CROYDON

Final Internal Audit Report

Information Governance – SAR and FOI

December 2024

Distribution:

Interim Assistant Chief Executive
Interim Chief Digital Officer & Director of Resident Access
Business Operations Manager
Data Protection Officer
Corporate Director Adult Social Care and Health
Corporate Director of Resources & S151 Officer
Director of Finance & Deputy S151 Officer

Assurance Level	Issues Identified	
Limited	Priority 1	2
	Priority 2	2
	Priority 3	0

forvis mazars

Contents

Page

Executive Summary

Detailed Report

Appendices

forvis mazars

1. Introduction

1.1. Subject Access Requests (SAR) enable individuals to request all the data held about them personally while Freedom of Information (FOI) requests enable individuals to ask any public sector organisation for information. FOIs can be rejected in certain circumstances, for instance if it would cost too much, the information is commercially sensitive or the information is already publicly available.

1.2. The Freedom of Information Act 2000 (FOIA) is intended to promote greater openness and accountability by providing a general right of access to information held by local authorities, central government, NHS, schools, and police. The FOIA provides exemptions to the general right of access. If any of the information requested is exempt, the requestor will be informed which exemption applies and why.

1.3. As per Croydon's Freedom of information (FOI) extract, 485 information requests were received during the period: 1 January 2023 to 31 March 2023. Out of these requests 71 (15%) remained open at the time of the audit and the remaining were as follows:

- 235 (48%) requests had the status 'Provided in Full;
- 89 (18%) requests had the status 'Part Provided, Part Rejected';
- 42 (9%) requests had the status 'Information Not Held';
- 38 (8%) requests had the status 'Rejected – Exempt';
- 9 (2%) requests had the status 'Rejected – Exceeds Reasonable Limits'; and
- 1 request was withdrawn by the requestor.

1.4. As per Croydon's Subject Access Request (SAR) extract, 114 requests were received during the period: 1 January 2023 to 31 March 2023. Out of these requests 24 (21%) remained open at the time of the audit and the remaining were as follows:

- 23 (20%) requests had the status 'Provided in Full';
- 44 (39%) requests had the status 'Part Provided, Part Rejected';
- 6 (5%) requests had the status 'Information Not Held';
- 7 (5%) requests had the status 'Rejected – Exempt' or 'Rejected – ID not provided'; and
- 10 (10%) requests had the status 'Withdrawn'.

1.5. At Croydon Council (the Council), there is a central Information team who manage all FOI and SAR requests that are received across the Council. However, Corporate Directors are also involved in the process to respond to requests. The Council uses the system 'Infreemation' to track, manage and report on all requests. The general process is as follows.

- Requests are received for information in the Council's dedicated inbox for FOI requests or SAR and then manually logged onto the Infreemation system by the Information team;
- Any requests submitted via online web form are automatically logged onto Infreemation;
- The case is then assigned to the relevant Corporate Directors who has responsibility to ensure that the Council provides the necessary response or give a reason why it should be rejected;
- Information officers use this response to create the final document in the correct format and send to requestor; and
- The case is closed on Infreemation, and the FOI is added to the disclosure log, which is published on the Council's website.

1.6. There are many exemptions for not having to disclose the information requested, these can range from to protect national security to not disclosing personal information under the Data Protection Act 2018.

1.7. Individuals have the right to appeal the decision of a FOI, and these are also tracked on the Infreemation system. Requestors have 40 working days after receiving their response to submit an appeal. To help ensure objectivity, appeals are conducted by a member of the legal team who must not have been involved in the original decision. Once received, the deadline to respond to an appeal is the same 20 working days as an original FOI request.

1.8. Weekly management reports are sent to the Corporate Directors and Directors across the Council which include the total number of FOIs/SARs open and overdue. These figures are then broken down into each directorate and summary statistics are produced which show the data trends.

1.9. Whilst the review and testing were performed remotely, the relevant documents required to complete the review were obtained.

1.10. The audit was undertaken as part of the agreed Internal Audit Plan for 2022/23. The objectives, approach and scope are contained in the Audit Terms of Reference at Appendix 1. This audit was focussed on the process and compliance with the Council policies and procedures. It was not conducted by a GDPR or data privacy specialist auditor.

2. Key Issues

Priority 1 Issues
There was no internal policy or guidance in relation to all aspects of the FOI process in place at the Council. **(Issue 1)**
Not all FOIs had been responded to within the mandated deadline of 20 working days. **(Issue 2)**
Priority 2 Issues
The completion of staff training was not being monitored. **(Issue 3)**
The weekly management reports did not include the number of appeals. **(Issue 4)**

2. Actions and Key Findings/Rationale

Control Area 1: Regulatory, Organisational and Management requirements;

<table>
<tr><th>Priority</th><th>Action Proposed by Management</th><th>Detailed Finding/Rationale - Issue 1</th></tr>
<tr><td>1</td><td>There are now policies, procedure and training for all staff handling FOI requests.

This was actioned as part of the ICO improvement plan.</td><td rowspan="3">Expected Control

Procedures are in place covering all aspects of the FOI process, which are up to date and available to all members of staff. Those with responsibility for responding to FOI requests are clearly identified and communicated to all staff.

Finding/Issue

The acting Information Manager explained that there were no centralised procedure documents which covered all aspects of the FOI process. Therefore, there was no guidance available to staff to direct them when processing FOI requests. It was explained that the Council relied on the knowledge of staff members to implement the FOI processes.

Risk

Where there are no formal procedure documents in place, there is an increased risk that important knowledge can be lost when staff leave and cause delays in responding to FOIs. These delays can lead to non-compliance of the Freedom of Information Act 2000.</td></tr>
<tr><td>Responsible Officer</td><td>Deadline</td></tr>
<tr><td>Data Protection Officer</td><td>Complete</td></tr>
</table>

Control Area 2: Recording, Processing and Responding to SAR and FOI Requests;

<table>
<tr><th>Priority</th><th>Action Proposed by Management</th><th>Detailed Finding/Rationale - Issue 2</th></tr>
<tr><td>1</td><td>Completed. There are regular review meetings being held and reported via IM Internal control board that reports into CMT.

Resource of the central team is being invested in until October 2024 by which time there will be a review as part of the wider CDS review.</td><td rowspan="3">Expected Control

The work systems in place result in FOI requests being responded to in accordance with the 20 working days deadline. This timeframe is stated in the Freedom of Information Act 2000.

Finding/Issue

The acting Information Manager explained that not all FOI requests have been responded to in the 20 working days deadline. This was demonstrated in the management report where only 40% of FOIs in March 2022 were returned within 20 days.

Although it was noted that the percentage of FOIs responded on time had improved to 91% in February 2023, this turnaround rate needed to be sustained.

Risk

Where not all FOIs are responded to within 20 working days, there is an increased risk of non-compliance with the Freedom of Information Act 2000, which can affect the Council's reputation. Non-compliance leads to investigation and intervention by the Information Commissioners Office.</td></tr>
<tr><td colspan="2"><table><tr><th>Responsible Officer</th><th>Deadline</th></tr><tr><td>Data Protection Officer</td><td>Complete</td></tr></table></td></tr>
</table>

Control Area 1: Regulatory, Organisational and Management requirements;

<table>
<tr><th>Priority</th><th>Action Proposed by Management</th><th>Detailed Finding/Rationale - Issue 3</th></tr>
<tr><td rowspan="3">2</td><td rowspan="3">Training has been created and delivered to all relevant staff upskilling the use of exemptions and increasing the understanding of statutory responsibilities. The training is now available on the Croydon Learning portal so we can report and manage on the uptake of the training.</td><td rowspan="3">Expected Control
Specific training exists for processing FOIs and SARs. This training is made available to all relevant staff and completion is monitored.
Finding/Issue
Evidence was requested of staff training delivered and completed; however, this was not provided as the acting Information Manager explained that these records did not exist. Therefore, the Council were unaware which officers have completed training and when this last completed.
Risk
Where staff training records are not being monitored, there is a risk that staff do not have the necessary skills to perform their job efficiently which leads to errors or delays in the responding of requests.</td></tr>
<tr><th>Responsible Officer</th><th>Deadline</th></tr>
<tr><td>Data Protection Officer</td><td>Complete</td></tr>
</table>

Control Area 4: Performance and Management Information;

<table>
<tr><th>Priority</th><th>Action Proposed by Management</th><th>Detailed Finding/Rationale - Issue 4</th></tr>
<tr><td>2</td><td>A report is circulated weekly to monitor FOI and SAR compliance across the Council – reports are also shared at the monthly IM Control board meeting. As of November 2024, this report includes an ‘internal reviews’ section, duplicated across each Directorate.</td><td rowspan="3">Expected Control
Weekly and monthly reporting of FOI requests and SARs to CMT takes place to allow management to monitor performance and compliance with legislation. Reporting includes the number of appeals, highlighting both successful and unsuccessful cases. Where reporting demonstrates underperformance or non-compliance, action plans are established to take corrective action.
Finding/Issue
A review of four weekly management reports between 6 March 2023 and 4 April 2023 found that there was no information included on appeals. The acting Information Manager confirmed that the Council did have the ability to create these reports, but it was not being done.
Risk
Where the number of appeals is not reported on, there is a risk that actions are not discussed and implemented which could reduce the number of appeals.</td></tr>
<tr><td>Responsible Officer</td><td>Deadline</td></tr>
<tr><td>Data Protection Officer</td><td>Complete</td></tr>
</table>

Appendix 1

AUDIT TERMS OF REFERENCE

Information Governance – FOI and SAR

1. INTRODUCTION

1.1 The General Data Protection Regulations (GDPR) and the Data Protection Act (DPA) 2018, detail that anyone has the right to find out if the Council is using or storing their personal data. This is called the right of access and is achieved through making a subject access request (SAR).

1.2 With respect the GDPR and the DPA 2028, the Council will, as an example:

- Fully observe the legal conditions regarding the collection and use of the personal information they hold;
- Meet legal obligations to specify the purposes for which information is used and are detailed in the relevant privacy notices and statements;
- Meet legal obligations to specify the purposes for which information is used and are detailed in the relevant privacy notices and statements;
- Take appropriate technical and organisational measures to safeguard personal information and protect your privacy; and
- Ensure that the rights of people about whom information is held are able to be fully exercised

1.3 Multiple relevant procedures are published on the Council's website which can provide additional guidance. Examples of these policies are:

- General Data Protection Regulation (GDPR) guidance; and
- Data protection policy.

1.4 The Freedom of Information Act 2000 (FOIA) is intended to promote greater openness and accountability by providing a general right of access to information held by local authorities, central government, NHS, schools, and police. The FOIA provides exemptions to the general right of access. If any of the information requested is exempt, the requestor will be informed which exemption applies and why. Examples include information that is commercially sensitive, confidential, or readily available elsewhere.

1.5 All public authorities in line with the requirements of the FOIA must maintain a 'Publication Scheme,' which is a catalogue of information that an Authority already makes available to the public as a matter of course. A 'Publication Scheme' should state what format the information can be supplied, who can provide access and whether there will be a fee to provide that information.

1.6 Possible outcomes following an information request review are that:

- Information may be disclosed which was previously withheld, and/or;
- The Council has not followed its procedures in relation to Freedom of Information. The Council will apologise and tell the requestor what to be

done to put it right and to make sure that similar errors do not occur in the future, or;
- The initial decision to withhold information is upheld and/or;
- The Council has correctly followed its procedures.

1.7 Per Croydon's Freedom of information (FOI) archive, 57 information requests were processed during the period: 1 April 2022 to 31 May 2022. Out of these 57 requests:

- 26 (45.6%) requests have the status 'All information sent';
- 25 (43.8%) requests have the status 'Some information sent but part exempt';
- Five (8.7%) requests have the status 'Some information sent but not all held'; and
- One information request has a note on an email received for a case to be processed by 11 May 2022.

1.8 This audit is part of the agreed Internal Audit Plan for 2022/23.

2. OBJECTIVES AND METHOD

2.1 The overall audit objective is to provide an objective independent opinion on the adequacy and effectiveness of controls / processes.

2.2 The audit will for each controls / process being considered:

- Walkthrough the processes to consider the key controls;
- Conduct sample testing of the identified key controls, and
- Report on these accordingly.

3. SCOPE

3.1 This audit included the following areas (and issues raised):

Control Areas/Risks	Issues Raised		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Legislative, Organisational and Management Requirements	1	1	0
Recording, Processing and Responding to SAR and FOI Requests	1	0	0
Appeals	0	0	0
Performance and Management Information	0	1	0

Control Areas/Risks	Issues Raised		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Total	2	2	0

Appendix 2

Definitions for Audit Opinions and Identified Issues

In order to assist management in using our reports:

We categorise our **audit assurance opinion** according to our overall assessment of the risk management system, effectiveness of the controls in place and the level of compliance with these controls and the action being taken to remedy significant findings or weaknesses.

	Full Assurance	There is a sound system of control designed to achieve the system objectives and the controls are constantly applied.
	Substantial Assurance	While there is basically a sound system of control to achieve the system objectives, there are weaknesses in the design or level of non-compliance of the controls which may put this achievement at risk.
	Limited Assurance	There are significant weaknesses in key areas of system controls and non-compliance that puts achieving the system objectives at risk,
	No Assurance	Controls are non-existent or extremely weak, leaving the system open to the high risk of error, abuse and reputational damage.

Priorities assigned to identified issues are based on the following criteria:

Priority 1 (High)	Fundamental control weaknesses that require immediate attention by management to action and mitigate significant exposure to risk.
Priority 2 (Medium)	Control weakness that still represent an exposure to risk and need to be addressed within a reasonable period.
Priority 3 (Low)	Although control weaknesses are considered to be relatively minor and low risk, still provides an opportunity for improvement. May also apply to areas considered to be of best practice that can improve for example the value for money of the review area.

Appendix 3

Statement of Responsibility

We take responsibility to London Borough of Croydon for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Forvis Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

Registered office: 30 Old Bailey, London, EC4M 7AU, United Kingdom. Registered in England and Wales No 0C308299.