ISLE OF ANGLESEY COUNTY COUNCIL	
Report to:	Governance and Audit Committee
Date:	19 September 2024
Subject:	Information Governance – Annual Report of Senior Information Risk Owner (SIRO) for the period 1 April 2023 – 31 March 2024.
Head of Service:	Lynn Ball Director of Function (Council Business) / Monitoring Officer / SIRO.
Report Author:	Lynn Ball Director of Function (Council Business) / Monitoring Officer / SIRO
Nature and Reason for Reporting: To provide the Senior Information Risk Owner's analysis of the key Information Governance (IG) issues for the period 1 April 2023 to 31 March 2024 and to summarise current information risks and mitigations.	

1.0 Introduction

It is good practice within the public sector to have a data security accountability framework including the designation of a Senior Information Risk Owner (SIRO). The SIRO is required to provide assurance of practice, progress, and developments in information risk management.

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

It is my view that the greater part of the Council's information risk relates to digital data sets and cyber threats. As SIRO, I recognise that the direction of travel in terms of good practice, which is aimed at helping organisations to achieve and demonstrate an appropriate level of cyber resilience, will ensure that the role of SIRO will be closely aligned with managing cyber threat and evidencing good practice.

It is my intention to revise the focus of my report for the period 2024-2025 to refer to this risk and the effectiveness of the Council's controls and mitigations to manage this threat.

Therefore, I recommend that:

The SIRO and the Council's senior leaders are provided with regular updates on cyber risks and mitigations so that informed, strategic decisions relating to the constant cyber threat to the integrity and confidentiality of the Council's data assets can be made promptly and effectively.

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

Data security incidents (23/24): 13 incidents

Level 0 – Level 1 (near miss or confirmed as a data security incident but **no** need to report to ICO and other regulators) = **12**

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	12
Lost data/ hardware	0
Unauthorised disclosure	0
Lost in transit	0
Other	0
Category 2	**Number**
Disclosed in error	0
Unauthorised disclosure	0
Technical failing	0
Other	1

Appendix 2. Agreed actions following data security incidents.

Action
No formal actions were agreed during the period of this report.

Appendix 3. Data breaches reported to the ICO.

1.0 A data breach was reported to the ICO in July 2023. The report was made following the discovery that the Council's partners in an enterprise involving the processing of personal data, including special categories of personal data*, were processing it in a way that appeared to be contrary to the statutory obligations of the partners under data protection law.

The report was made independently of the Council's partners, in compliance with the statutory duty under Article 33(1) of the UK GDPR.

The incident was allocated to a case officer then escalated by the ICO for formal investigation. The ICO provided their report in November 2023 and found that the incident reported demonstrated that the processing breached Articles 28(2); 5(1)(a); and 6 of the UK GDPR.

The ICO decided not to proceed with enforcement action, a decision that was based on mitigations that had been implemented by the partnership following the report.

* *Personal data revealing race or ethnicity, political views, religion or philosophical belief, trade union membership, processing genetic data or biometric data to identify a natural person, health data or data relating to sexual life or sexual bias*.

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

4.1 Freedom of Information Act 2000 requests
During 1 April 2023 and 31 March 2024 the Council received 1002 requests for information comprising 6329 individual elements.

i.	**Total Number of Requests Received**	1002
ii.	**Total Number of Elements Received**	6329
iii.	**Percentage of requests responded to within statutory timescale**	80.1%
iv.	**Total number of requests for an Internal Review in accordance with the Statutory Code of Practice**	10

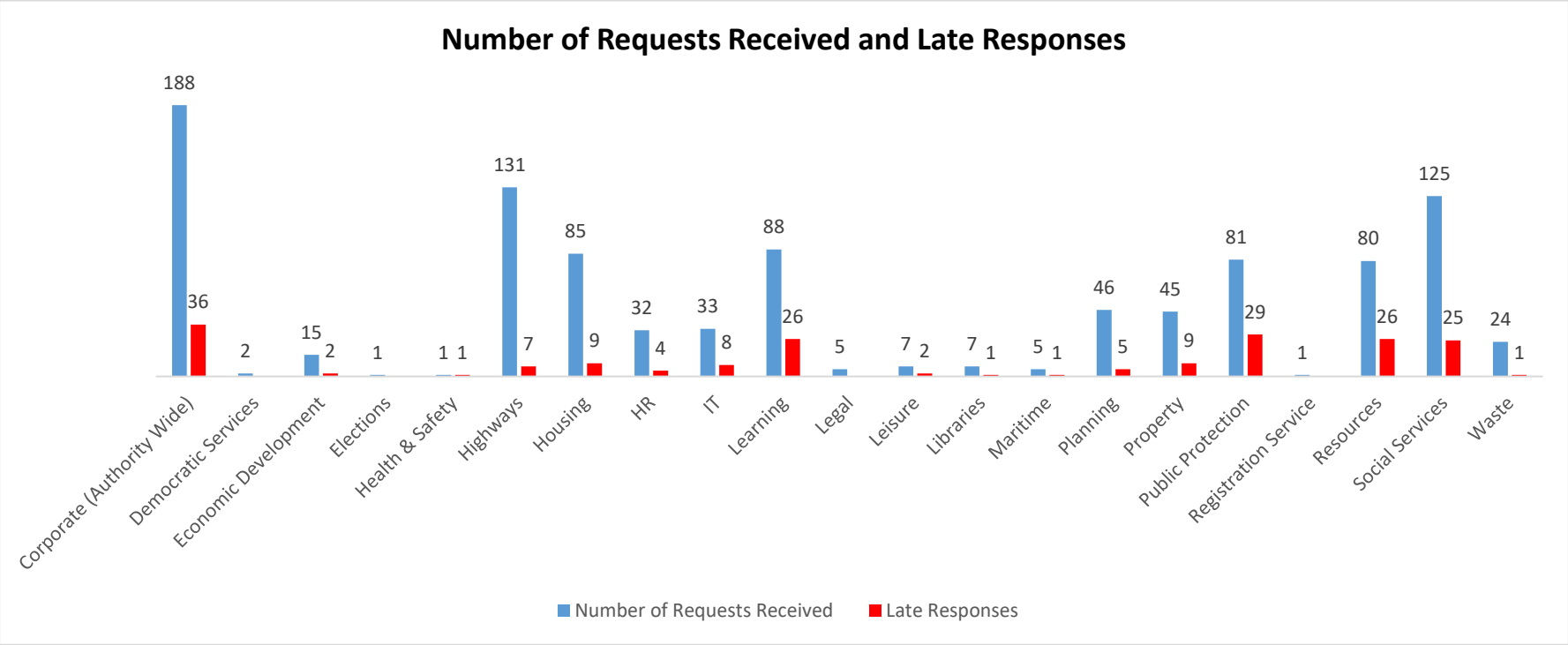
Exemptions used and frequency:

Section 12 (above the appropriate limit) on 3 occasions.
Section 14 (repeated requests) on 1 occasion.
Section 21 (accessible by other means) on 8 occasions.
Section 30 (investigations & proceedings) on 2 occasions.
Section 40 (personal data) on 1 occasion.
Section 41 (information provided in confidence) on 22 occasions.

4.2 Freedom of Information Act 2000 requests and late responses.

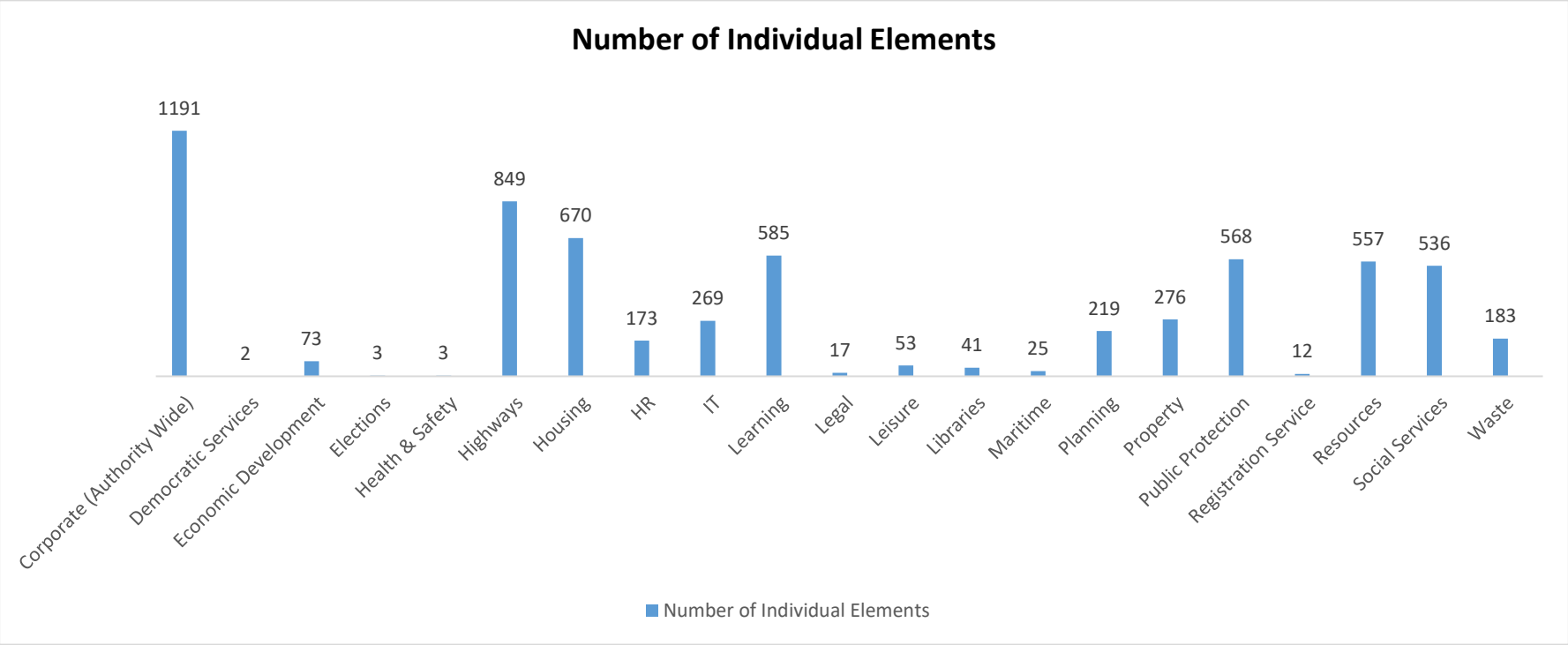
During 1 April 2023 and 31 March 2024 the Council received 1002 requests for information.

There were192 late responses. The number of requests received (shown in blue), and the number of late responses (shown in red) are presented below.



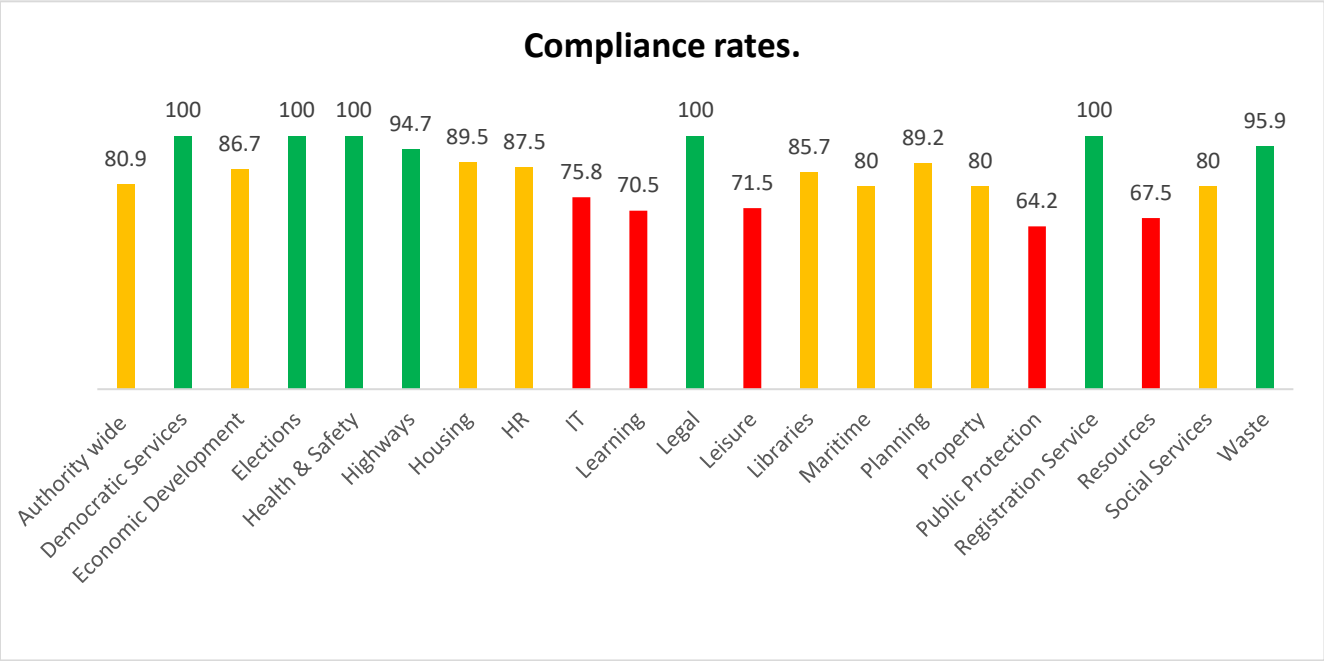
4.3 Freedom of Information Act 2000 requests.

During the period 1 April 2023 to 31 March 2024, the Council received 1002 requests, which contained **6329 individual elements** or questions. Information about the allocation of these elements is provided below.



4.4 Compliance broken down by service areas.

The ICO advises that public authorities should respond to 90% of FOIA requests within 20 working days. During the year 1 April 2023 - 31 March 2024, the Council's corporate average compliance was 80.1%. Whilst there are pockets of compliance with the ICO standard of good practice, it is evident that there are performance challenges being demonstrated in some services. The information presented below should be compared with the information in 4.3 (above) for a comprehensive view.



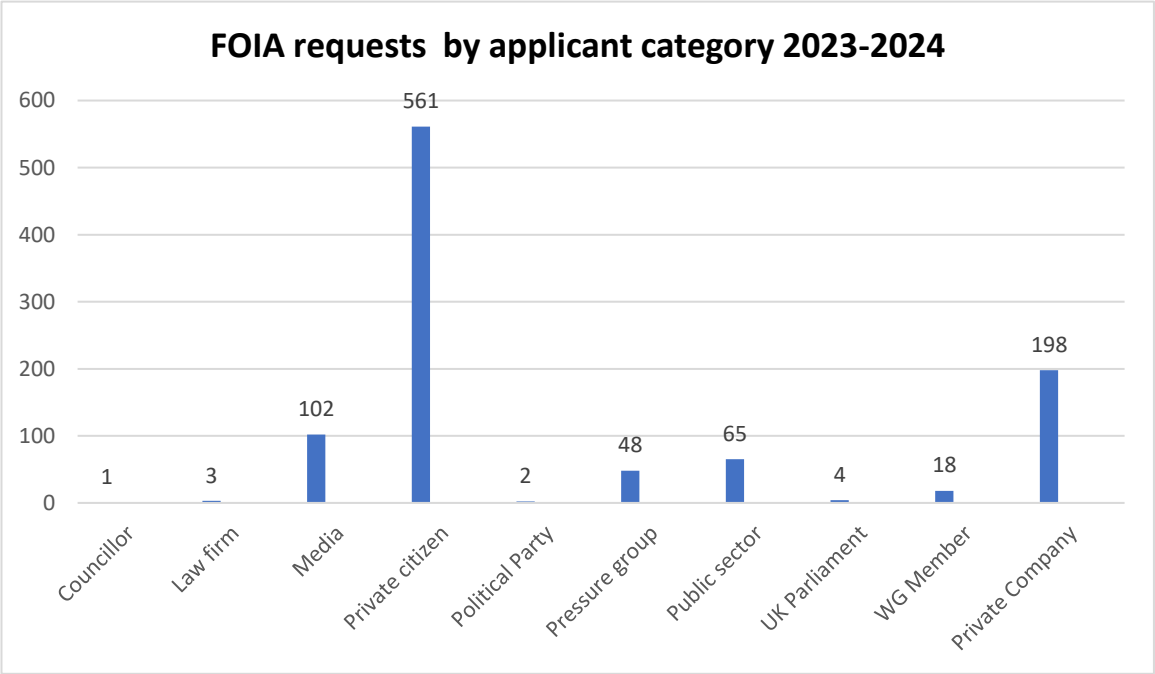
Key

Meets or exceeds ICO good practice standard of 90%.
Meets or exceeds corporate average for 2023-2024
Below corporate average for 2023-2024

4.5 Freedom of Information Act 2000 requests.

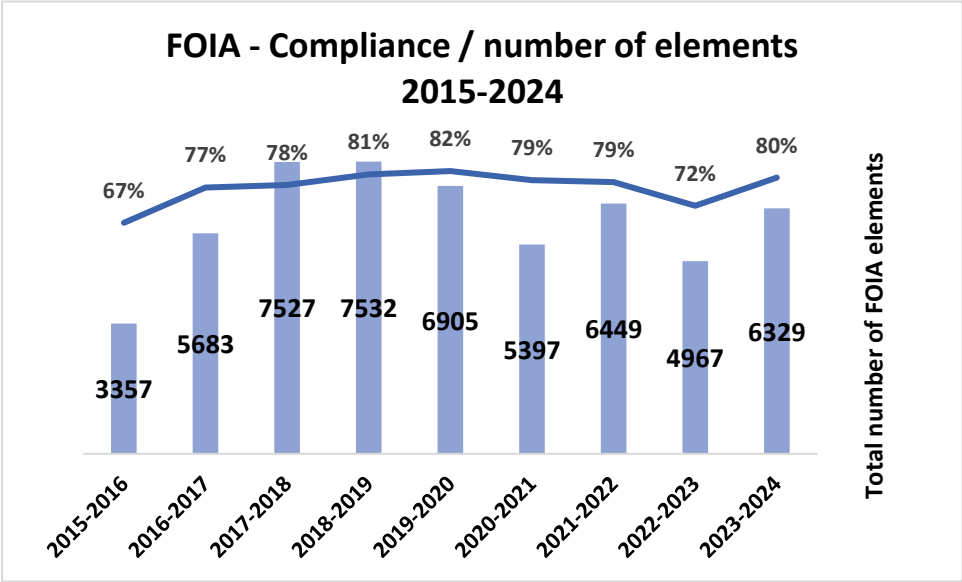
The Council categorises requests based on types of applicants that submit FOIA requests.

During the period of this report, it is apparent that majority of requests were submitted by private citizens in a personal, non-official or non-business capacity.



4.5 Comparative data on Freedom of Information Act 2000 requests and performance 2015-2024.

Over the past 9 years, the Council has received and processed 54,146 FOIA elements or questions. This equates to an average of 6016 FOIA elements per year. The average compliance rate (response within 20 working days) over this period is 68%. It is interesting to note that whilst the number of requests received dipped during the Pandemic, the Council's FOIA compliance rates did not diminish. However, the decreased number of FOIA elements processed and the dip in compliance evidenced during 2022-2023 is likely the result of staffing issues on the Council's processes during this time.



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
2 DPA complaints were received, 1 complaint related to a request to **erase personal data** 1 complaint related to an **objection** to the Council's processing of personal data Following investigation by the Data Protection Officer, it was found that**:** **1 case was upheld**. The Council's processing had compromised an individual's rights; **1 case was not upheld**. The Council's processing had not compromised the individual's data protection rights.

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

Subject Access Requests and compliance
I am only able to report on the number of data subject access requests that have been received by the DPO and processed by Social Services. 49 SARs were received during the period with 50% (19) responses sent within the appropriate statutory deadline, i.e. within 1 month with 1 late response. A total of 29 requests are on hold pending confirmation or clarification regarding the identity of the applicants.

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.

As the Council's SIRO, I am also Senior Responsible Officer (SRO) for the Council's RIPA compliance. I can confirm that during the period of this report that:

i. The Council's arrangements for compliance with the legislation were inspected by IPCO and were deemed to be compliant. There were no recommendations for improvement and Sir Brian Levenson confirmed: "As such, your Council will not require further inspection...."

ii. 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.
Two complaints were investigated by the ICO, with one investigation running beyond the period of this report. In both cases, the ICO required no further action from the Council.

Freedom of Information Act Appeals to the ICO
Two decisions were appealed to the ICO during the period of this report: In one case, the decision of the ICO being that the Council ought to provide a substantive response to the request within 10 working days; The other case required the Council to consider the data protection elements of the FOIA complaint separately, but no further steps were required.

7.3. Surveillance Camera Commissioner

I have nothing to report for this period.

Appendix 8. Update on resolutions of the Committee in respect of the 2022-2023 report.

In February 2024, I presented my annual report for the period 2022-2023 and made the following recommendations, which the Committee resolved to accept. These are shown, below, with an update (to 31 March 2024).

i. **assess the Council's use of CCTV and its use, of any, of drone technology.**
It has not been possible to undertake this assessment due to lack of capacity within the IT Service.

ii. **undertake an assessment of the data protection risks of partnership working, together with the cyber threat of contract management/procurement in the Council.**
The Head of Function (Resources) & S151 Officer advises that this issue will be addressed as part of the Council-wide STAR Procurement improvement programme, for which a workplan has been developed and agreed with STAR. This includes workstreams for the development and revision of the Procurement Strategy, the new Procurement Regulations and Contract Management, specifically: *PS2-6* – Development, agreement, and promotion of Procurement Strategy; *NPR1-3* – Implementation plan focusing on the four key areas of processes and policies, systems, people and transition. Areas to consider premarket engagement and supplier assessment along with governance documentation; *CON 1* – Contract Management roles and responsibilities to be agreed; *CON 2* – More detailed guidance and support to be developed; *TRA2* – More specific training sessions on key areas where need to mitigate risks such as evaluation, commercial awareness, contract management and risk in procurement, including cyber risk.

iii. **put in place appropriate arrangements to ensure that the Leadership Team is adequately sighted on the Council's cyber threats and mitigations.**
It has not been possible to undertake this assessment owing to lack of capacity within the IT Service. However, this issue aligns closely with the Council's intention to adoption of the National Cyber Security Centre's Cyber Assurance Framework (CAF).