CYNGOR SIR YNYS MÔN / ISLE OF ANGLESEY COUNTY COUNCIL	
Meeting:	Governance and Audit Committee
Date:	8 February 2024
Title of Report:	Information Governance – Senior Information Risk Owner's Annual Report for 1st April 2022 – 31 March 2023
Purpose of the Report:	To Inform Members as to the Level of Compliance and Risk
Report by:	SIRO/Monitoring Officer Ext 2586 lynnball@ynysmon.llyw.cymru
Contact Officer:	SIRO/Monitoring Officer Ext 2586 lynnball@ynysmon.llyw.cymru

Purpose of this report

To provide key Information Governance (IG) issues for the period 1 April 2022 to 31 March 2023 and to summarise current IG risks.

1.0 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 2-8.

2.0 Senior Information Risk Owner's Statement

As SIRO I make the following recommendations:

i. the SIRO's report be accepted as an accurate reflection of IG issues in the Council for the relevant period;

ii. the Committee supports the SIRO in asking the Leadership Team to:-

(i) assess the Council's use of CCTV and its use, if any, of drone technology;

(ii) undertake an assessment of the data protection risks of partnership working, together with the cyber threat of contract management / procurement in the Council;

(iii) put in place appropriate arrangements to ensure that the Leadership Team is adequately sighted on the Council's cyber threats and mitigations

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

Data security incidents (22/23): 22 incidents

Level 0 – Level 1 (near miss or confirmed as a data security incident but **no** need to report to ICO and other regulators) = 21

Level 2 incidents (data security incident that **must** be reported to the ICO because of the risk presented by the incident = 1

Category Level 0 -1	**Number**
Disclosed in error	19
Lost data/ hardware	2
Unauthorised disclosure	0
Lost in transit	0
Other	0
Category 2	**Number**
Disclosed in error	0
Unauthorised disclosure	1
Technical failing	0
Other	0

Appendix 2. Agreed actions following data security incidents.

Action
Following an unauthorised disclosure when a photograph of a service user's confidential hospital letter was attached to an e-mail to an internal user Group. Three actions were identified and agreed in order to reduce the likelihood of a similar incident.

Appendix 3. Data breaches reported to the ICO.

1.0 A data breach was reported to the ICO in September 2022 following an unauthorised disclosure of a service user's confidential hospital letter. The ICO required no further action from the Council.

2.0 Following an investigatory process of over 20 months, the ICO provided feedback on a data breach that was initially reported in June 2021, involving the security of servers of 5 secondary schools. The breach was initially

detected by the Council when several outbound suspicious SMTP traffic flows (simple mail transfer protocol i.e. suspicious email activity) were identified from the secondary school's network. The servers and IT infrastructure was developed and maintained by a third party on behalf of the schools.

Unable to identify the cause of the suspicious activity, the decision was made to quarantine the virtual machines and any other potentially compromised networked devices and user accounts for the five secondary schools. A report to the ICO was made by the Council's DPO, later by the schools as the responsible data controllers. An investigation was carried out by the NCC Group, the leading UK cyber threat advisory organisation and an Incident Management Team was set up by the Council.

During the investigation it was found that the systems contained several known vulnerabilities, leaving them vulnerable to attacks. The NCC Group discovered several issues which relate to the overall poor security posture of the estate. It was discovered that key systems were deployed on unsupported end of life, legacy Operating Systems. The NCC Group also noted that the effectiveness of their investigation was significantly affected due to the lack of logging across the estate.

Whilst the investigation's conclusions were that whilst there was no evidence of compromise, several key compliance elements were missing and the ICO supported the development plan created and implemented by the Council to ensure that the schools were able to process personal data securely and in a way that complied with UK data protection law.

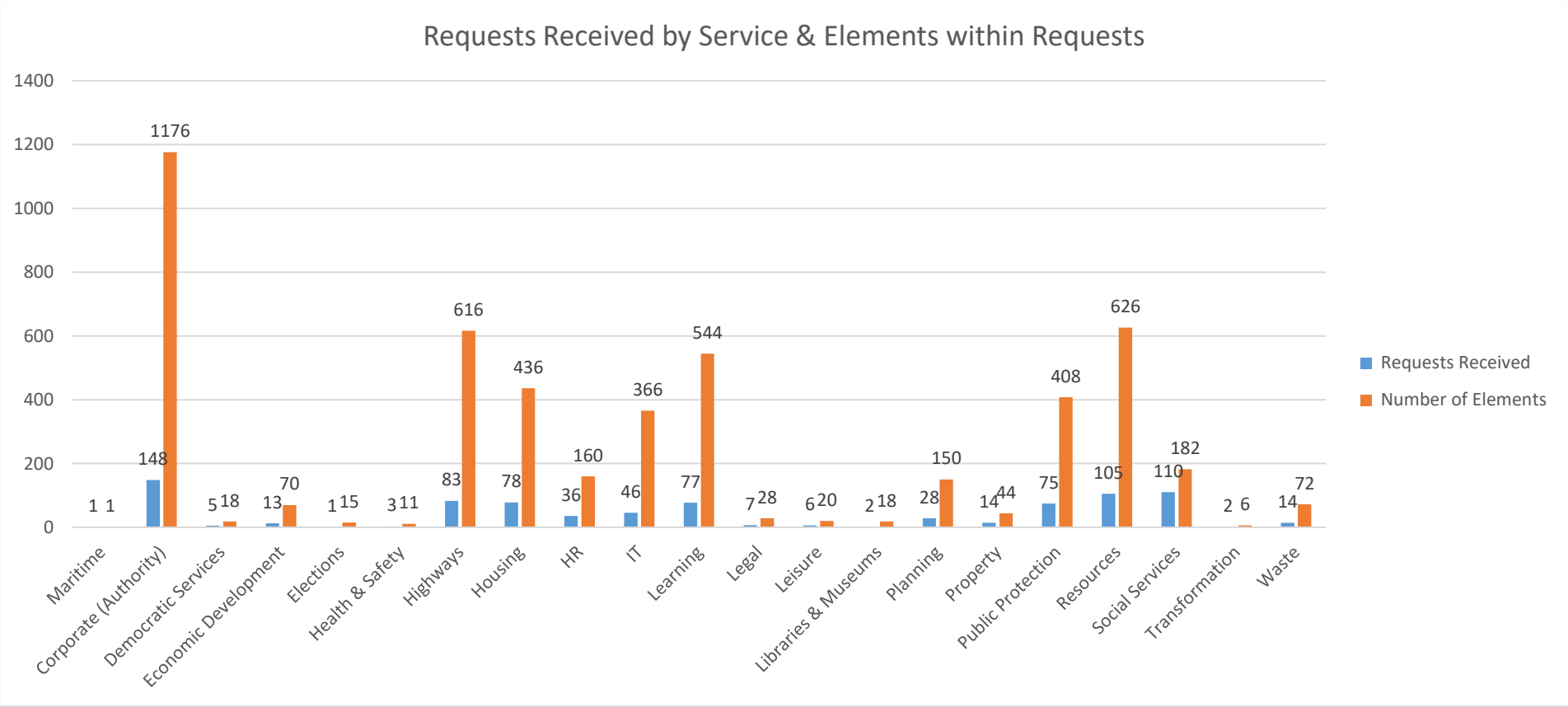
The remediation that the Council implemented to the digital security of the schools systems and the data protection governance of the schools made a significant and immediate improvement to security and compliance and this, more than any other factor, resulted in the ICO taking no further action against the Council and schools. The data protection elements of this work remain ongoing in the Learning Service.

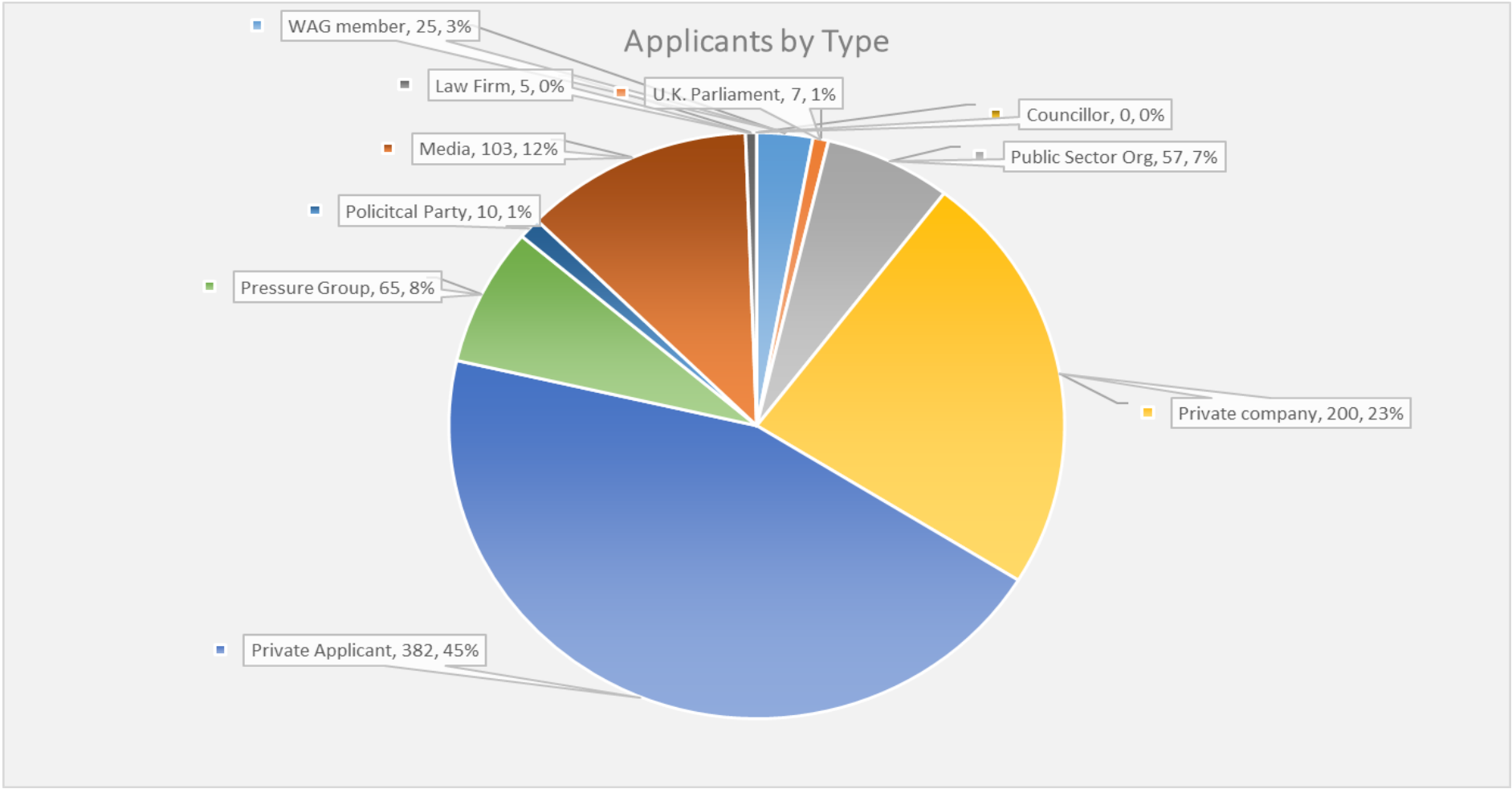
Appendix 4. Information about Freedom of Information Act 2000 requests and complaints

Freedom of Information Act 2000 requests and Internal Reviews

During 1 April 2022 and 31 March 2023 the Council received 854 requests for information comprising 4967 individual elements.

Total Number of Requests Received	854
Total Number of Elements Received	4967





Of the 854 requests, 2 resulted in an Internal Review of the responses supplied by the Council. The outcomes are as follows:

- In both cases the original decision was upheld;

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

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

Data Protection Act Complaints to the Council
3 DPA complaints were received, 1 related to a request to **rectify 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 **all cases were not upheld**. The Council's processing was considered to be lawful and the data subject rights were not compromised.

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

Subject Access Requests and compliance
24 SARs were received with 50% (12) responses sent within the appropriate statutory deadline, i.e. within 1 month with 1 late responses 10 SARs are on hold. 2 SARs were designated as being complex requests and the statutory time limit was extended to three months. 1 of these were responded within the extended timescale and the other was still open with Social Services.

Appendix 7. Information about Regulatory Oversight

7.1. The Investigatory Powers Commissioner's Office

The Investigatory Powers Commissioner's Office (IPCO) oversees the conduct of covert surveillance and covert human intelligence sources by public authorities in accordance with the Police Act 1997, the Protection of Freedoms Act 2012 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 authorisation by senior officers who have to be satisfied that the surveillance is necessary and proportionate; the authorisation must then be judicially approved.

The Council's SIRO is also Senior Responsible Officer (SRO) for the Council's RIPA compliance.

The Council's Policy was reviewed and refreshed during the period of this report. However, no authorisations were made during the period of this report.

7.2 Information Commissioner

The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 2018 and the UK GDPR; the Freedom of Information Act 2000; the Privacy and Electronic Communications Regulations; the Environmental Information Regulations; the Re-use of Public Sector Information Regulations; the INSPIRE Regulations. The 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.

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.
Nil.

Freedom of Information Act Appeals to the ICO
Nil.

7.3. Surveillance Camera Commissioner

The office of Biometrics and Surveillance Camera Commissioner (BSCC) 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 Biometrics and Surveillance Camera Commissioner has assumed the responsibilities of the now defunct Surveillance Camera Commissioner. In 2019 the Surveillance Camera Commissioner wrote to UK local authority Chief Executives requesting that the DPOs were appointed to the role of CCTV Senior Responsible Owner.

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. Whilst advice regarding compliance and governance is provided to services by the DPO at their request and training has been arranged for managers, there is no compulsion on Services to proactively communicate information about their CCTV systems to the DPO or the CCTV Single Point of Contact (SPOC). Attempts to survey the Council's CCTV systems since 2019 have elicited mixed responses of questionable value. It is acknowledged that the Council's use of CCTV is less intrusive than other councils who operate town centre systems, but the risks exist, particularly because of the interaction with the Police, which could lead to governance challenges.

It is my opinion that the corporate knowledge about the Services' use of CCTV systems is patchy and not comprehensive. Consequently, it is likely that the Council does not have adequate oversight of its systems and cannot identify compliance and training gaps. Ownership of the risks of CCTV must belong to the Council's Senior Leadership Team.

I am aware that Services are considering using Drone technologies and body worn CCTV systems and whilst this technology offers great potential for effective service delivery, the increased governance issues and compliance risks that accompany this technology calls for senior oversight of CCTV compliance and governance through delegation to the SIRO to support the operational role of the CCTV SPOC.

As SIRO, I have identified the need for a survey of the Council's use of CCTV, broken down on a service by service basis.