Gateshead Council

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

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

Summary
The report provides an overview of Information Governance arrangements within the Council and the work of the Information Governance Team in the last 12 months.

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 provides an update on Information Governance arrangements alongside data relating to Freedom of Information requests and data breaches.

Service update

3. 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.

4. To ensure priority could be given to the recommendations, resources were realigned to create the Information Governance Team in April 2022, dedicated to ensuring the Council is able to meet its Information Governance obligations.

5. In 2023, Natalie Baldwin was appointed as Data Protection Officer for the Council, taking over from Angela Simmons Mather. Hannah Hales was appointed as the Deputy Data Protection Officer. The Information Governance team now consists of –

   - the Council's Data Protection Officer
   - the Deputy Data Protection Officer
   - a Senior Business Support Officer
   - an Information Rights Officer; and
   - a Subject Access Request Officer

6.   The team can also draw some limited support from the newly created role of the Governance Support Officer; and is in the process of recruiting an Information Governance & Complaints Assistant. The team is managed by the Governance Manager, Tim Briton.

Work undertaken by the Team

7.   There has been an enormous amount of work undertaken by the team in the last 12 months in addition to daily operational work. This includes:
  (a) Data Breach procedure reviewed, updated and published
  (b) Data Protection Impact Assessment – template document and procedure reviewed, updated and published, including introducing a new DPIA referencing system and new DPIA forms for specific circumstances such as Teams / Share point requests.
  (c) Continuing the Information Asset Register / Record of Processing Activity project (see below)
  (d) Continuance of the Corporate Data Protection Group (see below)
  (e) Commencement of the Retentions project (see below)
  (f) Completion of the Privacy Notice review project
  (g) Trial of switching-off 'autocomplete' in Outlook

8.   The Information Asset Register / Record of Processing Activity project as a high priority recommendation from the 2021 internal audit. It has involved the team liaising directly with every service in the Council and relies up on services completing the template documentation, with help from the team where required. The project is near completion, with only two services still to complete their documentation. An escalation process has been developed and implemented by the team to ensure that the Service Director for those remaining services who have not completed their documentation are now involved so that the project can be brought to completion.

9.   A further recommendation of the internal audit was for the Information Rights Working Group to be reconvened. This was renamed the Corporate Data Protection Group and the first meeting of the group took place on 1 February 2023, with the group convening monthly from this date. At the last meeting in February 2024, it was agreed that meetings will take place every 6 weeks rather than every month going forward, and new terms of reference were agreed.

10.   The attendees of the group represent each service across the Council and are known as Information Asset Assistants (IAA). The meetings allow the team to cascade important messages throughout the council via the IAAs and, where necessary, allow the team to task the IAAs with projects or tasks in their own service to ensure the Council continues to meet its data protection obligations.

11.   The team have led on the trial switching-off of 'autocomplete' within Outlook. The trial has now reached its review point and the team are currently reviewing the impact that this has had on lowering the number of email-related data breaches across the Council.

12. In the last 12 months, the largest undertaking for the team has been in relation to the final recommendation of the 2021 internal audit; reviewing the Council's retention periods. This has been a very resource-intensive piece of work as each team within the Council has needed to work with the Information Governance team to consider each information asset they hold and how long they need to keep that information to ensure retention periods are acceptable and documented.

13. This work has also led to various other record management related projects, such as the work completed on introducing 'autodelete' within Outlook and work carried out to determine which information is stored in the Council's GOSS and CEM systems.

14. These additional projects have delayed the completion of the overall retentions project as it has not been possible to implement retention periods until these additional projects have been completed. It is envisaged that the team will be able to develop an overarching corporate retentions policy by the end of September 2024.

15. It is intended that there will be an annual, rolling program 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.

16. Despite further changes to the structure of the team resulting in less resources in the team, the team is continuing to work well and raise 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

Summary of Procedure

17. The procedure has three stages:

> (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 Corporate Services & Governance 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 they are still dissatisfied, following the internal review.

Data

18. 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%
2021	1135	93.39%
2022	1162	90.79%
2023	1277	91.00%
2024 (so far)	334	

19. The number of internal reviews has remained steady since 2021;

Year	Number of Requests
2020	11
2021	16
2022	14
2023	16
2024 (so far)	4

20. 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".

21. 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	3	2 – no further action 1 – partially upheld
2024 (so far)	0	

22. 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.

23. 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

24. 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 IG Team to determine whether the matter needs to be reported.

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

Year	Number of Data Breaches
2020	30
2021	64
2022	98
2023	157

2024 (so far)	55

26. From analysis, the increase in reported data breaches is believed to be a result of awareness methods implemented by the Corporate Data Protection Group and direct work with services from the Information Governance Team. Stronger reporting leads to a more accurate picture of data breaches, allowing the development of more precise mitigations to data breach risks.

27. The criteria for reporting a data breach to the ICO is where the breach is likely to result in 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	15 (9.55%)	15 – No further action
2024 (so far)	6 (10.91%)	3 – No further action 3 – awaiting outcome

28. 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.

29. Breaches reported to the ICO in 2023 included:
    - Test data on the Councils GOSS system accidentally being made 'live' and visible on certain council operated websites.
    - Social work and / or Occupational Health data being posted to an out of date address.

30. 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 IG 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.

31. As a result of advice from the Information Governance Team and the ICO, the Council trialed switching off 'autocomplete' in Outlook to determine whether this reduced the number of the email related data breaches. The Information Governance Team are currently reviewing the results of the trial.

32. 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.