertake the e-learning data protection module do so within three months of this meeting;

ii. the Learning Service ensures that adequate resources are allocated to ensure that the consent audit is completed by the end of March 2020;

iii. the Council's audit of its CCTV systems is supported by the Services;

iv. the Data Protection Officer for Schools considers the risks of CCTV and provides support and guidance to the schools on best practice;

v. the Committee endorses the remaining actions on the Data Protection Action-Plan as reflecting the information governance risks currently facing the Council.

Appendix 1

Summary of annual return made to the Investigatory Powers Commissioner's Office in respect of the Regulation of Investigatory Powers Act.

Regulation of Investigatory Powers Act		
i.	The number of applications made for a CHIS authorisation?	**1**
ii.	Of these, the number of applications made for a Juvenile CHIS authorisation?	**Nil**
iii.	The number of CHIS authorisations successfully granted?	**1**
iv.	Of these, the number of Juvenile CHIS authorisations successfully granted?	**Nil**
v.	The number of urgent applications made for a CHIS warrant?	**Nil**
vi.	Of these, the number of urgent applications made for a Juvenile CHIS authorisations?	**Nil**
vii.	The number of CHIS authorisations granted in an urgent case?	**Nil**
viii.	Of these, the number of Juvenile CHIS authorisations granted in an urgent case?	**Nil**
ix.	The number of CHIS authorisations that were renewed?	**Nil**
x.	The number of CHIS authorisations that were cancelled?	**Nil**
xi.	The number of CHIS authorisations extant at the end of the year?	**1**
xii.	The number of applications made for a Directed Surveillance authorisation?	**Nil**

Appendix 2

Data Protection Action Plan

Action	Description		Start date	End date	RAG Status
1. Training	Address identified data protection and other information governance training needs.	1.1 Identify data protection training (1) To ensure that staff identified by the Heads of Service receive additional data protection awareness training;	1/11/18 1/12/18	30/3/19 Within 2 months of training	
		2) To develop a data protection training workbook	15/11/18	1/4/19	
		(3) To ensure that members have access to e-learning module.	15/11/18	30/5/19	
		1.2 Identify RIPA training	15/11/18	1/04/19	
		1.3 General FOIA training to ensure that FOIA Contact Officers are trained to respond effectively.	30/11/18	1/4/19	
2. To review the use of consent as a lawful ground for processing and to review consent recording processes	Audit the use of consent in: Adults; Children; Housing, Education forms. Also to challenge the reliance on consent as a lawful basis by partners.	Using the Article 30 ROPA as a reference tool, to require relevant Heads of Service to initiate a review to identify where Service customer facing forms refer to consent, or where the use of consent by partners is demonstrated. To commence in (a) Children's; (b) Housing; (c) Adults; (d) Learning, at monthly intervals.	30/11/18	31/5/19	

3. Review and audit Council CCTV systems	To provide the Council with a suitable CCTV Policy and identify key contacts within services, ensure compliance with current Codes and legislation.	In addition to preparing a policy statement and governance arrangements, a desktop audit of current systems and signage must be undertaken, including audit of compliance with data subject rights.	1/1/19	30-6-19	
4. Review RIPA Key Staff	To ensure that the Council has adequate arrangements for RIPA authorisations.	Ensure that relevant Services have RIPA Authorising Officers.	15/11/18	30/12/18	
5. To develop and monitor the Council's Article 30 ROPA	Following on from item 2, to develop the ROPA by including links to Privacy Notices, Sharing Protocols, major Contracts or Data Processing Agreements	To work with (a) Children's Services and (b) Housing to represent all major Sharing Protocols, major Contracts or Data Processing Agreements on the ROPA.	1/7/19	1/12/19	
To develop resources on the Council's Intranet and Policy Portal.	The information on the Intranet (Monitor) is out of date. The pages require revision to provide appropriate information.	Review and refresh data protection content on Monitor; Review and refresh FOIA content on Monitor	1/1/20	1/6/20	