CYNGOR SIR YNYS MON / ISLE OF ANGLESEY COUNTY COUNCIL	
MEETING:	**AUDIT & GOVERNANCE COMMITTEE**
DATE:	**19 September 2018**
TITLE OF REPORT:	**INFORMATION GOVERNANCE – SENIOR INFORMATION RISK OWNER'S ANNUAL REPORT FOR 1ST APRIL 2017– 31ST MARCH 2018**
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**

1. 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 2017 – 31 March 2018 and to summarise current priorities. The report also provides an update on the Council's progress with its GDPR Implementation Plan; this element of the report spans the period 25 May 2018 to 31 July 2018.

2. Introduction

This report provides an overview of the Council's compliance with legal requirements in handling corporate information, including compliance with the Data Protection Act 1998; 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 2017-2018; and also identifies future plans. 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.

This report follows the format of the previous Annual Report. Whereas this report contains an update on the issue of GDPR implementation between the period 31 March - 31 July 2018, it is the intention of the SIRO to retain the focus of future reports on the period of the financial year.

3. Background

IG is the way organisations process and manage information. In its broadest sense, the term covers the whole range of corporately held information, including financial and accounting records, policies, contracts etc. However, for the purpose of this report, IG is

defined as how the Council manages and uses *personal information*; that is information about people, be they service users or employees.

Sound IG provides assurance that the way we deal with personal information is effective, lawful and secure. Legislation places a responsibility on the Council to keep personal information safe and IG provides a means to respond if the security of personal information is compromised.

4. Information Governance at the Council

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.

The main statutory driver for the period of the report was the Data Protection Act 1998; significant breaches of which 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.

It is useful to explain at this point that a considerable amount of audit work, including that of the Information Commissioner's Office (2013-2014) has highlighted deficiencies in the Council's data protection arrangements. Since 2013, the Council has invested in improving its compliance with the 1998 Act and now has in place the relevant policies and procedures to support compliance with the Act.

It is considered good practice to have a SIRO to provide direction and leadership at a senior level. This role is undertaken here by the Head of Function (Council Business) and Monitoring Officer. In order to address information risk, a **Corporate Information Governance Board** (CIGB) was established in November 2014, chaired by the SIRO. This Group is an appropriate forum for addressing IG issues. It receives reports on how well each Service is performing in key information management areas. It assesses risk, and recommends and monitors remedies to mitigate risks to information assets owned by the relevant Heads of Service. The CIGB may report matters directly to the Council's Senior Leadership Team.

Other IG roles within the Council include:

- **Corporate Information Governance Manager (Data Protection Officer post 25 May 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 revised 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 revised job descriptions);
- **Internal Audit**

5. Key Organisational Information Risks and Controls

Non-compliance with protection legislation is likely to be the primary information risk for the Council and therefore this report does not refer to the adequacy of the controls and mitigations of non-personal information risk.

To this end, much progress has been made to develop awareness about personal data risk in order to introduce mechanisms to manage the risk in accordance with best practice and in anticipation of data protection reform.

The Council has identified risks around personal data in its corporate and service risk registers.

The Council recognises that harm and distress to individual(s), financial penalties, enforcement action, adverse publicity, and loss of confidence in the Council are risks associated with its personal data assets.

The Council also recognises the following risks to the security of its information:

- **negligence** or **human error**;
- **unauthorised** or **inappropriate access**, including processing confidential personal data without a legal basis;
- **loss** or **theft** of information or equipment on which information is stored;
- **systems** or equipment **failure**;
- **unforeseen circumstances** such as fire, flood and other environmental factors;
- **inappropriate access**, viewing information for purposes other than specified / authorised;
- **unauthorised access**, using other people's user IDs and passwords;
- **poor physical security**;
- **inappropriate access controls** allowing unauthorised use;
- **lack of training** and awareness;
- **hacking** attacks;
- '**blagging**' offences where information is obtained by deception.

In addition to technical and physical measures to protect the Council's information, the following main technical and organisational safeguards are in place against information risks:

- suitable **IG Policies** and procedures (as required by the data protection legislation at the time);
- a complete **Information Asset Register**;
- suitable **data protection training** (under the 1998 Act) provided to staff on a rolling basis;
- **encrypted ICT** equipment;

- appropriate **service level lessons learnt logs**;
- **data security incident recognition and reporting procedures**, including an investigation and incident-severity analysis methodology;
- **IG KPIs** are gathered and reported to the CIGB every quarter;
- appropriate **IG key roles** identified, designated and trained;
- Council **services are procured** in a data protection compliant way;
- Privacy by Design principles are incorporated into project management methodologies;
- participation in the Welsh Government's **Wales Accord on the Sharing of Personal Information** (WASPI) in order to ensure that sharing of personal data is lawful and proportionate.

Some of the most important and current issues were/are:

5.1 The General Data Protection Regulation.

Part A: Period of the report (to 31 March 2018).

The period covered by the SIRO report saw the development of the Council's plans to implement the General Data Protection Regulation (GDPR). Although the GDPR and the Data Protection Act 2018 would come into force after the period of the report, this issue became the primary information risk for the Council, so it is appropriate to provide information about the work undertaken up to 25 May 2018 and a separate update for the period 25 May to 31 July 2018.

During the period of the SIRO report, the Council's Legal Services developed its approach to what the legislation would look like in operation by designing a suitable programme of work in the form of a Corporate Plan. The Plan was developed from analysis of the GDPR, advice issued by the European Data Protection Board and various drafts of the UK Data Protection Bill. The absence of formal guidance from the ICO, the UK data protection Regulator, was disappointing. The Corporate Plan identified 75 major action points, representing a considerable body of work.

The 75 action points were then summarised into a Five-Stage Plan, intended to assist the Council's Services to work towards compliance with the new legislation. The first stage of the Plan was rolled out in November 2017. The five stages of the Plan were introduced incrementally so that Services had the opportunity to manage the implementation in stages. The stages were:

Stage 1	**Tell People how we use their data**
Stage 2	**Know what we do and why**
Stage 3	**Keep accurate evidence for as long as it's needed**
Stage 4	**All our policies and processes will be compliant**
Stage 5	**Training**

The headings of the stages mask the complexity of the tasks required to implement the Plan. The new legislation required the development of processes, in addition to policies, which impact on the way the Council operates and how it interacts with its customers and others. The Five Stages provided a sound foundation for implementation and operation of

the legislation. All work carried out by each Service was saved to a separate dedicated drive within the Council Network.

The GDPR introduces more stringent and prescriptive compliance challenges, underpinned by a more punitive regulatory environment with serious regulatory penalties of up to the UK equivalent of €20 million euros, possible litigation and serious reputational harm.

However, rather than an enhanced level of potential fines, the real risk to the Council is that the scope of activities for which the Council may be fined is broadened. This shift can be described as being from enforcement by the ICO for breaches of security to enforcement for non-compliance with the rights of data subjects. In particular, as the Council is not only responsible for compliance, it must also be able to demonstrate compliance with the data protection principles. Therefore, the Corporate Plan, summarised in five stages, was intended to establish a culture of monitoring and accountability regarding the Council's processing of personal data.

Part B: GDPR implementation since 31 March 2018 (up to 31 July 2018).

The Council's preparations for the GDPR were audited by the Council's Internal Auditors during April 2018 and a final report was issued on 16 May 2018. The report concluded that there was limited assurance regarding the Council's preparations for GDPR. Work to implement the five stages of the Plan were ongoing at the time of the audit.

The Internal Audit report of 16 May 2018 does not refer to the Council's obligations with regard to the UK Data Protection Act 2018, however the SIRO wishes to report on its implementation, as it is key legislation. The Council's compliance with the Data Protection Act 2018 is set out below.

In the period following the publication of the Internal Audit report, the Council's Plan has been completed as follows.

Stage 1.

This stage was called ***Tell People how we use their data***. It was intended to implement the obligations of the Council regarding *lawfulness, fairness and transparency*. The key outputs were the development of suitable privacy notices which satisfied the legislation's requirements to be specific and detailed yet understandable to their intended audiences.

The privacy notices produced by the Services are published on the Council's website and, where necessary, on paper forms. The privacy notices were subject to corporate quality assurance during July 2018. This review also looked to the evidence of the completed record of personal data processing created as part of **Stage 2** to establish whether the necessary purposes, lawful grounds for processing and references to appropriate data subject rights were represented on the privacy notices.

The Data Protection Officer is satisfied that all Council Services have now met this requirement of the Plan. As part of its ongoing work, the Council will create a digital archive of privacy notices as an evidential record of its compliance over time. .

Stage 2.

This stage was called ***Know what we do and why***. This stage involved the creation of the Article 30 Record of Processing Activities (ROPA). This stage implemented the GDPR *accountability* principle. In addition, it facilitated compliance with the *purpose limitation* and *storage limitation* principles of GDPR. The Council's ROPA is an essential element in its compliance with the accountability principle of the GDPR. The ROPA details all the Council's personal data processing activities, including the lawful grounds for the processing.

The ROPA is not intended to be a static document. Therefore, assurance will be sought from the Services that their elements of the ROPA reflect their current personal data processing activities. As part of ongoing work, the ROPA will be reviewed to examine where the Council makes use of legitimate purposes as a lawful ground for processing. Eventually, it is also intended to insert links from the ROPA to individual information sharing protocols.

The substance of the Council's ROPA was subject to corporate quality assurance in July 2018. The conclusions of the review were that all the Council's Services have now made an adequate contribution to the Council's ROPA. All Services have now met this requirement of the Plan.

Stage 3

This stage was called **Keep accurate evidence for as long as it's needed**. This stage involved the development of a corporate data retention schedule. Identifying suitable data retention periods and examining existing practices is a key element of the storage limitation principle of GDPR. The stage was informed by the outputs of the first two stages of the Plan. Also, the retention periods identified by this stage of the plan helped to quality assure the first two stages.

All the Council's Services have adopted agreed retention periods for the personal data processed as part of their activities. As all the Council's services have now complied with this stage, assurance can be given that the Council has implemented this element of the Plan. However, ongoing operational compliance will be part of future work.

Stage 4

This stage was called ***all our policies and processes will be compliant***. This stage required the development of mandatory data protection policies and mandatory processes. In order to successfully implement the stage, it was recognised that guidance on the mandatory polices and processes would be necessary in order to embed the processes in the working culture of the Council. The GDPR and Data Protection Act 2018 required the review of all the Council's existing Information Governance policies.

Policies and Guidance

The Council was required to develop and adopt new policies to respond to the broader extent of the GDPR, particularly in the area of data subject rights. In addition, it is necessary to support key data protection policies with additional resources and guidance. Policies are published on the *Porth Polisi* and supporting resources are made available on the Council's Intranet.

The Data Protection Act 2018 also mandates specific policy statements relating to the Council's functions which are not covered by the GDPR. The Processing of Special Categories Policy, for example, is required by the 2018 Act and enables the Council to lawfully process special categories of personal data such as criminal records information and also to undertake processing of personal data as part of its law enforcement functions.

The following policies have been developed and published:-

Data Protection Policy

Data Subject Access – guidance notes for staff

Corporate Privacy Notice

Website Privacy Policy

Data Processing Agreement Guidance

Data Protection Impact Assessment Policy

Personal Data Security Incidents Policy

Personal Data Security Incidents Investigation Guidance

Personal Data Security Incidents Reporting Form

Data Processing Policy (appointing processors)

Data Retention Schedules Guidance notes for staff

Data Subject Access Policy

Processes and procedures

In addition to policies, which set out what organisations ought to do, the legislation also specifies that organisations must have certain important processes in place. In keeping with the legislation's emphasis on evidence of accountability, the Council is required to maintain

records of the mandatory processes. The legislation establishes the requirement for data protection impact assessments; data breach reporting; data protection compliant contracts when the Council appoints processors to undertake processing activities on its behalf. The Record of Processing Activity, which is discussed above, is a mandatory requirement.

The Council has implemented all mandatory requirements, supported where necessary with guidance, including:

Initial DPIA Assessment;

Data Protection Impact Assessment (DPIA) and guidance for its completion;

Data Processing Agreement Template and guidance for its completion;

A Data Breach investigation process and letter templates

Stage 5

Training

It should be noted that the Council has mandated data protection training for its staff since 2013. As discussed above, the changes to data protection legislation represent an evolution rather than a revolution of approach. The GDPR specific training builds on an existing knowledge base.

The training stage of the Plan addressed the GDPR specific training needs of the Council and its elected Members. Training provides the Council with assurance that its staff understand the requirements of data protection as it affects them and the Council's service users. This is important, as the level and adequacy of training is a safeguard against data security incidents occurring and also mitigation if an incident must be reported to the Information Commissioner.

Evidence of training, in combination with evidence of policy acceptance, provides a measurable assurance for the Council.

The Council's approach to data protection training is commonly adopted by medium sized and large organisations; namely using e-learning and, where more advanced training is necessary, an additional level of classroom based training. An e-learning module suitable for all staff was introduced in May 2018. This will be supplemented by classroom training for those identified by their Heads of Service as requiring a higher level of training

The take-up of the e-learning module by the Council's services to 31 July 2018 is shown below.

	Completed	Number of staff	Percentage of staff
Adults	68	475	14.32%
Children's	89	112	79.46%
Corporate Transformation	72	81	88.89%
Council Business	32	32	100%
Housing	117	131	89.31%
Learning	71	168	42.58%
Economic	150	315	47.62%
Highways, Property and Waste	75	329	22.80%
Resources	73	94	77.65%
Total as at 31 July 2018	**747**	**1737**	**43%**

Development of Advanced training

It is recognised that some roles within particular services present a greater opportunity to breach data protection law. This is because the nature of their duties involves processing sensitive personal data, often in bulk. The concept of data protection risk has been viewed in the past as being commensurate with seniority within the organisation; the more senior, the greater the data protection risk associated with the role.

The approach now adopted by the Council represents a shift towards a more realistic acknowledgement that risk sits with some roles because of the nature of the duties and not seniority. This model recognises administration staff within some services as demonstrating a greater data protection risk than the Council's Chief Executive; which reflects the experience of the SIRO regarding the number of data protection security incidents reported. Therefore, the Council's Services have nominated key staff for further training. As of 31 July 2018, 118 staff have been nominated for additional training. A training brief has been developed and suitable trainers are being sourced by HR.

Unfortunately, bilingual training tailored for elected Members was not developed in Wales and English only training was developed in England. Therefore, no training for elected Members was provided during the period. However, it is intended to provide access to the e-learning module on GDPR for Members in September 2018. (i.e. the training already available to staff)

GDPR Policy acceptance

As already mentioned, policy acceptance is a safeguard for the Council because it provides evidence that staff have read and understood the policy. The Council's Data Protection

Policy was made mandatory for acceptance between 4/6/2018 and 2/7/2018 and the acceptance rate was 83%. The Data Protection policy remains open for acceptance.

5.2 Information Asset Register

An Information Asset Register is the key mechanism for understanding an organisation's information holdings and the risks associated with them. The register allows the mapping of information content and information systems as they interact with changes to business requirements and the technical environment. The Council's CIGB developed the first version of the Council's Information Asset Register in accordance with best practice. The Information Asset Register captured information about the Council's information assets relating to a broad range of systems.

Development of the Council's Information Asset Register, to identify the main risks associated with each of the Council's business critical systems and assets had been tabled for further development. However, resources have had to be diverted to developing the Council's GDPR Article 30 Record of Processing Activities (ROPA), which builds on the Information Asset Register but has as its focus the processing of data about individuals. (The Information Asset Register is broader) The ROPA is a statutory requirement, therefore the intention is to prioritise the maintenance and development of the Article 30 ROPA. Therefore, the SIRO proposes not to report on the Information Asset Register in future reports but, rather, to provide updates on the development of the ROPA.

5.3 Key IG Policies and Governance

Policies are a key safeguard and are an important element in the Council's IG arrangements. The Council's Heads of Service, in their roles as IAO's, have a singular role in embedding and maintaining policies around the use and handling of information which will improve the quality and consistency of information management across the Council.

Key IG policies are available on the Council's Policy Portal, supported with resources on the Council's Intranet. The policies are reviewed and updated by the CIGB. This work is timetabled and will always be subject to an ongoing programme of review. This section and 5.4 below relate to the period 1 April 2017 – 31 March 2018. For further information about policies developed as part of GDPR implementation see 5.1 above.

5.4 Policy Acceptance ('Click to Accept')

The link between policy acceptance (i.e. system to evidence training, understanding and implementation) and good practice in data protection is clear. The Information Commissioner highlighted this element in the 2013 audit report, and again in 2015, when the Council was asked to ensure that it had procedures for gathering, collating and demonstrating that its staff had accepted key policies. It was also a recommendation from Wales Audit Office in their Annual Improvement Report of 2014-15 dated 1st December 2015.

The Council implemented its policy management system, *Policy Portal*, which served as a library of policies since November 2016. The policy acceptance function was introduced in April 2017. *Policy Portal* provides assurance that key IG policies are being read, understood and formally accepted by individual members of staff. The engagement of the Council's staff

with the *Policy Portal* demonstrates that it has been a success. Moreover, the availability of the Policy Portal has made the task of monitoring data protection compliance post 25 May 2018 significantly easier.

During the period covered by the SIRO report, the Clear Desk Policy, Records Management Policy, and Data Classification Policy were mandatory policies for acceptance by the Council's staff. This ensures that employees are clear about the Council's expectations of them with are regard to information security.

Acceptance rates for the mandatory policies are shown below:

Clear Desk Policy	95 % of users accepted
Records Management Policy	95 % of users accepted
Data Classification Policy	95 % of users accepted

The Policy Portal relies on the Council's Active Directory (AD), and now includes around 1000 active users, following the inclusion of the Learning Service.

The Portal's reliance on the AD has been recognised as a compromise from the outset and this Committee has previously raised concerns that staff who are not AD users are not included in the process. The number of staff who do not have Active Directory accounts is estimated at around 686, including:

Adults Services	Home Carers; Re-ablement; Care Homes; Day Services; Canolfan Byron, Supported Living	350
Children's Services	Specialist Support Workers	21
Learning	Libraries, Youth Workers, Relief Staff	85
Highways, Waste and Property	Cleaners (including schools), Môn Community Transport, Recycling Centres	190
Regulation and Economic Development	Cleaners, café staff, coaching staff	40

AD users with email accounts occupy Microsoft Client Access Licences which are expensive. In addition, the provision of any IT equipment to facilitate access, such as laptops, would also have cost implications. Whilst providing AD accounts for all staff would be technically possible, it would likely be too costly and therefore not a current priority.

5.5 Privacy Impact Assessments

During the period of the SIRO's report Privacy Impact Assessments (PIAs) were a tool to help organisations identify the most effective way to comply with their data protection obligations. An effective PIA allows organisations to address problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. Conducting a PIA was not a legal requirement of the Data Protection Act 1998 representing good practice on the recommendation of the ICO.

During the period of this report **no** PIA's were completed. However, under the new data protection regime, Data Protection Impact Assessments (DPIAs) are a mandatory requirement. The Council's arrangements for conducting DPIAs has been discussed above. It is a statutory requirement for the Council's Services to seek the advice of the Data Protection Officer about the circumstances in which DPIAs are required.

5.6 Training (1 April 2017 – 25 May 2018)

As this report covers the period when a GDPR specific e-learning module was introduced which superseded the corporate IG training, please see the report on the implementation of Stage 5 of the Corporate Plan.

5.7 Personal Data Flows and Information Sharing

During the period covered by this report, in addition to maintaining Information Asset Registers, IAOs were required to understand and document data flows in and out of the organisation. This is largely done by means of the Wales Accord on Sharing of Personal Information (WASPI) information sharing protocols, which are good practice and a means of identifying whether information is being transferred outside the UK and EEA, contrary to the Data Protection Act 1998, then in force. WASPI information sharing protocols (ISPs) identify risks to the security of information and mitigations that are in place. Assured ISPs are published on the Wales Accord on Sharing of Personal Information Website.

The Council also participates in the Quality Assurance process of WASPI ISPs through the North Wales Information Governance Group.

With the advent of the new data protection regime, the importance of information sharing protocols as a safeguard is increased. It is timely, therefore, that the WASPI framework has been entirely revised in response to the new legislation. One benefit of the revised documents and templates is that they are less complex and more flexible. It is anticipated that the Council can now make greater use of the WASPI framework in order to evidence its information sharing. Information sharing will be recorded on the Council's ROPA and reported to the Committee in future reports.

5.8 Data Security Incidents

During the period covered by the SIRO report, the Council's IG arrangements complied with the Information Commissioner's Guidance on reporting data security incidents that breached the Council's statutory duty to protect personal data. Under the 1998 Act, there was no legal duty to report breaches to the Information Commissioner. Information relating to the period after 31 March will be reported in a future report.

The Council has therefore established a Data Security Incident Methodology for identifying, investigating and reporting data security incidents. A corporate log is maintained and service logs are also in operation. Additionally, the Council has developed a tool for assessing the severity of data security incidents. The tool enables the SIRO to assess, in 3 steps, the severity of a data security incident by attributing weight to specific factors relating to the scale and sensitivity of incidents. Incidents are scored as Level 0, Level 1, or Level 2.

- **Level 0** are categorised as near-misses.
- **Level 1** confirmed data security incident but **no** need to report to ICO and other regulators.
- **Level 2** confirmed data security incident that **must** be reported to ICO and other regulators (as appropriate).

During the period of the report it was not yet clear whether major revision of the Council's methodology was required in order to comply with the GDPR. However, after 25 May 2018, a new policy and process were developed in order to comply with the requirement to report data protection breaches to the ICO. The scoring methodology is no longer used because the key factor is now risk to the rights and freedoms of data subjects.

The number of incidents recorded by the Council is provided in **Appendix A.** It is evident that the proportion of Level 0 – Level 1 incidents had decreased (from 33 in the previous report). A significant proportion of the incidents have involved information being sent by email.

5.9 IG Key Performance Indicators (KPIs)

During the period of the report, the Council monitored specific IG KPIs; some on a monthly, and others on a quarterly, basis. It also publishes its access to information data on its website on a quarterly basis.

Indicator Reference	***Indicator***	***Measure + Results for 2017/2018***	***Description***
Q1	Subject Access Request compliance	Number of requests received = **22 requests responded to** Number of responses sent w/n 40 days as a % = **91% (20 out of 22)**	People have the statutory right to access their own personal data that is held by an organisation within a specific time period. It is essential that all services correctly identify SARs so that they may be logged.
Q2	Data security incidents	Number of data security incidents (including near misses) = **20** **19** near misses and **1** matter reported to the ICO	Principle 7 of the DPA states that organisations must have "Appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data." In practice, this means we must have appropriate security to prevent the personal data we hold from being accidentally or deliberately compromised. Recording information about the number of data security incidents is essential.
Q3	Access Rights	Number of leavers = **77**	It is essential that the access rights of all members of staff who leave the authority

Indicator Reference	*Indicator*	*Measure + Results for 2017/2018*	*Description*
		number of leavers whose access rights revoked no later than the final day of work as % (Physical access and ICT) = **100%**	are revoked no later than the final day of work.
Q4	Privacy Impact Assessment completion	Number of new projects where PIA's are required number of PIA's completed as a % = **None Reported**	The Council's Project Management Methodology requires that PIAs are undertaken whenever a new project is considered – see Proposed Business Case Template. *http://monitor.anglesey.gov.uk/corporate-resource/programme-and-project-management/programme-project-and-task-documentation-templates/*
Q5	Privacy Notice Compliance	Number of Privacy Notices completed = number of Privacy Notices copied to CIO as a % **None Reported**	Privacy Notices are required by the law as part of fair processing. People have a right to know why their personal information is being gathered, used and shared

Information about the number of Freedom of Information Act 2000 complaints investigated by the Information Commissioner is provided in **Appendix B**.. In addition, the Council also holds, at the request of complainants, Internal Reviews of its responses under FOIA; this information is also provided at **Appendix B**.

The Council also investigates complaints made to it about data protection matters; further information is provided in **Appendix C**.

Subject access, the fundamental right under the Data Protection Act 1998 to access their own personal information, is an important element of IG. Subject Access Requests (SARS) are often complex and resource intensive. Information about the number of Subject Access Requests and the Council's compliance is provided in **Appendix D**. The majority of SARS are received by Social Services and are complex to process. Whereas Social Services have, as a consequence of the complexity of the requests, sometimes struggled to meet the statutory deadline under the 1998 Act, the new legislation provides that the time for compliance is extended for complex requests.

6. 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.

6.1 Information Commissioner

The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA) later 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'.

6.2 The Office of Surveillance Commissioners and Investigatory Powers Commissioners Office

The Office of Surveillance Commissioners (OSC) (to 31 August 2017) and thereafter 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's processes and practitioners were last inspected by the OSC during August 2015 and were found to be satisfactory. The OSC commended the Council's procedure which ensures that its authorising officers are not based within the service applying for authorisation. The OSC recommended that minor changes were made to the Council's Policy and these were made immediately after the recommendations were received.

The Council did not use RIPA at all during the relevant period..

6.3 Office of 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 completed the OSCC's self-assessment toolkit in December 2015. A Surveillance Camera policy was developed in January 2018, but has not been implemented due to the capacity intensive implementation of GDPR.

7. Conclusions

The SIRO considers that there is significant documented evidence to demonstrate that:

- the Council's arrangements for IG and data protection compliance are reasonably effective;

- the Council has successfully met the challenge of implementing the new data protection legislation and it operates in a compliant way;

- the Council has processes in place to demonstrate compliance to the ICO and it complies with the GDPR's accountability principle;

- Data protection remains, and is likely to always remain, a medium risk to the Council because of the sensitivity of the personal data it processes, which varies between the Services

Appendix A

The number of incidents recorded by the Council during the period 2017-2018

Data security incidents (17/18): 20 incidents

Level 0 – Level 1 (near miss or confirmed as a data security incident but **no** need to report to ICO and other regulators
= **19 incidents**

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

= 1 incident

Category Level 0 -1	**Number**	**Details**
Disclosed in error	12	5 x emails sent using autocomplete function 5 x post sent to incorrect addresses 2 x incorrect version of form published on internet
Lost data/ hardware	1	data put in HQ box but never received by the Service
Non-secure disposal	1	data left in locked drawer in a cabinet in building sold by the Council
Other	5	2 x post sent to officer without Service included in the address and received by incorrect officer 2 x internal mail sent to Social Services without being marked official sensitive 1 x issue relating to social media
Category 2	**Number**	**Details**
Other	1	Temporary worker e-mailed work to home computer – ICO closed the case following initial consideration as the Council had taken appropriate action

Appendix B

The number of Freedom of Information Act Internal Reviews undertaken during 2017-2018 and the number of complaints to the ICO processed by the Council during the period.

Three stage process:-

Stage 1: FOI requests received and responded to.

Stage 2: Internal Review - if requestors are unhappy with the original response they may request an Internal Review (appeal) which must be undertaken by the Council's Corporate Information Governance Manager.

Stage 3: Information Commissioner (ICO) - if the original response is upheld at the Internal Review stage then they may take the matter to the ICO who will assess whether or not to investigate.

Freedom of Information Act requests for Internal Review (17/18)
In 2017/18, the Council received/answered 7527 questions under the Freedom of Information Act 2000. Of these only 5 resulted in requests for an Internal Review and in all cases the original responses were confirmed at Internal Review.
Freedom of Information Act Appeals to the ICO (17/18)
3 appeals were lodged with the ICO in this period. 1 - as a result of dissatisfaction with the Internal Review but the Council's original decision and Internal Review was upheld by the ICO. 1 – original request not responded to within timescale and was reported to the ICO. Council then had 10 working days to respond and this was done. 1 – appeal against refusal – withdrawn by complainant

Appendix C

Information about the number of data protection complaints made to the Council during 2017 – 2018 by individuals about its processing of their personal information.

Data Protection Act Complaints to the Council (17/18)
2 DPA complaints were made and investigated: 1 related to inadvertent disclosure of an email address – explanation and apology provided and informed of right of appeal. Nothing further known. 1 related to statements provided in relation to a civil court case – not upheld but complainant informed of right of appeal. Nothing further known.

Appendix D

Information about the number of data protection Subject Access Requests and the Council's compliance during 2017 - 2018.

Subject Access Requests and compliance (17/18)
22 SARs were received/answered
91% responses sent within the 40 day deadline (20 of the 22)