CORPORATE RESOURCES

OVERVIEW AND SCRUTINY COMMITTEE

17 April 2023

TITLE OF REPORT: **Annual Report – Information Governance**

REPORT OF: **Mike Barker, Strategic Director, Corporate Services and Governance**

Summary

The report provides an overview of Information Governance arrangements within the Council. Due to the focus of the Committee's business during the pandemic, it is 4 years since the Committee was last presented with a report regarding Information Governance matters, specifically Freedom of Information, and there have been significant changes in that time.

Background

1. Corporate Resources Overview and Scrutiny Committee requires confidence in the way in which the Council manages Information Governance as part of the performance management process.

2. This annual report will provide an update generally on Information Governance arrangements as well as data relating to Freedom of Information requests and data breaches.

Service update

3. In 2019, the Officer with long term responsibility for Information Governance left the organisation which led to an unsettled period with a temporary Data Protection Officer in post.

4. Two internal audit reports were undertaken during 2019/2020, one in respect of Information Governance and one regarding Data Protection. The outcome was satisfactory, however due to the limited resources available at that time, the recommendations were not fully implemented (there were no high priority recommendations).

5. In April 2020, Angela Simmons-Mather was appointed as Data Protection Officer for the Council and she undertook a review of the organisation's ability to meet data protection obligations and the management of Information Governance generally. There was weakness identified, particularly the lack of a dedicated team dealing with Information Governance matters.

6. In 2021 an internal audit of Information Governance took place and confirmed there were areas which needed improvement, finding that there were significant weaknesses overall in Information Governance. This audit consolidated the recommendations of the previous audits with one high priority, 5 medium priorities and 2 best practice recommendations. The recommendations are set out in Appendix 1.

7. To ensure priority could be given to the recommendations, resources were realigned to create the DPO Team in April 2022, dedicated to ensuring the Council is able to meet its Information Governance obligations. The team consists of the Council's Data Protection Officer, one data protection solicitor, a senior information governance officer and a senior business support officer.

Work undertaken by the DPO Team

8. There has been an enormous amount of work undertaken since the team was created 12 months ago. This is on top of the daily operational work that is undertaken by the team:
   (a) Data Breach procedure rewritten and published
   (b) Data Protection Impact Assessment – template document and procedure rewritten and published
   (c) Information Governance Framework drafted – awaiting Cabinet approval (25 April 2023)
   (d) Data Protection Policy drafted – awaiting Cabinet approval
   (e) Information Asset Register / Record of Processing Activity project (see below)
   (f) Creation of Corporate Data Protection Group (see below) – terms of reference drafted and agreed
   (g) Privacy Notice project – new Corporate Privacy Notice and template drafted

9. The largest undertaking has been the Information Asset Register / Record of Processing Activity project. This task was a high priority recommendation from the 2021 internal audit. It has been carried out in two phases across every team in the Council. The team have worked closely with each person completing the documentation and provided both written guidance and training sessions at the start of each phase.

10. The first stage was to create the Information Asset Register – this lists all personal and non-personal information held by the team. It is a simple way to help understand and manage each team's information assets and the risks to them. It is important to know, and fully understand, what information you hold in order to protect it.

11. The second stage was to distill the personal information into a Record of Processing Activity, which is a legal requirement (Art.30 UK GDPR) where personal information is processed. Importantly it sets out the lawful basis for processing personal data, allowing the Council to comply with its wider data protection obligations.

12. The project was started in May 2022 and is still to be completed. As it has involved every team in the Council, this has led to approximately 126 IARs and 126 RoPAs being required. The team has reviewed and provided feedback on each document. There are approximately 14 outstanding RoPAs before the project can brought to an end. In 12 months time they will be reviewed and updated.

13. A further recommendation of the internal audit was for the Information Rights Working Group to be reconvened. This group had stopped meeting during the pandemic. It was agreed that the group would be renamed as the Corporate Data Protection Group to more accurately reflect the work to be undertaken by its members.

14. The first meeting of the group took place on 1 February 2023. The attendees represent each service across the Council and are known as Information Asset Assistants (IAA). They will be tasked with a project at each meeting to ensure the Council is meeting its data protection obligations. At the meeting on 1 March 2023 the group was asked to review their Service's Privacy Notices, another recommendation of the internal audit. The DPO Team have created a new Corporate Privacy Notice and a new template for each Service to use to ensure a consistent approach for those individuals accessing the Council's Privacy Notices.

15. The next piece of work to be carried out will be reviewing each team's retention periods, the final recommendation of the internal audit to be undertaken. This will be a resource intensive piece of work as each team will need to consider each information asset they hold and how long they need to keep that information.

16. It is intended that there will be an annual, rolling programme of work to ensure documents, policies and procedures are regularly reviewed and updated. There will also be further projects, such as a review of CCTV across Council buildings and improving active publication of transparency data.

17. Despite the challenges of the last four years, the DPO Team is working well and has raised the profile of Information Governance across the Council, evidenced by teams actively seeking advice on data protection / IG when planning new projects.

Freedom of Information

Procedure

18. The procedure has three steps:

    (a) The first stage is to provide the information sought within the statutory timescale of 20 working days, unless there is an exemption to the disclosure as set out in the Freedom of Information Act 2000. There is an electronic tracking system in which to log requests. This tracking system provides a full audit trail of how the request has been handled and provides template response letters, which fulfill the statutory requirements of the Act. This first stage relies on the Information Champion within each service to prepare the response in line with provisions of the Act.

(b) The second stage requires the Council to have an internal review process so that, if a requester is dissatisfied, they have an avenue of complaint, which is separate from the corporate complaints procedure. The review stage involves the requester writing to request an independent review of the matter within 40 working days of receiving their initial response. The internal review, ordinarily, will be undertaken by the Strategic Director of Legal and Corporate Services and a formal response provided to the requestor within 20 working days.

(c) The third stage gives the requester a right of appeal to the Information Commissioner if he/she is still dissatisfied, following the internal review.

Data

19. The following data covers the period since the last FOI annual report:

Year	Number of requests	Percentage dealt with in the statutory timeframe
2020	1006	90.35% (909)
2021	1135	93.39% (1060)
2022	1162	90.79% (1055)
2023 (so far)	282	95.74% (270)

20. The number of internal reviews has steadily increased since 2017 when only 2 reviews were undertaken:

Year	Number of Requests
2020	11
2021	16
2022	14
2023 (so far)	5

21. The majority of internal reviews have upheld the position taken in the Council's initial response. A small number have upheld the decision "in part". Only one internal review provided for full disclosure of the information sought, with the reviewer disagreeing with the application of the exemption originally applied.

22. Where requestors have remained unhappy with the Council's response, it is open to them to make a formal complaint to the ICO:

Year	Number of Complaints to ICO	Outcome
2020	2	1 – required to disclose information 1 – agreed to disclose information
2021	1	1 – required to disclose partial information
2022	2	2 – no further action required
2023 (so far)	2	1 – no further action (1 decision awaited)

23. In 3 of the ICO complaints the Council was found to have provided the refusal notice or internal review outside of the statutory timescale although in making that determination, no further action was required of the Council. We do strive to provide all responses within the required timescales.

24. Requests for information vary considerably and are difficult to categorise. We receive regular requests around contracts, what hardware / software is used, when contracts are up for renewal and what our unit costs are. So far this year we have received a large number of requests around housing, bus lanes, road changes across the borough and climate change.

25. In the last 12 months, the following teams have received the most requests:

- Housing, Environment and Healthy Communities - 346
- Corporate Services and Governance - 200
- Resources and Digital - 197
- Economy, Innovation and Growth - 155
- Children's Social Care and Lifelong Learning - 139
- Integrated Adults and Social Care Services - 73
- Public Health and Wellbeing - 45

26. The Council is required to publish certain information, for example senior officers' salaries, and a transparency page is available on the Council's website so that members of the public can access the information covered by the Publication Scheme from a single access point. It has always been hoped that

proactively publishing information would reduce the number of FOI requests received, however there is little evidence to suggest that is the case.

Data Breaches

27. Following the redrafting of the data breach reporting procedure in early 2022, the need to report data breaches, following the procedure, was widely publicised across the Council, using the Employee Bulletin, the intranet carousel and the online data protection training course.

28. Officers are required to complete the data breach reporting form with as much detail about the breach as possible. The form must be completed as soon as the breach is discovered, as the Council has only 72 hours in which to report the matter to the ICO should that be required. It is therefore important to include all of the information sought in the form to allow the DPO Team to determine whether the matter needs to be reported.

29. The Council is required to keep a record of all data breaches:

Year	**Number of Data Breaches**
2020	30
2021	64
2022	98
2023 (so far)	39

30. Whilst the number of breaches has gone up, it is believed the increase in awareness around reporting data breaches over the last 2 years is responsible.

31. The criteria for reporting a data breach to the ICO is where the breach is likely to result in there being a risk of adversely affecting individuals' rights and freedoms. Breaches reported to the ICO:

Year	**Number of Data Breaches reported to ICO (percentage of overall total)**	**Outcome**
2020	2 (6.7%)	2 – No further action
2021	1 (1.6%)	Advice given – no further action
2022	5 (5.1%)	5 – No further action

2023 (so far)	2 (5.1%)	2 – No further action

32. Whilst it may appear that the increasing numbers are a concern, a cautious approach is taken to reporting matters to ensure the Council is being transparent with regards to data breaches. Where the Council has reported a data breach to the ICO, no action has been taken by the Regulator.

33. Reasons for reporting breaches include:
    - A generic email sent to 118 recipients using the CC rather than BCC function. The inclusion in the email group revealed personal data about the recipients.
    - A residential address included in a document where the individuals had asked for it to be removed.
    - Missing paper forms containing financial information.

34. The most common cause of data breaches is human error – using the wrong email address, attaching the wrong document, sending letters to the wrong property. Advice is always provided to the service when the DPO Team respond to data breaches, usually it is to reinforce the need to be vigilant when handling personal data. More detailed advice and training can be provided depending upon the nature of the breach.

35. All staff are required to undertake annual data protection training which is provided via the Learning Hub.

Recommendation

The Corporate Resources Overview and Scrutiny Committee is asked to:

a) note the information in the annual report, and

b) satisfy themselves that the Freedom of Information and data breach procedures are operating satisfactorily.

Annual Report – Information Governance **APPENDIX 1**

High Priority	1
Medium Priority	5
Best Practice	2

High

Records of Processing Activity

Records of Processing Activity should be produced or updated as required, with an annual review carried out as a minimum by all Council Services in line with the GDPR and Data Protection Act requirements.

Medium

Information Governance Management Framework

Management should ensure that an Information Governance Management Framework is implemented that clearly outlines accountability structures, governance processes and includes all required documented policies and procedures, including a Data Protection Policy document. The framework should be formally approved and reviewed annually and then updated on the intranet.

Key Person Dependency

The Council should ensure that there is a Deputy Data Protection Officer in place to eliminate the key person dependency risk and to enable both strategic and operational duties to be carried out timely and effectively to ensure the Council adheres to regulatory requirements.

Privacy Notices

Management should ensure that all Council Services that collect, use and share personal information, outline in a Service specific Privacy Notice the legal basis for processing personal data; retention periods; and who the information may be shared with.

Data Retention

Services should be reminded to review and cleanse as required the personal data that is held within systems and databases on an annual basis as a minimum to ensure that information is not used beyond relevant retention periods.

Data Protection Impact Assessments (DPIAs)

An updated training presentation or brief for management teams should be developed and circulated to ensure that the completion of DPIAs is fully embedded for data processing considered high risk to individuals, and for major projects that require processing of personal data in line with the GDPR guidance.

Best Practice

Information Rights Working Group

The Information Rights Working Group should be reconvened, and a schedule of meetings arranged to review the data that is held by Council Services and to identify any gaps in compliance.

Operational Risk Register

Management should ensure that all specific risks associated with Information Governance and Data Protection are identified and recorded in the Council's Operational Risk Register, and that effective controls are implemented to mitigate the risks. Risk management should be an ongoing process. An annual review of the Operational Risk Register should be carried out as a minimum.

Contact: Angela Simmons-Mather **EXT:** 2110