

Committee Name and Date of Committee Meeting

Audit Committee – 24 September 2025

Report Title

Information Governance Annual Report 2025/26

Is this a Key Decision and has it been included on the Forward Plan?

No, but it has been included on the Forward Plan

Strategic Director Approving Submission of the Report

Judith Badger, Strategic Director of Finance and Customer Services

Report Author(s)

Luke Sayers, Service Director- Customer, Information and Digital Services

luke.sayers@rotherham.gov.uk

Sam Ulyatt, Service Manager - Information Management

sam.ulyatt@rotherham.gov.uk

Ward(s) Affected

Borough-Wide

Report Summary

This report is an annual report on the Council's compliance with Data Protection and Freedom of Information legislation.

Recommendations

The Audit Committee is asked to:-

1. Note the production of the Data Protection and FOI Annual Report.
2. Note that it is a requirement that the Council continues its maintenance of its Information Governance practices and processes in compliance with legislation.
3. Note that this report will be published online to meet the Council's obligation to annually publish its FOI performance statistics.

List of Appendices Included

Appendix 1 FOI & RoAR Statistics

Appendix 2 Data Breaches

Background Papers

Information Commissioner's Office

<https://ico.org.uk/>

Consideration by any other Council Committee, Scrutiny or Advisory Panel
No

Council Approval Required
No

Exempt from the Press and Public
No

Error! Reference source not found.

1. Background

- 1.1 This report is an annual report on the Council's compliance with Data Protection legislation and the Freedom of Information Act 2000 (which for the purpose of this report includes the Environmental Information Regulations 2004).
- 1.2 The Data Protection Act 2018 (DPA) is the UK's implementation of the General Data Protection Regulation (GDPR).
- 1.3 The DPA makes it a legal requirement for organisations to adhere to the 'data protection principles'. Organisations must make sure that information is:
 - 1.3.1 Used fairly, lawfully and transparently;
 - 1.3.2 Used for specified, explicit purposes;
 - 1.3.3 Used in a way that is adequate, relevant and limited to only what is necessary;
 - 1.3.4 Accurate and, where necessary, kept up to date;
 - 1.3.5 Kept for no longer than is necessary; and
 - 1.3.6 Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.
- 1.4 The Act also provides stronger legal protection for more sensitive personal information.
- 1.5 The Freedom of Information Act 2000 (FOI) provides public access to information held by public authorities. It does this in two ways:
 - 1.5.1 Public authorities are obliged to publish certain information about their activities; and
 - 1.5.2 Members of the public are entitled to request information from public authorities.
- 1.6 The FOI Act covers **any recorded** information that is held by a public authority (or by a third party on behalf of the Council).
- 1.7 The Information Commissioner's Office is the UK's independent body set up to uphold information rights and it is responsible for enforcement of the rights and responsibilities set out in the DPA and FOI.
- 1.8 It is obligatory for the Council to undertake an annual registration with the ICO, with the Council's unique reference number being Z5759798 and available on the ICO's registration pages: [Rotherham Metropolitan Borough Council | ICO](#)
- 1.9 Monitoring of the Council's compliance with DPA and FOI is carried out by the Corporate Information Governance Group (CIGG) and is a standing agenda on the Service Directors' Group attended by the Council's Senior Information Risk Officer (SIRO) and the Council's Data Protection Officer (DPO), or a representative from the Council's Information Management Team.

- 1.10 Any risks relating to Information Governance (including GDPR, Data Protection and FOI legislation) are monitored on a regular basis by this group. Risks and actions are logged and reviewed at CIGG meetings and, if necessary, are escalated in line with the Council's risk management processes.

2. Key Issues

2.1 Maintain Compliance:

- 2.1.1 The key issue is to ensure that compliance with data protection and freedom of information legislation is maintained.
- 2.1.2 Compliance with data protection and access to information principles is a continuous project. CIGG fulfils a core function in monitoring and overseeing information risks by regularly monitoring the effectiveness of the council's governance and implementation of its responsibilities for Data Protection and Freedom of Information.
- 2.1.3 CIGG forms part of the SD Group meetings to ensure compliance messages, as well as actions required, are informed to all Directorates.

2.2 Monitor Performance of Freedom of Information and Right of Access Requests:

- 2.2.1 **Freedom of Information Requests:** Public authorities must respond to requests for information promptly and within 20 working days following the date of receipt of the request (subject to legitimate and notified extension).
- 2.2.2 The statutory target is 100%. The Council strives to meet this target but has an in-house target of 92% minimum.
- 2.2.3 The number of requests received during 2025/26 was 1,423 compared to 1,347 in 2024/25. Overall, 97% of Freedom of Information requests were responded to within the statutory time limits (numerically being 1,380 of the 1,423).
- 2.2.4 This is a 1 percentage point decrease in performance compared to the previous year, but a further numerical increase in the number of requests received.
- 2.2.5 Whilst performance for 2025/26 is 97%, being 1 percentage point lower than previous Year 24/25, analysis of the data did not raise any concerns on the year's performance.
- 2.2.6 In 2025/26 there were no requests formally refused as invalid.
- 2.2.7 There is one individual who remains vexatious on a specific line of enquiry. However, should a vexatious request be received it still receives a formal response (i.e. formal refusal) under the Act. The vexatious status is

reviewed on a six-monthly basis to ensure the Council is applying it proportionately.

2.2.8 **Right of Access Requests:** Organisations normally have one calendar month to reply to a valid and verified request.

2.2.9 RoARs are increasing on a year-by-year basis. For example, RoAR numerical volumes in 2022/23 were 214 requests and have gradually increased to 392 requests in 2025/26.

2.2.10 The number of requests received during 2025/26 was 392, which is a substantial and a step-change increase to the numerical volume received in 2024/25 (which was 235). This continues the trend of the volume of RoARs increasing year-on-year.

2.2.11 Despite this increase, performance improved by 4 percentage points compared with the previous year, with 264 (67%) requests processed within the statutory time frame for 2025/26, compared to 149 (63%) in 2024/25.

2.2.12 The performance of requests is reported under the following categories:

- CCTV footage
- Social care
- Housing
- Joint (i.e. spans more than one Directorate)
- Other

Performance has only been reported in this way for a full year since 2025/26, therefore there is no direct comparison available for 2024/25.

2.2.13 RoAR requests for CCTV footage only are deemed as straightforward to extract, validate, review and process. In 2025/26, of the 392 total RoAR received of these, 97 were for only CCTV. Of these, all 97 CCTV requests were completed within the statutory timeframe (being a performance of 100% for CCTV only requests).

2.2.14 The remaining RoARs can vary in size and complexity. Social Care related requests, especially Childrens, tend to remain large and complex. Attempts have been made, without causing an unnecessary administrative burden, to split these requests into sub-sections in an effort to identify potential improvements.

2.2.15 The increase in requests appears to be relatively equal across all types of requests, which includes growth in large and complex requests. The large and complex cases do have a significant impact on capacity.

2.2.16 These large social care related requests are very resource intensive as they involve reviewing large volumes of historical data, linked to various systems and services, with a notable percentage often linked to legal

cases and/or CSE matters. To place this into context, a single request can take an officer several months to review and complete.

2.2.17 Resource was increased within the Information Management Team in the last 24 months to address workflow increases (especially Right of Access) and this has assisted at allowing some improvements and mitigating adverse impacts of increasing volumes. However, new and/or smarter ways of working will need to be considered to counter increasing workloads.

2.2.18 Appendix 1 provides FOI and RoAR performance for the last five financial years.

2.2.19 Performance will continue to be closely monitored with the focus on improving time to completion (i.e. customer wait times) and keeping customers informed.

3. Data Protection Incidents and Breaches

3.1 The Council actively encourages services to report any suspected data incidents, and all reported cases are investigated. Appendix 2 provides a breakdown of the number and classification of incidents.

3.2 Monitoring information security incidents enables the Council to proactively improve the Council's risk profile by learning lessons from an incident and reducing the likelihood of it happening again. By monitoring and responding to incidents within a 'no blame culture' has ensured that even the smallest of concerns are raised.

3.3 Most data breaches are assessed as low risk or below the threshold for statutory reporting.

3.4 Every reported incident is logged, investigated and recommendations are made to the service that will reduce the likelihood of a repeat incident.

3.5 In 2025/26 the Council logged and investigated 223 reports of incidents, of which 167 were recorded as breaches.

3.6 Examples of low-risk breaches remain the same as previous years, such as misdirected emails with limited or no personal data, emails sent with Carbon Copy (CC) instead of Blind Carbon Copy (BCC) exposing email addresses, and Council Tax bills sent to the wrong address. These are also classed as 'disclosed in error' and account for the significant bulk of incidents.

3.7 Disclosed in error breaches accounted for 134 of the 167 total breaches, being a percentage share of 80% of all breaches for 2025/26. In the previous year (2024/25) the equivalent figures were 129 out of 142 breaches, being a percentage share of 91% of all the reported breaches

- 3.8 With the huge volume of emailing and correspondence that the Council undertakes on a daily basis, these types of 'minor' breaches are unwanted, but incredibly challenging to eliminate. The primary cause is human error (e.g. selecting wrong email address) and it can be any employee of the Council.
- 3.9 Serious breaches and/or breaches that cause concern are escalated beyond the Information Management Team and DPO, and up to the SIRO for awareness and action. These can be cases that may have reputational impact for the Council, large scale safeguarding concerns, or cyber security concerns. Such escalations are not recorded, nor are they needed to be recorded; however, this is being referenced to demonstrate escalation route.
- 3.10 Any data breach with specific safeguarding concerns for children and/or adults will engage the relevant Caldicott Guardian, if the matter is deemed a risk by the Information Management Team. Again, such escalations are not recorded, nor are they needed to be recorded; however this is being referenced to demonstrate escalation route
- 3.11 Serious breaches that cause further concern and/or meet ICO's reporting threshold must be reported to the Information Commissioner's Office (ICO). Reporting should be done by the organisation within 72 hours of the issue being identified. Two incidents were reported to ICO in 2024/2025 financial year, where no action was taken by the Information Commissioner, however zero cases were reported for 2025/26.
- 3.12 The Council also monitors non-fault data breaches of its data, where we are advised of any issues. This would be where an organisation processing personal data on behalf of the Council (e.g. a contractor) loses or exposes Rotherham data it is holding. This monitoring is to ensure the Council understands what has occurred, why and what measures are being put in place to resolve and mitigate recurrence. If necessary, it will also be reviewed from a breach of contractual stance from the relevant service.

4. Options considered and recommended proposal

- 4.1 There are no new proposals or recommended options. However, it is a requirement that the council continues the maintenance of its Information Governance processes in compliance with Data Protection and Freedom of Information requirements.
- 4.2 It should be noted that continued compliance to the Data Protection Act 2018 and the Freedom of Information Act 2000 (including Environmental Information Regulations 2004) can only be achieved by the continued support of all Council Staff and Councillors. Key roles such as Information Asset Owners and Data Protection Officer can use existing governance structures to ensure ongoing compliance.

5. Consultation on proposal

5.1 None

6. Timetable and Accountability for Implementing this Decision

6.1 None

7. Financial and Procurement Advice and Implications

7.1 There are no direct financial or procurement implications arising from this report.

8. Legal Advice and Implications

8.1 There are no legal implications arising from this report, except to reiterate that the council has a duty to comply with Data Protection legislation.

9. Human Resources Advice and Implications

9.1 There are no direct implications for HR arising from this report.

10. Implications for Children and Young People and Vulnerable Adults

10.1 There are no direct implications for children and young people or vulnerable adults arising from this report.

11. Equalities and Human Rights Advice and Implications

11.1 There are no direct equalities or human rights implications arising from this report.

12. Implications for Partners

12.1 There are no direct implications for partners arising from this report.

13. Risks and Mitigation

13.1 Risks and mitigation will be managed by CIGG and the council's risk processes.

14. Accountable Officer(s)

Luke Sayers, Assistant Director- Customer, Information and Digital Services
luke.sayers@rotherham.gov.uk

Sam Ulyatt, Service Manager - Information Management
sam.ulyatt@rotherham.gov.uk

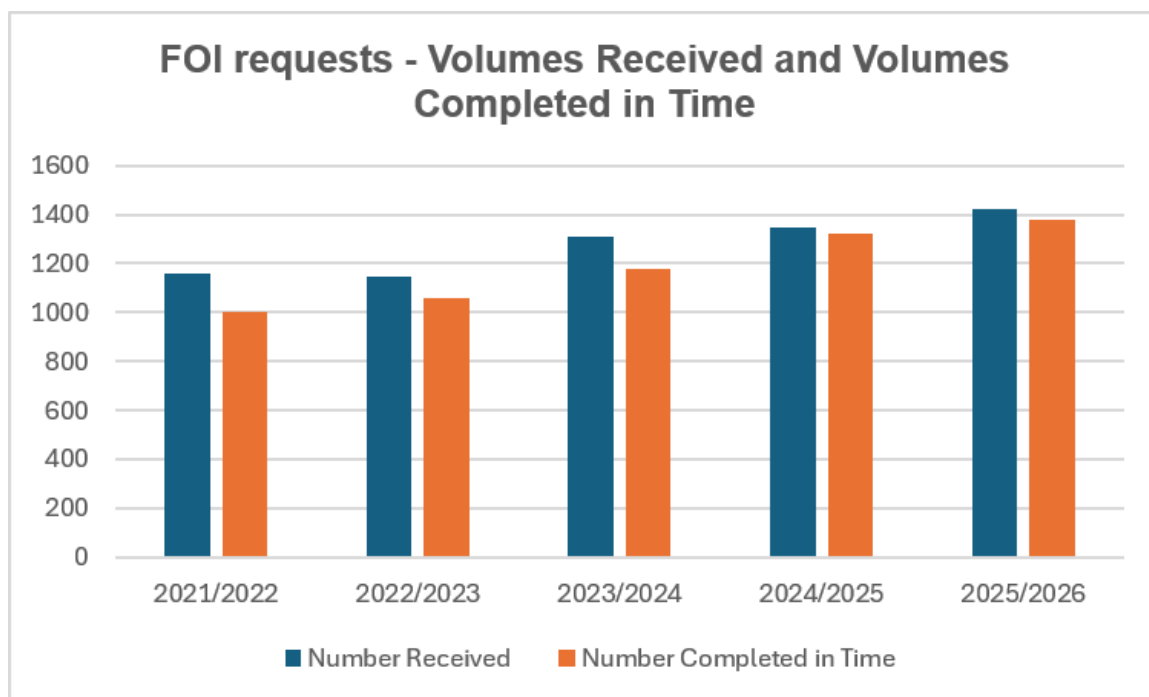
Report Author:

Luke Sayers, Assistant Director- Customer, Information and Digital Services
luke.sayers@rotherham.gov.uk

Sam Ulyatt, Service Manager - Information Management
sam.ulyatt@rotherham.gov.uk

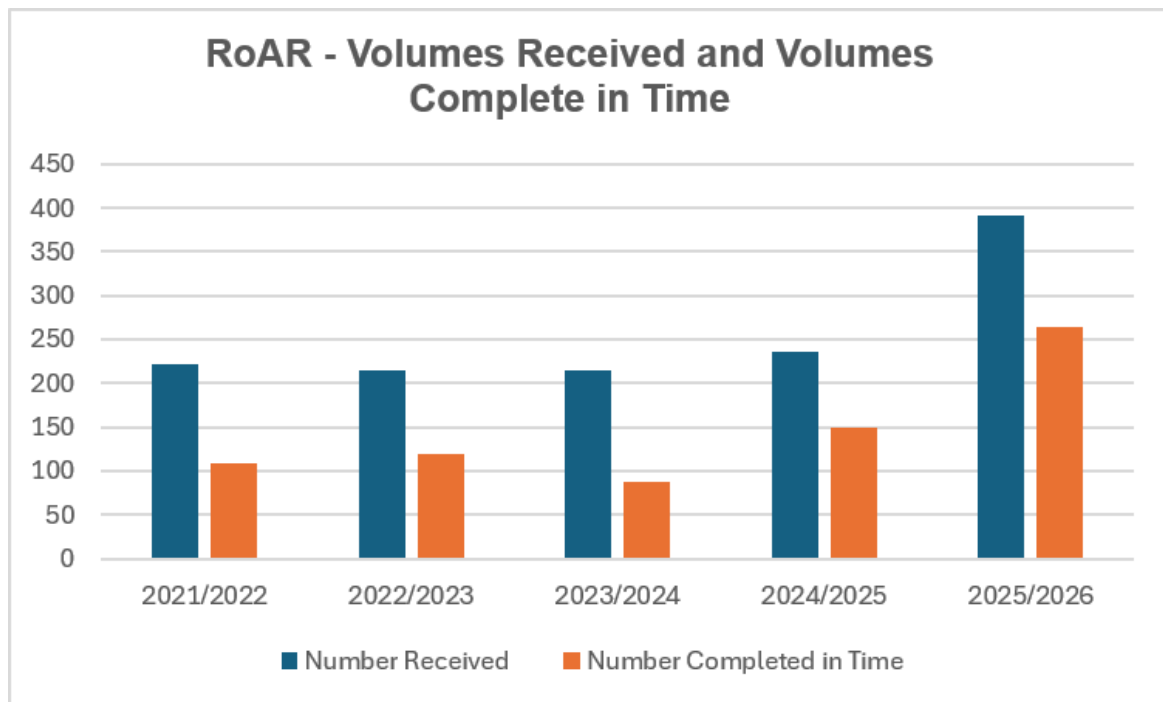
Appendix 1: FOI & RoAR Statistics

Freedom of Information (FOI) Requests



Freedom Of Information Requests			
Year	Number Received	Number Completed in Time	% Completed in Time
2021/2022	1160	1002	86%
2022/2023	1145	1060	92%
2023/2024	1307	1177	90%
2024/2025	1347	1323	98%
2025/2026	1423	1380	97%

Right of Access Requests (RoARs)



Right of Access Requests			
Year	Number Received	Number Completed in Time	% Completed in Time
2021/2022	222	109	49%
2022/2023	214	120	56%
2023/2024	214	87	41%
2024/2025	235	149	63%
2025/2026	392	264	67%

Appendix 2: Information Security Incidents (data breaches)

Information Data Incident Stats 2025/26						
Cases Investigated	Total number of incidents	Reported to ICO	Complaints from ICO			
223	167	0	0			
Incident Category	CS	PSE	R&E	PH	CYPS	ACX
Lost or stolen hardware	2	0	0	0	1	1
Lost or stolen paperwork	2	0	0	0	0	0
Disclosed in Error	27	24	14	0	59	10
Uploaded in error	0	0	2	0	5	0
Unauthorised access/disclosure	3	2	1	0	2	1
Non-secure Disposal – paperwork					1	1
Social Media Platforms	0	0	0	0	1	0
IG Other	4	1	1	0	2	0
Totals No of Incidents 25/26	38	27	18	0	71	13

Year	Cases Investigated	Total Number of Incidents	Reported to ICO
2021/2022	179	122	1
2022/2023	173	134	2
2023/2024	201	154	1
2024/2025	195	142	2
2025/2026	223	167	0