TITLE: INFORMATION GOVERNANCE ANNUAL REPORT

Committee: Audit Committee

Date: 16th July 2024

Author: Director Legal & Monitoring Officer (SIRO)

Report No: Z35

Contact Officer: Maggie Camp, Director Legal & Monitoring Officer
maggie.camp@eastcambs.gov.uk
01353 616277
Room 112, The Grange, Ely

1.0 ISSUE

1.1. To receive an overview of the Council's activity in respect of how it has discharged its responsibilities in matters relating to information governance during 2023/24.

2.0 RECOMMENDATION(S)

2.1. Members are requested to note the report.

3.0 BACKGROUND/OPTIONS

3.1. The Council has statutory obligations to meet as set out in legislation including dealing with Freedom of Information requests, Environmental Information Regulation requests, Subject Access requests, Data Protection requests and Data Breaches. The Information Commissioner's Office ("ICO") is the UK's supervisory authority set up to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals and monitors compliance with legislation.

3.2. This report provides a summary of the Council's performance during 2023/24 in responding to requests for information received under the legislation referred to above. It also reports on the management of data breaches and data protection training. More information is provided in each section.

3.3. Freedom of Information

The Freedom of Information Act 2000 and the Environmental Information Regulations 2004 impose an obligation on public authorities to provide public access to certain information held by them. On receipt of a valid request for information, the authority must comply with that request as required by the legislation, unless an exemption can be applied.

3.4. Anyone has a right to request information from a public authority. The Council's three separate duties when responding to these requests are:

- To tell the requester whether we hold any information falling within the scope of their request.
- To provide that information; and

- To respond to the request within twenty working days.

3.5. Statistics

Table 1: Number of FOI/EIR requests received

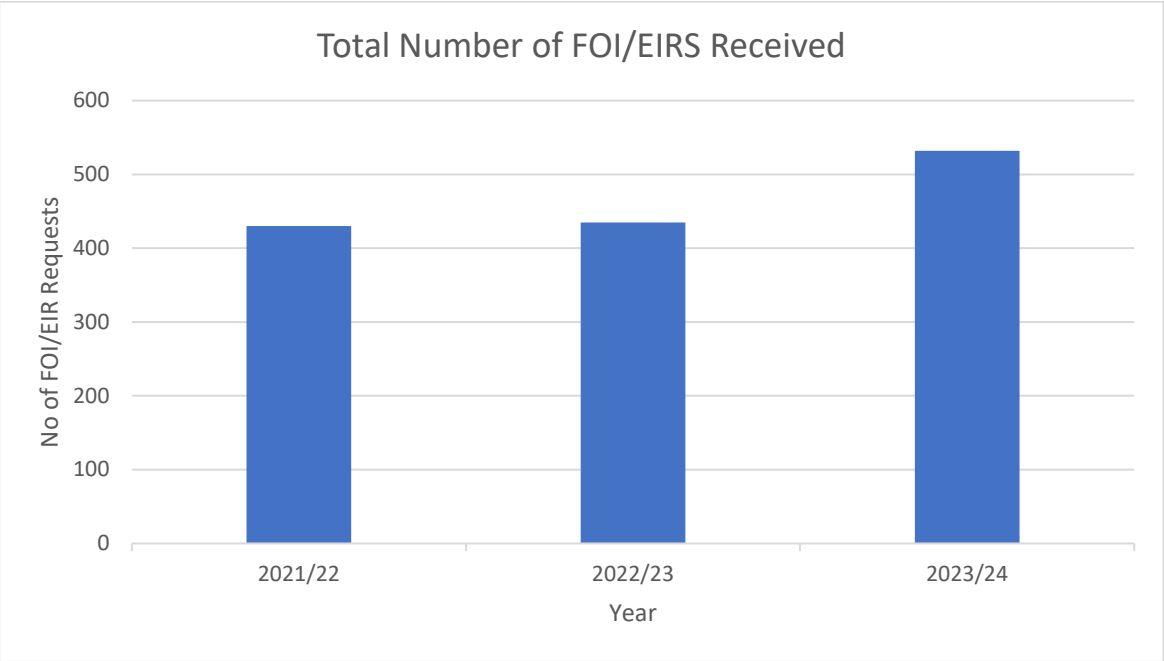
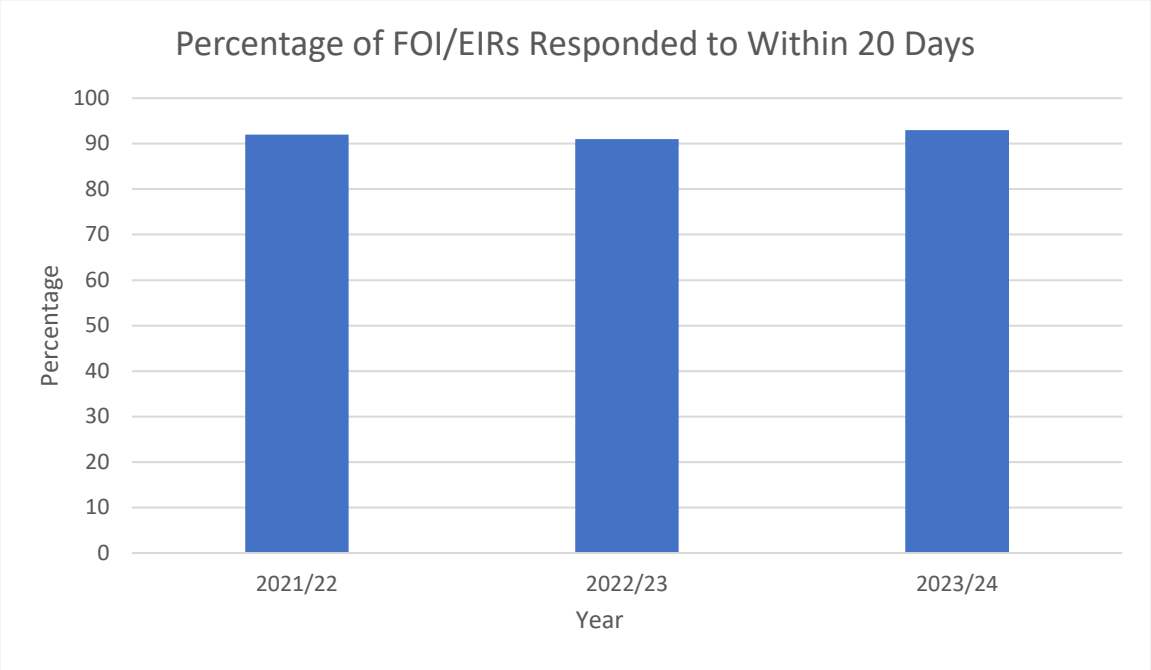


Table 2: Proportion of FOI/EIR requests completed within target time



3.6. The ICO consider a 90% response rate to be adequate; however, as can be noted above, the Council is consistently above this each year.

3.7. If a requester is unhappy with their FOI/EIR request, they can request an internal review. If they remain unhappy following an internal review, then the matter can be referred to the ICO.

3.8. In 2021/22, 5 internal reviews were requested, with one being escalated to the ICO. The ICO agreed with the Council's original decision.

3.9. In 2022/23, 4 internal reviews were requested, and none were escalated to the ICO.

3.10. In 2023/24, 5 internal reviews were requested, and none were escalated to the ICO.

3.11. The average officer time to respond to a FOI request is 1 hour and 36 minutes. All FOI responses that are answered by officers are sent back to the Information Officer for double checking and if requested, redacting, prior to being sent out to the requester. This procedure reduces the risk of releasing incorrect and/or personal data.

3.12. Data Subject Access Requests and Data Protection Requests

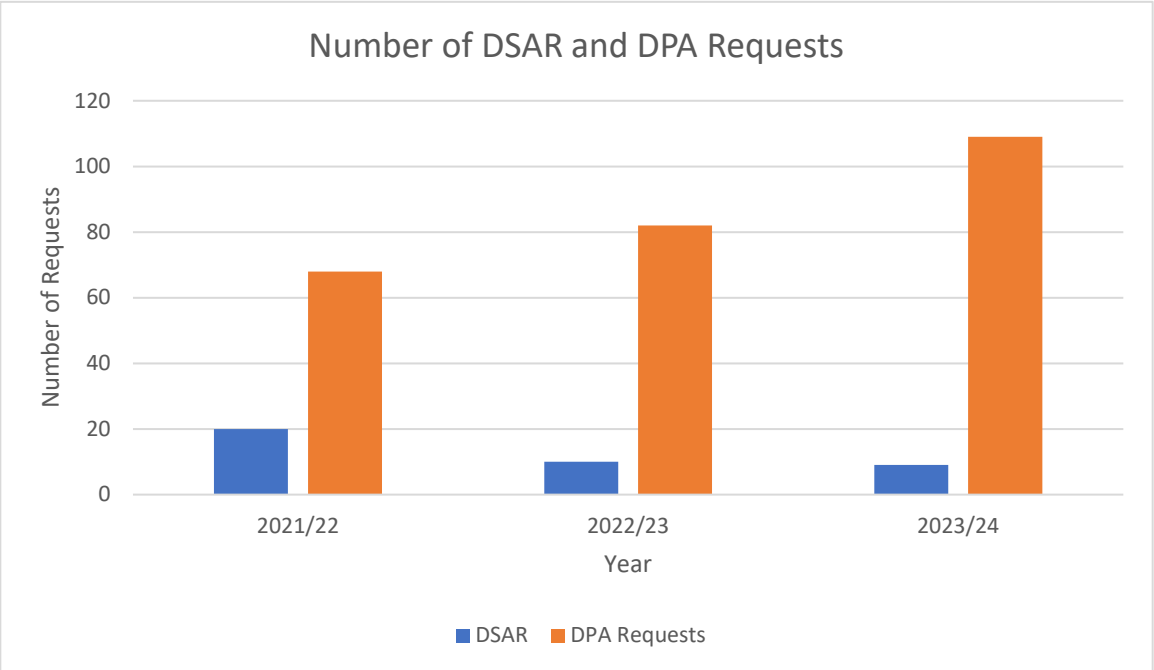
The UK General Data Protection Regulation ("UK GDPR") enables individuals the right to access any personal data an organisation holds on them. This is known as a Data Subject Access Request ("DSAR"). A Data Protection Request is a request from other public bodies, either internal or external, for personal data for investigation purposes.

3.13. DSAR's can be complex to process as they often involve multiple data subjects' personal data within each record. This means that detailed redaction has to take place to ensure that disclosure is accurate and does not inadvertently include other data subjects' personal data. Each request may include hundreds of records from multiple departments within the Council.

3.14. The Council also receives "one off" requests for personal information from third parties, including the police and other government agencies. The Information Officer maintains a register of these requests, which includes assessing whether the Council can lawfully disclose the information and logging exemptions relied on when personal data is shared with third parties.

3.15. Statistics

Table 3: Numbers of DSARs and DPA Requests received



3.16. Data Breaches

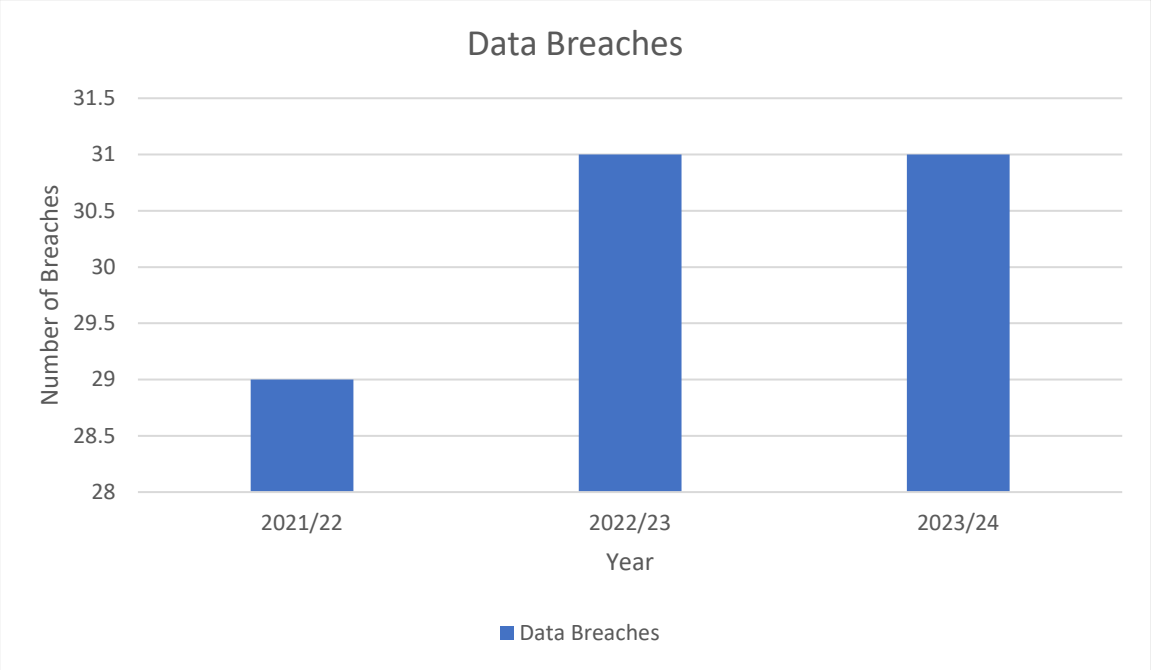
A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

3.17. The Information Officer assesses each breach to consider the likelihood and severity of the risk of rights and freedoms as a result of the breach. From this assessment, it is decided if the breach needs to be reported to the ICO. By law, the Council has 72 hours from time of notification of the breach to report breaches that meet the threshold to the ICO. In 2020, only one data breach was reported to the ICO and no further action was required by the ICO. There have been no further breaches which required notification to the ICO.

3.18. For each reported breach, recommendations are made to the relevant officer and Service Lead. The most common data breach is sending emails to the wrong party.

3.19. Statistics

Table 4: Number of Data Breaches



3.20. Data Protection Training

There is no requirement set out in the UK GDPR regarding Data Protection training for staff; however, Principle 7 of the UK GDPR states that "*Data Controllers (i.e. the Council) are responsible for the compliance with the principles and must demonstrate this to data subjects and the regulator*".

3.21. Data Protection training for all staff. The training is on a 2-year schedule, with full training in year 1 and refresher training in year 2. The Council has a 100% complete rate for staff for 2023/24.

3.22. Staff who do not have access to a computer in their role with the Council are provided with appropriate level training, i.e. via toolbox talks for ECSS and ECTC staff.

3.23. The Council decided not to make Data Protection training compulsory for Members. To date 5 Members have completed Data Protection training.

3.24. Transparency Code

The Council has statutory obligations to publish data as required by the Local Government Transparency Code 2014. Publishing under the Code gives the public access to numerous datasets of information covering a wide range of matters, for example from procurement to parking.

3.25. The data sets are updated regularly according to the Transparency Code on the Council's Open Data page on the Council's website, and these are updated either monthly, quarterly or annually.

4.0 ARGUMENTS/CONCLUSION(S)

4.1. The Information Governance Audit Report 2022/23 noted that the Council provides Members with information regarding Freedom of Information requests monthly.

4.2. However, to raise data protection awareness and to provide assurance to members that matters such as data breaches are managed, together with actions taken to mitigate similar breaches occurring, the recommendation was to develop an Annual Information Governance report to be presented to Members and the first report was presented to Audit Committee in October 2023. It was agreed at that meeting that an Information Governance Annual Report would be added to the forward agenda plan for the July Audit Committee going forward.

5.0 FINANCIAL IMPLICATIONS / EQUALITY IMPACT STATEMENT / CARBON IMPACT ASSESSMENT

5.1. There are no additional financial implications arising from this report.

5.2. Equality Impact Assessment (EIA) not required.

5.3. Carbon Impact Assessment (CIA) not required.

6.0 APPENDICES

None.

Background Documents:

East Cambridgeshire District Council Open Data page
https://www.eastcambs.gov.uk/notices/open-data