CYNGOR SIR YNYS MON / ISLE OF ANGLESEY COUNTY COUNCIL	
MEETING:	**AUDIT & GOVERNANCE COMMITTEE**
DATE:	**1 September 2020**
TITLE OF REPORT:	**INFORMATION GOVERNANCE – SENIOR INFORMATION RISK OWNER'S ANNUAL REPORT FOR 1ST APRIL 2019– 31ST MARCH 2020**
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 2019 to 31 March 2020 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 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 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.

Information Governance at the Council

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

Other IG roles within the Council include:

- **Data Protection Officer** – required by the GDPR and Data Protection Act 2018

- **Corporate Information and Complaints Officer**
- **Information Asset Owners** – Directors and Heads of Service who '*own'* information assets and are responsible for making sure their information assets properly support the business; that risks and opportunities connected with it are monitored and acted upon (included within revised job descriptions); and, ensure that their staff accept mandatory policies and receive ongoing training to meet identified needs.
- **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 revised job descriptions);
- **Internal Audit**

Senior Information Risk Owner's Statement

The Council's arrangements for information governance have been strengthened following a continuous period of development, triggered initially by the consensual audit of the Council by the information Commissioner's Office in 2013. Whereas the driver for change was initially external to the Council, the subsequent improvements to information governance resulted from the recognition of the Council's senior leaders of the importance and value of good information governance. The Council has been able to identify areas for its own improvement and introduce necessary change organically. This has been evidenced during the period of this report in the areas of surveillance and in the governance of general personal data processing operations.

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, as the events of the final months covered by this report demonstrates.

Of particular note, the Council's information governance policies were reviewed and quality assured during the period of this report. Ten key policies were reviewed in order to ensure their conformity with current ICO guidance and case law. The review also looked for internal inconsistencies, gaps and omissions in the corporate policies and provided quality assurance for the Council's data protection policies, its fundamental corporate safeguard. The policies are due for their next review in 2022.

The latter part of this reporting period saw the commencement of the COVID-19 Pandemic, a period of unprecedented strain on the Council, including its information governance. Many of the innovations and solutions introduced to respond to COVID-19 have involved the use of personal data with data protection implications. The speed at which emergency and interim measures required implementing defied the order of events established in the legislation for data protection and the Council's activity. This meant that the analysis of data protection risks often had to occur concurrently with the implementation of innovative measures. Nonetheless, the Council responded in a pragmatic manner to the challenges of complying with data protection legislation by undertaking verbal Data protection Impact Assessments (DPIA), followed up by written documents almost concurrently with the actual processing getting underway.

The innovative uses of technology to facilitate different ways of working and engagement with the public or partners had important data protection elements. For example, the use of technology in the form of mobile phone apps to enable social workers to maintain contact with service users or hold safeguarding meetings remotely were involved undertaking rigorous data protection work at a fast pace. The sharing of data in new or innovative ways in order to ensure the wellbeing of the public, for example working with foodbanks and other agencies to ensure that vulnerable individuals were supported with the basic necessities of food, involved the analysis and mitigation of data protection risks at an unprecedented pace.

The way that DPIAs have become embedded within the fabric of the Council's operations was highlighted by the way that Services demonstrated their understanding of the need for DPIAs, even amongst the other priorities presenting during the emergency. The cultural awareness of data protection as a key component of the Council's response to the Pandemic was clearly evidenced; the Council's arrangements underwent stress testing.

The Council's processing during the emergency developed quickly and a record of new data processing activity was created in order to contain evidence of the data protection elements of the innovative partnership working, which the Council commenced in response to COVID-19. This record is held centrally by the SIRO and DPO.

Finally, during the latter part of the period of this report, the Council became involved with the data governance aspects of working in partnership to develop the Welsh Government's Track, Trace and Protect strategy. The complexity of the work coupled with the risks of the processing resulted in a regional and national dialogue concerning the relationship of the partner organisations. The SIRO and DPO participated in the effort to develop an alternative framework to the one initially presented to better represent the risks and liabilities of the various partners.

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 and that this was demonstrated during the extraordinary times of the Pandemic. 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;
iii. the Council's development of its GDPR Article 30 Record of Processing Activities is supported by its Services;
iv. the Committee endorses any remaining actions on the Data Protection work plan as reflecting the information governance risks facing the Council.

Appendix 1.

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

Data security incidents (19/20): 31 incidents

Level 0 – Level 1 (near miss or confirmed as a data security incident but **no** need to report to ICO and other regulators) = 31.

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

Category Level 0 -1	**Number**
Disclosed in error	24
Lost data/ hardware	2
Non-secure disposal	2
Unauthorised access	2
Lost in transit	1
Category 2	**Number**
Unauthorised disclosure	2

Appendix 2

Information about Freedom of Information Act 2000 requests and complaints

Freedom of Information Act requests for Internal Review

During 1 April 2019 and 31 March 2020 the Council received 6905 requests for information under the Freedom of Information Act 2000. The category of applicants is set out as follows:

Category of Applicants	Number of requests
County Councillor	64
Law Firm	24
Media	1440
Private applicant	2635
Pressure Group	328
Public Sector Organisation	684
U.K. Parliament	9
WAG Member	137
Private company	1584
Total:	**6905**

Of the 6905 requests, 12 resulted in requests for an Internal Review of decisions made by the Council. The outcomes are as follows:

- In 9 cases the original decision was upheld;
- 2 cases resulted in the Council Service's response being changed and new refusal notices issued;
- In one case, it was decided that a Section 21 refusal notice should have been issued as the information was available to the applicant by other means.

Appendix 3

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 Act Complaints to the Council
7 DPA complaints were made and investigated: 6 related to requests for erasure of personal data; 1 complaint related to an objection to the Council's processing of personal data. None of the complaints was upheld, the Council's processing was lawful and the data subject rights could not be exercised.

Appendix 4

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

Subject Access Requests and compliance
24 SARs were received. 83 % responses sent within the one month deadline. The responses to three of the requests were late by a few days; one request was complex and took 3 months to respond (one month over the statutory time permitted for complex cases).

Appendix 5

Information about Regulatory Oversight

5.1. 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.

The Council's processes and practitioners were last inspected by the IPCO during September 2018. During the period of this report, **the Council's Policy and procedures were revised**. The Investigatory Powers Commissioners Office kindly reviewed the amended Policy and gave positive feedback, stating "*checked through your revised policy, guidance and document and it is very good…the document is accurate… very useful advice for practitioners*".

In order to comply with the new surveillance Codes of Practice, the Council's Policy was accepted by the Council's Members. It is intended to seek the acceptance of Members on an annual basis.

The Council's SIRO is also Senior Responsible Officer (SRO) for the Council's RIPA compliance. The process of **designating RIPA Authorising Officers was revised** and a new process was introduced, which was also reviewed by IPCO. The number of Authorising Officers have reduced over previous years and **additional Authorising Officers were designated**.

As shown in the table below, which replicates the information provided to IPCO, the **Council makes responsible but limited use of RIPA**. However, the development of the Council's Policy and processes during the period of the report represents a significant strengthening of the Council's arrangements.

A summary of the Council's use of the Regulation of Investigatory Powers Act 2000 during the period.

Regulation of Investigatory Powers Act		
i.	The number of applications made for a CHIS authorisation	**2**
ii.	Of these, the number of applications made for a Juvenile CHIS authorisation	**0**
iii.	The number of CHIS authorisations successfully granted	**2**

iv.	The number of CHIS authorisations that were renewed	**1**
v.	The number of CHIS authorisations that were cancelled	**1**
vi.	The number of CHIS authorisations extant at the end of the period	**1**
vii.	The number of applications made for a Directed Surveillance authorisation	**1**
viii.	The number of Directed Surveillance authorisations successfully granted	**1**
ix.	The number of Directed Surveillance authorisations that were cancelled	**1**
x.	The number of Directed Surveillance authorisations extant at the end of the period	**0**
Key: CHIS – Covert Human Intelligence Sources		

5.2 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.

Data Protection Act 2018 complaints investigations by the ICO
The ICO contacted the Council in respect of 3 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 was dealt with fully. The complaints were reviewed and concluded.

Freedom of Information Act Appeals to the ICO
A total of 3 appeals were lodged with the ICO in this period,

- One was withdrawn prior to investigation;
- In one instance, the Council was required to provide advice and assistance to the requestor within a specified timescale
- In one instance, the Council were required to respond to the request within 10 working days.

5.3. 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.

During the period of this report, the Council introduced the **use of the SCC's CCTV specific Data Protection Impact Assessment (DPIA)** and Guidance. The DPIA is used by the Council whenever a new CCTV system is proposed. The SCC's produced its Welsh language version of the DPIA and Guidance at the request of the Council.

The Data Protection Officer reviewed the Council's CCTV processes and resources during the period of the 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 Policy** was also developed. The Policy assists the Council's Services by regulating their interaction with third parties, such as the Police, who make a reasonable and proportionate use of the Council's CCTV systems.

The Council also **participated in the SCC's survey of Local Authority CCTV** practice during the year, but awaits further contact from the Commissioner. Nonetheless, the adoption of a new CCTV Policy and governance processes during the period of the report is a major improvement of the Council's arrangements.

Appendix 6

Review of Data Protection Policies

The Council's data protection policies are a fundamental corporate safeguard. During the period of this report, a review of the Council's data protection policies was undertaken. This was the first review of the policies since the implementation of the new data protection legislation in 2018. The review considered the 10 key policies in order to ensure their conformity with current ICO guidance and case law. The review also looked for internal inconsistencies, gaps and omissions in the corporate policies.

The Council's Data Protection Policy is a mandatory policy for staff and Members, who are required to accept the policy on the Council's policy acceptance system. The Data Protection Policy will be reissued to staff for acceptance outside the period of this report. The other data protection policies are made available as resources on the policy acceptance system, along with resources on the Council's intranet site.

The completion of the review represents a major landmark in the Council's information governance arrangements. The policies are due for review in 2022.

Appendix 7

Data Protection Work plan

A work plan for data protection was developed in the months following the implementation of the new data protection legislation in 2018. 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 is to provide greater assurance regarding the Council's compliance. It is apparent that the intelligence gathered through undertaking the tasks assists to identify areas for possible development. Therefore, the work plan has a cyclical and iterative quality, which strengthens the governance of the Council's processing of personal data, thus providing the SIRO with increased assurance.

Below is a summary of the current work plan (ending March 2021). The items shown as outstanding and requiring completion will be addressed as soon as the Services are able to resume the work.

Key element		Summary of progress	Outstanding elements
1	Address identified data protection and other information governance training needs.	Data protection and Freedom of Information Act training was provided during the period.	The production of a hard-copy data protection workbook for staff without access to computers is outstanding. A draft has been prepared but its use may not be possible due to changes in work practices. **This is to be explored further during 2020-2021.** RIPA Training for key responsibilities was not delivered due to COVID-19. **Training will be delivered during 2020-2021.**
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, Learning forms. Also to challenge the reliance on consent as a lawful basis by partners.	The audit has been concluded in all services except for Learning. This element has resulted in a significant number of Council forms being redesigned to ensure compliance.	The Audit is not complete in Learning. The work had recommenced but was stalled by COVID-19. **This work to recommence during 2020.**
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.	This work was completed as described above.	
4	**Review RIPA Key Staff** To ensure that the Council has adequate arrangements for RIPA authorisations.	The review was undertaken and completed as described above.	
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		This work will recommence during 2020.

	Protocols, major Contracts or Data Processing Agreements		
6	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.	Content requiring revision has been identified.	This work is dependent upon the ICO publishing GDPR compliant guidance and advice. The action will be delayed until such times as the national regulator's site is updated.
Key: ***Green*** indicates completed elements; ***Yellow*** indicates outstanding elements			