Leicester City Council

INFORMATION GOVERNANCE: CASE MANAGEMENT

LEICESTER CITY COUNCIL

	Critical	Significant	Moderate	Opportunity
Findings	0	0	5	1
Overall audit opinion	**Reasonable Assurance**			

INTERNAL AUDIT REPORT

Status: Final

Date issued: 29 October 2024

Responsible officer: City Barrister and Head of Standards (Monitoring Officer)

Veritau

INTRODUCTION

The UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 place various responsibilities on organisations regarding the processing of personal information. It is essential that the council has effective measures in place to demonstrate and ensure ongoing compliance with this legislation and others, relating to access to information. Information remains one of the most valuable assets held by any organisation and failure to secure personal or sensitive data may lead to breaches under UK GDPR and the Data Protection Act. These breaches can cause significant harm to individuals, reputational damage to the organisation and lead to potential financial penalties or other forms of censure.

The Information Governance and Risk team at Leicester City Council performs a vital second line compliance role as well as providing technical support to officers, and handling information access requests. The team performs several key functions in these areas. It is involved with handling information requests such as Subject Access Requests (SARs) and Freedom of Information requests (FOIs), recording and investigating information security incidents, supporting work on information sharing and other processing matters, and providing a wide range of advice and corporate guidance on data protection and other information governance issues.

The team uses the Incase Intelligence system to manage, process and respond to FOIs and SARs, as well as for logging data breaches, data protection impact assessments (DPIAs) and information sharing agreements.

OBJECTIVES AND SCOPE

The purpose of this audit was to provide assurance to management that procedures and controls within the system ensured that:

- Policies and procedures relevant to the functions of the Information Governance & Risk team, are in place and subject to regular review.
- Clear arrangements are in place for recording and handling information requests (SARs, other rights requests, and FOIs), and information security incidents in a timely manner.
- DPIAs are completed and reviewed, with recommendations followed up, and information sharing agreements are logged and reviewed.

- Performance information is reported to key stakeholders.

The audit reviewed the responsibilities directly under the Information Governance and Risk team which included information security incidents, SARs and FOIs, information sharing agreements (ISAs) and DPIAs. It provided assurance that controls were in place to effectively manage and oversee the team's specific functions.

The audit did not include review of the council's wider information governance arrangements such as information asset management, information security, or CCTV and surveillance.

KEY FINDINGS

The Information Governance and Risk team has a broad remit in relation to information governance, providing key specialist and administrative support to the council's compliance efforts. The findings from this audit support that the team has been delivering these functions effectively. The team is maintaining a very good level of performance, especially in relation to incident management and information requests, with performance levels consistently at or exceeding ICO expectations. For example, FOI in-time response compliance was at 96% in June 2024.

This level of performance is being maintained despite there being little support provided by the current Incase Intelligence system in managing the team's key workflows. As a result, the team is operating multiple systems, requiring extensive work outside of Incase, and resulting in duplication of effort, as well as increasing the chance of human error. The former Head of Information Governance & Risk (DPO) informed us that a new web-based version of Incase will be coming into effect during this financial year. This may provide an opportunity to improve the functionality and address some of the weaknesses with the current system.

A number of policies, procedures and guidance documents are in place that cover the key functions of the team. All key policies and procedures had been subject to regular review, although there were some guidance documents which had not been reviewed for several years. Some gaps were also identified as there were no specific procedures and guidance documents relating to DPIAs and the information security incident procedure contained some out-of-date information.

There are clear arrangements in place for handling information requests. Testing confirmed that the processing of FOIs and SARs is well managed, with all those sampled (10 FOIs and 10 SARs) being completed within statutory timescales. ID had been requested for SARs in all cases. Exemptions applied to FOI requests were recorded on the disclosure log but not Incase as the system does not have this functionality.

The sample of incidents and data breaches confirmed a reporting form was in place, they had been correctly logged, and the risk to data subjects had been assessed. Incidents were reported to the ICO within 72 hours where applicable. Investigations had taken place, with improvement recommendations given. However, formal timescales are not given for implementation of recommendations. As a result, some services had not responded and recommendations were not complete at the time of testing. The incident log was also not fully up to date with the closure of some incidents.

All DPIAs in the sample had been signed by the DPO, with recommendations given. However, examples were seen where DPIA forms had not been returned signed by the service area to confirm acceptance of DPO recommendations. Where DPIAs were outstanding, these were not always being routinely chased up.

ISAs are recorded and tracked using Excel. However, this is not fit for purpose for tracking their completion and review dates. From our discussions with officers, and from review of the Excel log, we were not able to provide assurance that the log is accurate and up to date, and reflects all ISAs the council has entered into.

Annual reports are being presented to CMT with key performance information, such as FOI and SAR. Directors also receive monthly statistics on data security incidents. However, performance information is not regularly reported to the Corporate Information Group (CIG), as a standing agenda item. It was also noted that there is no formal schedule in place for CIG meetings and these are currently scheduled ad hoc. CIG meetings have not taken place at the usual frequency this year due to the cyber-attack and resourcing difficulties.

OVERALL CONCLUSIONS

Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made. Our overall opinion of the controls within the system at the time of the audit was that they provided Reasonable Assurance.

1 Incase intelligence system

Moderate

Control weakness

The lack of functionality with the current system means workflow processes are manual, time consuming and information is stored in multiple places rather than centrally on one system. The system does not assist the team with carrying out and managing the performance of its key functions.

What is the risk?

Failure to respond in a timely manner to poor performance or compliance risks, lack of efficiency, and human error.

Findings

The Information Governance and Risk team uses Incase Intelligence system. However, the system does not currently have the functionality to record and track all workflow in its entirety. Therefore, key processes are performed manually, are time consuming and, at times, represent duplication of effort. For example, information relating to incidents and data breaches is stored in multiple places. Incidents are logged on Incase with basic information. However, the detail is recorded in a separate Excel workbook. The progress of information security incident investigations and the tracking of recommendations are also managed via a third system – a series of shared folders in the information security incidents email inbox. A fourth system sees key information stored on the shared drive in the incidents folder. Similar processes were also observed for the recording and monitoring of other key responsibilities of the team e.g. SARs and FOIs, although this was through Incase, emails and the shared drive rather than a separate log also.

The system does not have the functionality to set deadlines, due dates and to schedule reminders for the team. It also lacks the ability to provide useful management information to monitor performance (e.g. to summarise or visually display outstanding items). This therefore relies on officers labelling individual email folders with key dates and monitoring through this route or, in the case of ISAs, manually reviewing the log spreadsheet to check dates, which is not routinely taking place.

The former Head of Information Governance & Risk (DPO) explained that the current version of Incase does not have a readily available reporting functionality. Therefore, statistics for the annual report are manually counted rather than produced by the system. Furthermore, reports cannot be run to assist the team in the completion of tasks e.g. a report to monitor review dates and recommendations for DPIAs, overdue ISAs, key deadlines for SARs and FOIs.

Overall, the process of administering key tasks is significantly hampered by the number of separate systems in use and, in turn, on their reliance on manual operation. The former Head of Information Governance & Risk (DPO) informed us that the team are moving to a new web-based version of Incase, scheduled for later this year, which may improve the functionality and address some of the weaknesses with the current system.

Agreed action

It is recognised that there are limitations with the current system. A permanent DPO will be in place from November 2024 who will take actions with Incase to either improve the functionality of the current system or look to prioritise bringing in these improvements at the time of the renewal of the product in March, to InCase365 web-based version.

Responsible officer: City Barrister and Head of Standards (Monitoring Officer) **Timescale**: March 2025