

Committee Name and Date of Committee Meeting

Audit Committee – 25 September 2025

Report Title

Information Governance Annual Report 2024/25

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, Assistant Director- Customer, Information and Digital Services

luke.sayers@rotherham.gov.uk

Paul Vessey, Head of Information Management

paul.vessey@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/FOI Annual Report 2024/25.
2. Note that it is a requirement that the Council continues its maintenance of its Information Governance practices and processes in compliance with legislation.

List of Appendices Included

Appendix 1 FOI & RoAR Statistics

Appendix 2 Data Breaches

Background Papers

Information Commissioner's Office

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

A-Z of Information Management Documents

[Information Management - Home](#)

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:
 - 1.3.1 Is 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.
- 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 Monitoring of the council's compliance with DPA and FOI is carried out by the Corporate Information Governance Group (CIGG) which is a standing agenda on the Assistant Directors' Group and attended by the Council's Senior Information Risk Officer (SIRO) and a representative from the Council's Information Management Team.

- 1.9 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 AD 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.

- 2.2.2 Overall 98% of Freedom of Information requests were responded to within the statutory time limits. The number of requests received during Year 2024/25 was 1,347 compared to 1,307 in 2023/2024.

- 2.2.3 This is an improvement in performance compared to the previous year, and a further numerical increase in the number of requests received.

- 2.2.4 Analysis of the data did not raise any concerns on the year's performance.

- 2.2.5 In Year 24/25 there was 1 x request formally refused as invalid, due to the requestor being suspected of impersonation and refusing to verify their submission. Additionally, there is one individual who is vexatious on a specific line of enquiry. However, should a vexatious request be received it still receives a formal response under the Act.

- 2.2.6 **Right of Access Requests:** Organisations normally have one calendar month to reply to a valid request.

- 2.2.7 The number of requests received during 2024/25 was 235, which is an increase to the numerical volume received in 2023/2024. This continues the trend of receiving over 200 RoARs each financial year.

- 2.2.8 Performance improved by 22 percentage points compared with the previous year, with 149 requests processed within the statutory time frame.
- 2.2.9 Simple RoARs include requests for CCTV coverage and requests for information which is held in individual systems such as Housing and Council Tax. All are straightforward to extract, validate, review and process.
- 2.2.10 Large and complex RoARs have remained relatively stable but remain at a volume that has significant impacts.
- 2.2.11 These large requests are often social care related. These 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 in excess of six months to review and complete.
- 2.2.12 Additional resources were added to the team's capacity to improve performance and this is reflected in this year's improvements in FOIs and RoARs.
- 2.2.13 Appendix 1 provides FOI and RoAR performance for the last five financial years.
- 2.2.14 Performance will continue to be closely monitored with the focus on improving time to completion (i.e. customer wait times).

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 two 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 Examples of low-risk breaches are 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 are approximately 88% of the reported breaches.

- 3.6 Serious breaches are reported to the Information Commissioner's Office (ICO) and two incidents were reported to ICO in 2024/2025 financial year. No action was taken by the Information Commissioner.

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) 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.

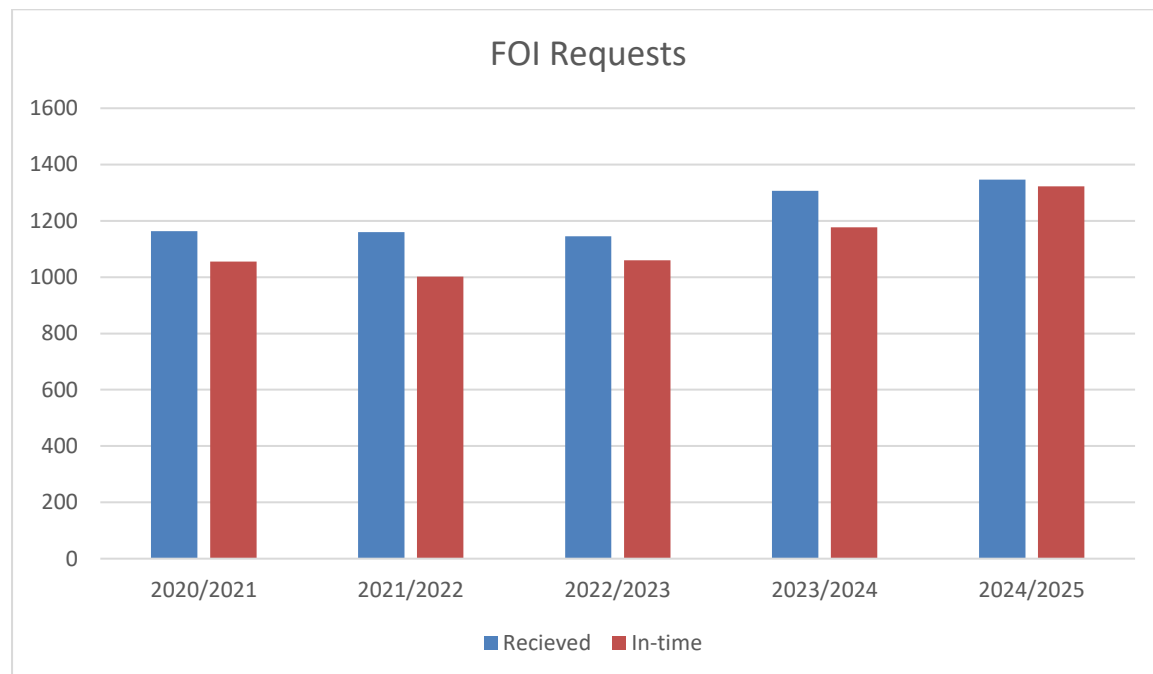
14. Accountable Officer(s)

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

Paul Vessey, Head of Information Management
paul.vessey@rotherham.gov.uk

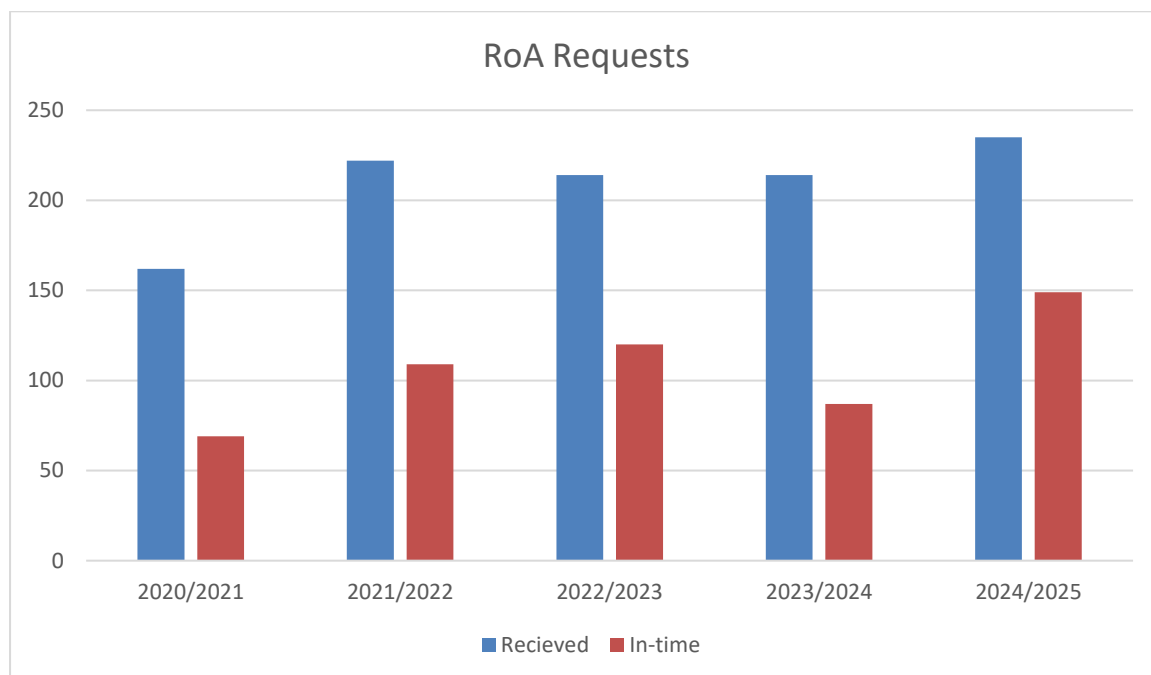
Appendix 1: FOI & RoAR Statistics

Freedom of Information (FOI) Requests



Freedom Of Information Requests			
Year	Number Received	Number Completed in Time	% Completed in Time
2020/2021	1163	1055	91%
2021/2022	1160	1002	86%
2022/2023	1145	1060	92%
2023/2024	1307	1177	90%
2024/2025	1347	1323	98%

Right of Access Requests (RoARs)



Right of Access Requests			
Year	Number Received	Number Completed in Time	% Completed in Time
2020/2021	162	69	43%
2021/2022	222	109	49%
2022/2023	214	120	56%
2023/2024	214	87	41%
2024/2025	235	149	63%

Appendix 2: Data Incidents

Information Data Incident Statistics 2024/25						
Cases Investigated	Total number of incidents	Reported to ICO	Complaints from ICO			
195	142	2	1			
Incident Category	FACS	ACH	R&E	PH	CYPS	ACX
Lost or stolen hardware		1			2	1
Lost or stolen paperwork		2			1	1
Disclosed in Error	25	27	11		55	11
Technical security failing					1	
Unauthorised access/disclosure		3			1	
Totals No of Incidents 24/25	25	33	11		60	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