

MALDON DISTRICT COUNCIL

INTERNAL AUDIT REPORT - FINAL

GENERAL DATA PROTECTION REGULATION (GDPR)
MAY 2025

Design Opinion



Moderate

Effectiveness Opinion



Moderate

CONTENTS

EXECUTIVE SUMMARY	2
DETAILED FINDINGS	6
APPENDIX I - DEFINITIONS.....	16
APPENDIX II - TERMS OF REFERENCE	17

DISTRIBUTION

Annette Cardy	Assistant Director - Resources
Emma Holmes	Data Protection Officer

BDO LLP APPRECIATES THE TIME PROVIDED BY ALL THE INDIVIDUALS INVOLVED IN THIS REVIEW AND WOULD LIKE TO THANK THEM FOR THEIR ASSISTANCE AND COOPERATION.

REPORT STATUS

Auditors:	Aaron Winter - Partner Christopher Beveridge - National Head of Privacy and Data Protection Services Andrew Billingham - Internal Audit Manager Antony Hadjirousos - IT Audit Senior Manager Alex Russell - IT Audit Assistant Manager Bismah Rahman - Internal Auditor
Dates work performed:	8 October 2024 - 16 December 2024
Draft report issued:	10 January 2025
Management Response Received:	16 May 2025
Final report issued:	16 May 2025

EXECUTIVE SUMMARY

Control Design



Moderate

Control Effectiveness



Moderate

Recommendations



SCOPE

BACKGROUND

The management and use of personal information in the current environment has become increasingly important as both expectations for information governance and the service expected by customers have become more demanding.

In May 2018, the General Data Protection Regulation (the UK GDPR) replaced the Data Protection Act 1998 (the DPA) as the regulation governing the protection of personally identifiable information in the UK. As a data controller, Maldon District Council ("the Council") is responsible for ensuring that it complies with the UK GDPR and that parties that process information on its behalf are also compliant with the UK GDPR.

The penalties for being in breach of the UK GDPR are greater than those that could be levied under the DPA. This regulation places greater responsibilities on data controllers whilst at the same time increasing the power of the Information Commissioner's Office (ICO) to levy fines of up to £17.5 million or 4% of an organisation's global revenue (whichever figure is higher). Personal data breaches must be reported to the ICO within 72 hours of the Council becoming aware of the breach if that breach is deemed to have a high risk to the fundamental rights and freedoms of the affected individuals.

PURPOSE

The purpose of the audit was to assess the Council's compliance against key parts of UK GDPR, including training and awareness, roles and responsibilities, data breach management, data protection impact assessments, policies and procedures, and governance of information assets.

AREAS REVIEWED

The following areas were covered as part of this review:

- ▶ Assess whether there is a governance framework in place to support compliance with data protection responsibilities, including defined, approved and up to date policies and procedures.
- ▶ Determine whether roles and responsibilities with regards to data protection are defined and whether there is a training programme in place for data protection and information management for staff which is regularly refreshed.
- ▶ Assess whether the Council has a Record of Processing Activities (RoPA) in place and that this is regularly reviewed and updated and captures appropriate information.
- ▶ Assess whether the Council has defined retention periods in place for held information and that this is adhered to.
- ▶ Determine whether the Council has defined the lawful basis for collecting, processing, retaining, and sharing information and assess whether this is transparent to data subjects using tools such as privacy

notices. For special category data, assess whether the reasons for processing are appropriate and in line with the original purpose of the processing activity.

- ▶ Assess whether there is regular monitoring of the Council's compliance with data protection legislation and regulations by senior management, including the identification, assessment, and remediation of identified risks.
- ▶ Assess whether there are procedures in place to deal with data subject rights requests, including Subject Access Requests (SARs) and Freedom of Information Act requests (FOIs). Determine the extent to which these requirements are complied with, responded to, monitored, and reported on.
- ▶ Assess whether adequate and effective data breach response procedures are in place.
- ▶ Assess whether there are adequate procedures in place for performing Data Privacy Impact Assessments (DPIAs) for the processing of data which is likely to present a high risk to the rights and freedoms of individuals.
- ▶ Where the Council shares personal data as part of its relationships with third parties, determine whether the risks posed by these relationships have been assessed and whether data sharing agreements have been implemented to mitigate these risks.



AREAS OF STRENGTH

During our review, we identified the following areas of good practice:

- ▶ The Council has a dedicated Data Protection Officer (DPO), who has clearly defined responsibilities in line with the requirements of the UK GDPR and regularly reports to Senior Management. The DPO is responsible for managing the Council's compliance with data subject rights requests, including SARs and FOIs.
- ▶ The Council has a defined Data Protection Policy in place, which was last reviewed and approved in September 2024 as part of a suite of GDPR policies which includes the Processing of Special Category Data Policy and the Document Retention Schedule policy (which breaks down retention periods by the different service areas). The Data Protection Policy sets out the Council's approach towards complying with the requirements of the UK GDPR, including a defined set of responsibilities that the Council must follow with regard to data processing and data protection.
- ▶ There is monitoring and reporting against data protection Key Performance Indicators (KPIs) via the Council's management reporting tool, the Balance Scorecard, which is shared with the Extended Leadership Team (ELT) ahead of every monthly meeting, so that performance against KPIs can be discussed as required. By review of the Balance Scorecard, we confirmed that the Council has consistently exceeded its FOI request response target of 95% by attaining 99% compliance through responding within 20 working days every month since May 2024.
- ▶ Subject Access Request Staff Guidance, which covers the Council's obligations and timelines in relation to Subject Access Requests (SARs), is clear, comprehensive and readily available to all staff on the Legal SharePoint Page.
- ▶ The Council has a documented process in place for reporting a data breach, the Information Security Data Breach Incident Reporting Management Policy, which requires that any suspected breaches are

reported to the DPO, who tracks all breaches within a Breach Record spreadsheet. While no breaches have been reported to the ICO since 2022, per the DPO's Breach Record, there have been nine minor breaches within the last year. We reviewed a sample of two of these and confirmed the correct data breach reporting and response procedure was followed, with the risk and impact assessed and appropriate remedial actions taken.

- ▶ The Council has a dedicated process in place for performing Data Privacy Impact Assessments (DPIAs) and provides a template for completing these. We reviewed the only DPIA completed in the last year for a Service Level Agreement with Southend Borough Council for the provision of burial services, and confirmed this was completed adequately. The responsible officer's assessment was reviewed by the DPO, who completed an assessment against the six principles of data protection, for which all areas were RAG-rated Green.



AREAS OF CONCERN

During our review, the following areas of improvement were identified:

- ▶ Although a centralised Record of Processing Activities (RoPA) is in place, our review found that this lacked sufficient detail to allow for accurate oversight of data processing activities, which could lead to ICO guidance not being met and an increased risk of a breach of existing data protection regulation. **(Finding 1 - Medium)**
- ▶ The RoPA does not clearly provide visibility on the Council's exposure to third party data transfers and, therefore, confirmation on whether the applicable data sharing agreements and/or international data transfer safeguards are in place. **(Finding 2 - Medium)**
- ▶ The Council's mandatory Data Protection training is comprehensive; however, as of December 2024, completion rates are 81% and 16% for staff and Members respectively. Training should have been completed by April 2024, and compliance is not being monitored and enforced adequately per meeting minutes reviewed for ELT. Furthermore, we noted that only one DPIA was completed at the Council in 2024, which may indicate that there is lack of knowledge and understanding regarding when to conduct a DPIA. While staff are informed about when a DPIA should be completed within the Data Protection e-learning, the training material and/or post-training assessment does not highlight examples of when a DPIA should be considered. **(Finding 3 - Medium)**
- ▶ We reviewed a sample of seven Subject Access Requests (SARs) and Freedom of Information (FOI) requests and found that three samples highlighted issues with the responses provided. For two of our SAR samples, no justification was provided for extending the response time beyond one calendar month and for one of our FOI samples, the Subject was not provided with a justification for delays outside of the 20 working day response time. **(Finding 4 - Low)**



CONCLUSION

We have raised three medium priority recommendations and one low priority recommendation to improve the Council's data protection controls for ensuring compliance with the requirements of the UK GDPR.

We recognise the Council have been through a significant journey of improvement regarding GDPR compliance. Therefore, we expected to identify gaps in the control environment and/or its effectiveness. As part of our conclusions drawn, we also consider the positive and effective commitment the Council have to this area in the coming months to continue

improving arrangements. The level of progress made by the Council to improve arrangements is commended.

We have highlighted the Council's RoPA as a medium finding due to the design being in line with ICO guidance, however it is not effectively completed at this point. This is a crucial aspect for ensuring that the Council complies with UK GDPR. As per finding 1, improvements need to be made to ensure that this contains the required information to record the Council's data processing activities.

The Council are aware of this, and our position is that if improvement is not made within the coming months, this would change our view to a Limited Opinion as prompt action is required. However, at this point we are content and expect progress to continue and therefore are content with a Moderate Opinion.

Control Design


We rated the design of the controls as moderate as there is generally, a sound system of internal control in place, however some weaknesses were identified, primarily with the issues identified with the RoPA in Finding 1. The RoPA is key to ensuring compliance with legislation and data protection principles such as transparency, lawfulness, and data minimisation. Furthermore, there were issues identified with the lack of up-to-date details on the information sharing arrangements the Council has with third parties.

Control Effectiveness

We have concluded moderate assurance over the effectiveness of the controls as we found evidence of non-compliance with some controls in our testing. This can be seen with the individual departments not having individual RoPAs in place in addition to the training compliance and the gaps identified with the response times for FOIs and SARs.

DETAILED FINDINGS

1 Record of Processing Activities

TOR Risk:	If the Council does not monitor its compliance with the requirements of data protection legislation and regulations, there is a risk that personally identifiable information may not be stored correctly, may be kept without sufficient legal basis or consent, or may be erroneously released into the public domain, leading to harm or distress for individuals and potential negative media or regulatory intervention.
Significance	 Medium



FINDING

The UK GDPR contains explicit provisions about how any organisation's processing activities should be documented and monitored. Data controllers must maintain a Record of Processing Activity (RoPA) in line with the requirements of the UK GDPR Article 30, which should set out all personal data processing activities that an organisation undertakes. For each data processing activity, the organisation must state what information is being processed by the organisation and why, the legal basis for processing this information, the specific retention periods that will be applied, and any data sharing arrangements. This is separate from an Information Asset Register (IAR) which records all information assets that an organisation possesses. The RoPA must be made available to the ICO upon request.

The Council has a central RoPA which includes the following information:

- Director
- Department
- Owner
- Date reviewed (due dates are not provided, and most entries are showing as overdue for review)
- Description of data processing (ie what is the processing activity)
- Classification (official vs official-sensitive, where official-sensitive denotes personal data)
- Lawful basis for processing ie consent, contract, legal obligation, public task, or vital interest (noting that legitimate interests are not specified)
- Location (ie data held on internal and/or external systems)
- Security measures in place (we note that there are gaps for many entries)
- Whether data is transferred out of EU (the RoPA does not indicate whether data is transferred to other jurisdictions)
- Was a DPA required / completed.

It should be noted that the objective of a RoPA is to detail all personal data processing activities. We have noted that the Council's central RoPA has been developed to include both the RoPA and Information Asset Register requirements, and therefore includes non-personal information, which detracts from focusing on GDPR requirements in relation to personal data.

We found that various pieces of expected information were missing for entries within the RoPA. While it cross-references to the Council's retention schedule, it does not state the specific retention periods that will be applied to data being processed by the Council. The RoPA does not outline who the data subjects are, the types of data being collected, and does not differentiate between activities which require processing under Article 6 and Article 9 (the latter is special category data, which requires an additional reason for processing). Furthermore, instances where data is shared with third parties (and, if so, where) are not adequately reflected in the RoPA (please Finding 2 for further details).

We have been informed by the DPO that the RoPA was last reviewed in April 2024, although this has not been subject to a complete review to account for individual departments. While the DPO has met with individual department heads to endeavour to understand the data processing activities in place across the Council, RoPAs are not collated and managed by the individual departments due to a lack of understanding regarding how to update and maintain RoPAs at this level. Individual departments therefore do not document their processing activities and the central RoPA maintained by the Council is high level.

A RoPA also helps the Council to comply with Principle (a) of UK GDPR in that it defines how the Council is processing information lawfully and transparently. The Council has a General Privacy Statement and five separate privacy notices that are published on its website. While each notice has clearly defined sections including what personal data is collected, why, how this is used, and how this is protected, there is lack of clarity around how long this data is retained for, and notice review dates are not provided. In conjunction with this, the lack of an appropriately defined RoPA increases the risk that the Council has not considered all data processing activities and retention periods within each privacy notice and may therefore not be complying with Principle (a).

We noted that the Council have started work on amending the existing RoPA so that it is in line with ICO guidance and consultations with business units have started in March 2024 to support this.

Where a RoPA is not adequately completed or maintained, there is a risk that the Council does not have a full understanding of what information it holds, why it holds it, what it is used for and how it is processed, which in turn can lead to information assets being inappropriately managed or not in line with the requirements of the UK GDPR.



RECOMMENDATION

- a) Management, in conjunction with each individual business unit or department, should conduct a full and comprehensive review of all information processing activities that are undertaken by individual departments. With regard to personal data, this information should be captured within a dedicated RoPA, and these should capture, at a minimum, the information identified as missing by this review. The updated RoPAs should be presented to and approved by Senior Management.
- b) Following this understanding of data processing activities at the service department level, the Council should revise the centrally defined RoPA and ensure that this captures all the Council's data flows and processing activities. This should be completed and updated on an ongoing basis and there should be arrangements for it to be fully reviewed on at least an annual basis to ensure that it remains current and appropriate.
- c) As part of the RoPA review, the Council should consider reviewing the existing privacy notices and updating them in case of any changes to data processing activities, to ensure continued transparency of data processing with data subjects. The Council should ensure that its privacy notices provide clarity on retention periods (even if only indicative timelines) and review dates (ie date notice was last reviewed, date of next review, frequency of review).



MANAGEMENT RESPONSE


The Council accepts the recommendations and would like to thank the auditors for their assistance in providing a compliant template for the Council's ROPA.

On receipt of this document and the draft report the Council immediately began updating the ROPA and quickly populated the new format with information that was already held and this process is in the final stages of completion. Individual Departments are now reviewing the current draft to confirm accuracy and completeness.

As part of the ROPA update all departments will consider if they have adequate Privacy Notices in place to cover specific areas which are not covered by the Council's general privacy notice. All current notices will be amended to include a date and review date for ease of monitoring. The Data Protection Officer will monitor this compliance.

Responsible Officer:	Data Protection Officer
Implementation Date:	31 August 2025

2 Third Party Data Sharing

TOR Risk:	If the Council has insufficient or ineffective procedures in place for managing data breaches, Data Protection Impact Assessments (DPIAs), data sharing or data subject rights requests, there is a risk of a potential failure to comply with the provisions of UK GDPR, and that personal or sensitive information may not be prevented from release into the public domain, resulting in reputational, legal and financial consequences for the Council.
Significance	 Medium



FINDING

As per the requirements of the UK GDPR, where data is shared with a third party, appropriate clauses should be in place between a data controller and data processor (including instances where the Council is a joint data controller) to protect a data subject. Due diligence checks and risk assessments should be undertaken to determine what risks are posed where data is shared with third parties (and how these risks are being mitigated). RoPAs should outline instances where data is being shared with third parties, including how the Council ensures appropriate safeguards if sharing personal data with a third party (via data sharing agreements) located in both a local or international jurisdiction.

Regarding the Council's procurement processes, the standard terms and conditions contain Data Protection and Data Sharing clauses as part of due diligence procedures. Furthermore, the Council's data protection policy states that processing activities undertaken by a third party should be subject to a specific contract, a data sharing agreement (DSA), which states how the processing complies with data protection legislation and the Council's policy. We have reviewed an example DSA in place with Essex Police which states the reasons for why information is being shared in addition to the security measures in place to safeguard the data. However, we found that the RoPA does not clearly indicate activities where data is being shared with a third party and, therefore, where applicable, DSAs are not being recorded within the Council's RoPA to ensure that there is clarity over whether data is being shared with third parties, the purposes for sharing this data, and that the Council is meeting its responsibilities under UK GDPR. The DPO has a list of DSAs with third parties, however this does not state when these agreements were signed and which activities these DSAs affect. Furthermore, the DPO has noted that the list contains only the agreements that they are aware of, and the existing agreements are not reflected within the Council's central RoPA.

The lack of clarity within RoPAs regarding third party data sharing, including where data may be being shared (ie in which jurisdiction) increases the risk that the Council is not aware of which sensitive information may be subject to release in the public domain, which in turn can lead to data breaches, inadequate data protection, excessive data transfer, and subsequent reputational and legal consequences for the Council.



RECOMMENDATION

For any third-party data transfers, the Council should ensure that these are being recorded within the applicable RoPA and that appropriate safeguards, such as Data Sharing Agreements, are in place. Arrangements should be made to ensure that the information sharing arrangements are subject to review on a regular basis.



MANAGEMENT RESPONSE


The Council is satisfied that it has data sharing agreements in place with those relevant organisations it regularly shares data with. The Council accepts that these were not all set out within the ROPA document.

The current review of the ROPA being undertaken (see above) will include the addition of third-party data transfers. This will ensure that the records are accurate and up to date.

The annual review of the ROPA will ensure that this continues.

Responsible Officer:	Data Protection Officer
Implementation Date:	31 August 2025

3 Mandatory Data Protection Training

TOR Risk:	If roles and responsibilities of members of staff for data protection are not adequately defined and communicated, there is a risk that robust data governance will not be implemented, leading to potential loss of personal or commercially sensitive information or non-compliance with data protection regulations.
Significance	 Medium



FINDING

Mandatory training is a key mechanism for communicating expected behaviours, responsibilities, frameworks, policies, and procedures. All staff and Members (councillors) are required to complete Data Protection e-learning upon joining the Council, and annually thereafter as a refresher.

As part of a suite of mandatory training, the Council has a dedicated Data Protection mandatory training e-learning module which covers key topics such as definitions, the Data Protection principles, Subject Access Requests, Data Privacy Impact Assessments, transfers of personal data, responsibilities including the role of the Data Protection Officer, and breaches. Staff are required to undertake the training upon joining the Council and annually thereafter. The training is deemed completed following a test of knowledge at the end to consolidate learning and achieve a pass mark of 100%.

The Data Protection e-learning for 2024/25 was rolled out on 8 March 2024, and was required to be completed by all staff within six weeks.

- As of October 2024, the compliance rate for staff across the Council was 79% (this had risen to 81% in December 2024)
- As of December 2024, 16% of Members (elected councillors) had completed the Data Protection 2024 refresher training.

Managers are required to follow up with staff in their teams who have not completed the mandatory training (per the Council's management reporting tool, the Balance Scorecard on PowerBI, managers can view the individual staff members who have not completed the training). While the training is mandatory for all staff and members, it is unclear whether this is enforced and monitored for members.

Regarding monitoring and enforcement, there is monthly reporting to the Extended Leadership Team (ELT) on compliance with mandatory training, which is a key performance indicator (KPI) on the Balance Scorecard:

- Per September 2024 ELT meeting minutes, completion was flagged as below target across the different services, and a colleague demonstrated how to identify staff who have not completed their e-learning, reminding teams to do this. Poor completion was also flagged in October 2024 per ELT minutes, however not in November 2024. It is unclear which remedial actions, if any, were implemented to increase compliance rates.
- KPIs should be reported by-exception to the Corporate Leadership Team (CLT) and Performance, Governance and Audit Committee where they have failed targets for three or more months. However, we found that poor training completion has not been escalated to the CLT (minutes reviewed for August, September and October 2024) or Performance, Governance and Audit Committee (minutes reviewed for June and September 2024).

If Data Protection training is not completed, there is a risk that staff and Members do not understand the Data Protection principles and their roles and responsibilities in relation to these.

Data Privacy Impact Assessments

While it is not expected that all staff should be responsible for completing a DPIA, it is good practice that staff can identify situations where a DPIA should be considered, in case a processing activity poses a high risk to the rights and freedoms of an individual. We note that only one DPIA has been completed in 2024; there was no issue with how the DPIA was completed, however the small number of DPIAs may indicate that there is lack of knowledge and understanding regarding when to conduct a DPIA.

Although all staff are informed about when a DPIA should be completed within the Data Protection training material, the training material and/or post-training assessment should also highlight examples of when a DPIA should be considered. Not having applicable coverage for when a DPIA is required to be completed can contribute to either unnecessary assessments being conducted, or necessary ones being missed.

Should staff not be able to identify instances of when a DPIA is required, this increases the risk that the Council may not fully understand the risks associated with data processing activities, which in turn increases the likelihood and impact of data breaches and regulatory non-compliance.



RECOMMENDATION

- a) Where staff and Members have not completed the mandatory refresher Data Protection training, the Council should investigate reasons for non-completion (including any possible barriers to completion) and implement remedial actions as required (for example, explore whether training can be delivered in another format).
- b) As Managers are required to follow up with staff in their teams who have not completed the mandatory training, Assistant Directors should follow up with managers to ensure that staff in their teams who have not completed the training do so as soon as possible.
- c) While poor completion has been noted at ELT as part of management reporting KPIs in the Balance Scorecard, KPIs should be escalated to CLT and Performance, Governance and Audit Committee where they have failed targets for three or more months, with remedial actions identified.
- d) The Council should ensure that Members complete the mandatory refresher Data Protection training, and that this is enforced and monitored going forward.
- e) Management should review and, where necessary, update the Council's training module so that it includes:
 - Further details on the expectations, roles and responsibilities of staff around DPIAs. The training material and/or post-training assessment should also highlight examples of when a DPIA should be considered, for example if a processing activity poses a significant risk to data subjects such as CCTV implementation.
 - FOI requests should be covered as part of the mandatory Data Protection e-learning in addition to SARs.
- f) As part of the RoPA review, the Council should retrospectively review all data processing activities, to determine whether a DPIA may be required.



MANAGEMENT RESPONSE

The Council has a comprehensive training programme across a large number of areas. This programme is rolled out annually and we will review the Data Protection and FOI Training with this annual review.


The Data Protection Officer has provided ad hoc and additional training where it has been requested by teams across the Council where a need has been identified and will continue to provide this opportunity. Staff have also received training on the internal systems to process FOI requests. This system provides standard responses to assist in compliance with our legal requirements.

Assistant Directors regularly monitor compliance with all training requirements. Any non-compliance will be raised with individual staff. The Council's balance scorecard is monitored by CLT and areas of concern are addressed.

Councillors will be reminded of the importance of the training and will be asked to complete the training as soon as possible.

Responsible Officer:	Data Protection Officer
Implementation Date:	April 2026

4 Subject Rights Requests

TOR Risk:	If the Council has insufficient or ineffective procedures in place for managing data breaches, Data Protection Impact Assessments (DPIAs), data sharing or data subject rights requests, there is a risk of a potential failure to comply with the provisions of UK GDPR, and that personal or sensitive information may not be prevented from release into the public domain, resulting in reputational, legal and financial consequences for the Council.
Significance	 Low



FINDING

Under the Data Protection Act 2018, any individual can ask to see a copy of any information held on them (Subject Access Request); the Council has one calendar month to respond (or an extra two calendar months to respond to complex requests, informing the requestor that there will be a delay before the end of the first calendar month). Under the Freedom of Information Act 2000, individuals have a general right of access to all types of recorded information held by most public authorities; the Council has 20 working days to respond to a Freedom of Information request.

We reviewed a sample of Subject Access Requests (SARs) and Freedom of Information (FOI) requests. We found that these were responded to appropriately and in a timely manner for most of our samples. We identified the following areas for improvement:

- The Council received four SARs in the last 12 months, and we reviewed a sample of two. For one sample, the one calendar month window commenced on 12 August 2024, and the Subject was emailed on 10 September 2024 that their data would be ready for collection on 9 October 2024. While this is outside the 1 calendar month window, the Subject was informed of progress on 10 September, ahead of the deadline (which would fall on 11 September 2024), therefore this is not considered overdue by the DPO. However, the Subject was not provided a justification for the extension (ie that this was a detailed request, which required more time).
- The Council received 272 FOIs in the last 12 months, and we reviewed a sample of five. For one of the FOIs in our sample, the 20-working days response window was not met, and this was not a complex request. A discussion with the DPO indicated that this was likely due to lack of staff in the Planning team. However, the individual was not kept informed that their request would be delayed and of the reason(s) for this, as is required by the FOI Act.

Since August 2024, the Council uses the Freshservice management system to manage SARs. This allows for 'tickets' to be raised by any colleague that receives a SAR (ie the DPO or another officer) so that a caseworker can take this forward and collate the request (the DPO has created a template for caseworkers to use to collate a request across different departments). Although since August 2024 procedure requires SARs to be recorded via Freshservice requests, there is a risk that all requests are not centrally logged/tracked, particularly for any historical SARs. We have been informed that, to help keep track of all SARs going forward, these will be logged by the DPO in a centralised spreadsheet, which we have reviewed. Furthermore, there are no policies or procedures to help staff with processing FOIs. Although training has been provided to staff in March 2024, it is helpful to have procedures in place to ensure that staff can respond to requests in a timely manner.

Where FOI and data subject right requests are not responded to within the timeframes required by the FOI Act and the UK GDPR respectively, there is an increased risk of non-compliance with regulatory requirements and financial and reputational harm to the Council.

**RECOMMENDATION**

- a) To help staff, the Council should compile a brief procedure note on completing FOIs (particularly because FOIs are not covered as part of the mandatory Data Protection e-learning).
- b) The Council should ensure that SARs and FOIs are responded to within a timely manner, with the subject kept informed throughout in case of any delays and provided a justification for any extensions.
- c) As already noted by the DPO, going forward, all SARs should be logged in a centralised spreadsheet. The Council may also wish to review any FOIs to ensure that these are not historical SARs.

**MANAGEMENT RESPONSE**

The Council exceeds its target for responding to FOI's and this is managed through the Dash System. A procedural note has been drafted to allow staff to respond to requests. The Dash system monitors timeframes and prompts staff where the 20-day deadline is approaching to ensure compliance.

The Council receives a very small number of requests every year on average 2/3 requests. These requests are now logged and managed in one location to ensure compliance with timeframes and to ensure customers are advised where delays are expected.

Responsible Officer:	Data Protection Officer
Implementation Date:	May 2025

APPENDIX I - DEFINITIONS

LEVEL OF ASSURANCE	DESIGN OF INTERNAL CONTROL FRAMEWORK		OPERATIONAL EFFECTIVENESS OF CONTROLS	
	FINDINGS FROM REVIEW	DESIGN OPINION	FINDINGS FROM REVIEW	EFFECTIVENESS OPINION
Substantial	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally, a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non-compliance with some controls, that may put some of the system objectives at risk.
Limited	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non-compliance and/or compliance with inadequate controls.

RECOMMENDATION SIGNIFICANCE

High	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

APPENDIX II - TERMS OF REFERENCE



KEY RISKS

Based upon the risk assessment undertaken during the development of the internal audit operational plan, through discussions with management, and our collective audit knowledge and understanding the potential key risks associated with the area under review are:

- ▶ Risk 1: If the Council has not defined adequate policies and procedures for the management of its information, there is a risk that information will not be controlled or processed by the Council in accordance with the requirements of UK GDPR, leading to potential regulatory intervention, fines, and loss of personal or commercially sensitive information.
- ▶ Risk 2: If roles and responsibilities of members of staff for data protection are not adequately defined and communicated, there is a risk that robust data governance will not be implemented, leading to potential loss of personal or commercially sensitive information or non-compliance with data protection regulations.
- ▶ Risk 3: If the Council does not monitor its compliance with the requirements of data protection legislation and regulations, there is a risk that personally identifiable information may not be stored correctly, may be kept without sufficient legal basis or consent, or may be erroneously released into the public domain, leading to harm or distress for individuals and potential negative media or regulatory intervention.
- ▶ Risk 4: If the Council has insufficient or ineffective procedures in place for managing data breaches, Data Protection Impact Assessments (DPIAs), data sharing or data subject rights requests, there is a risk of a potential failure to comply with the provisions of UK GDPR, and that personal or sensitive information may not be prevented from release into the public domain, resulting in reputational, legal and financial consequences for the Council.



SCOPE & APPROACH

The following areas will be covered as part of this review:

- ▶ Assess whether there is a governance framework in place to support compliance with data protection responsibilities, including defined, approved and up to date policies and procedures. (Risk 1)
- ▶ Determine whether roles and responsibilities with regards to data protection are defined and whether there is a training programme in place for data protection and information management for staff which is regularly refreshed. (Risk 2)
- ▶ Assess whether the Council has a Record of Processing Activities in place and that this is regularly reviewed and updated and captures appropriate information. (Risk 3)
- ▶ Assess whether the Council has defined retention periods in place for held information and that this is adhered to. (Risk 3)
- ▶ Determine whether the Council has defined the lawful basis for collecting, processing, retaining, and sharing information and assess whether this is transparent to data subjects using tools such as privacy notices. For special category data, assess whether the reasons for processing are appropriate and in line with the original purpose of the processing activity. (Risk 3)

- ▶ Assess whether there is regular monitoring of the Council's compliance with data protection legislation and regulations by senior management, including the identification, assessment, and remediation of risks. (Risk 3)
- ▶ Assess whether there are procedures in place to deal with data subject rights requests, including Subject Access Requests (SARs), Freedom of Information Act requests (FOIs) and the exercising of rights by individuals. Determine the extent to which these requirements are complied with, responded to, monitored, and reported on. (Risk 4)
- ▶ Assess whether adequate and effective data breach response procedures are in place. We will select a sample of recent data breaches to determine whether:
 - Internal and external reporting processes were accurately followed.
 - Risks and impacts arising from the data breaches had been assessed and mitigated to prevent harm to individuals.
 - Lessons learned had been discussed and documented.
 - Actions have been implemented to prevent recurrence and these are monitored on a regular basis. (Risk 4)
- ▶ Assess whether there are adequate procedures in place for performing DPIAs for the processing of data which is likely to present a high risk to the rights and freedoms of individuals. (Risk 4)
- ▶ Where the Council shares personal data as part of its relationships with third parties, determine whether the risks posed by these relationships have been assessed and whether data sharing agreements have been implemented to mitigate these risks. (Risk 4).

The scope of the review is limited to the areas documented under the scope and approach. All other areas are considered outside of the scope of this review. However, Internal Audit will bring to the attention of management any points relating to other areas that come to their attention during the audit.

We assume for the purposes of estimating the number of days of audit work that there is one control environment, and that we will be providing assurance over controls in this environment. If this is not the case, our estimate of audit days may not be accurate.

In delivering this review BDO may need to observe and test confidential or personal identifiable data to ascertain the effective operation of controls in place. The organisation shall only provide the Shared Personal Data to BDO using secure methods as agreed between the parties. BDO will utilise the data in line with the Data Protection Act 2018 (DPA 2018), and the UK General Data Protection Regulation (UK GDPR) and shall only share Personal Data on an anonymised basis and only where necessary.

FOR MORE INFORMATION:

Aaron Winter

Aaron.Winter@bdo.co.uk

The matters raised in this report are only those which came to our attention during the course of our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO Member Firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

Copyright © 2025 BDO LLP. All rights reserved.