# MALDON DISTRICT COUNCIL

## INTERNAL AUDIT REPORT (DRAFT)

INFORMATION MANAGEMENT
NOVEMBER 2020

| LEVEL OF ASSURANCE | |
|---|---|
| Design | Operational Effectiveness |
| Moderate | Moderate |

IDEAS | PEOPLE | TRUST

BDO

| DISTRIBUTION | |
|---|---|
| Chris Leslie | Director of Resources |
| Annette Cardy | Resources Specialist Services Manager |
| Emma Holmes | Data Protection Officer |
| Grant Hulley | Senior ICT Specialist |

| REPORT STATUS LIST | |
|---|---|
| Auditors: | Awais Farooq – IT Auditor |
| Dates work performed: | 19 October 2020 – 5 November 2020 |
| Draft report issued: | 01 October 2020 |
| Final report issued: | 17 December 2020 |

## EXECUTIVE SUMMARY

### LEVEL OF ASSURANCE: (SEE APPENDIX I FOR DEFINITIONS)

| | | |
|---|---|---|
| Design | Moderate | Generally a sound system of internal control designed to achieve system objectives with some exceptions |
| Effectiveness | Moderate | Evidence of non-compliance with some controls, that may put some of the system objectives at risk. |

### SUMMARY OF RECOMMENDATIONS: (SEE APPENDIX I)

| | |
|---|---|
| High | 0 |
| Medium | 2 |
| Low | 0 |

### TOTAL NUMBER OF RECOMMENDATIONS: 2

### CRR/BAF REFERENCE:

CRR11 :- Failure to protect personal or commercially sensitive information

### BACKGROUND:

The management and use of information has become more important as both the expectations of information governance and the service expected by customers get more demanding. Getting the use and management of information right has a significant part to play in the delivery of the Council's expectations and strategic objectives.

As well as being a key requirement for compliance with the General Data Protection Regulation (GDPR), maintaining a record of processing activities and information assets gives the Council oversight of its high risk instances of data processing, allowing it to take a risk-based approach when investing in security controls to secure its most critical assets.

The Council maintains both physical and digital records holding personal confidential information and has a duty to manage these records effectively. The Council could incur financial and reputational damage when information is found to have been poorly managed.

A GDPR compliance audit carried out in June 2019 provided substantial assurance over the design of the Council's GDPR compliance controls and moderate assurance over their operational effectiveness. The audit identified that improvements were required to ensure that the Council's information asset register is in line with the requirements of the GDPR.

Historical paper records are stored in-house, in two storage rooms located at the Council Offices. The Human Resources Department has separate storage arrangements due to the confidential nature of the HR records. Responsibility for the retention or disposal of information rests ultimately with the individual Heads of Service.

The purpose of this audit was to assess the design and effectiveness of the Council's information management controls and the processes for the storage, retention and destruction of paper documents to support compliance with the Council's retention schedule and current legislation.

## GOOD PRACTICE

Good practice was evidenced in the following areas:

- The Council has identified and recorded its information assets and has a defined Information Asset Register (IAR) in place, which was last reviewed in May 2020. At the time of the audit, the IAR was found to include details relating to 90 information assets, including the information asset owner, location, last review date and the lawful basis for processing the information asset. The IAR also includes a tracker for the number of days to the next scheduled review date and a validation sheet pointing to the documentary evidence relating to the individual assets reviews.
- The Council has arrangements in place for ensuring that the principle of least privilege is exercised and that information is only accessible and available to those that have a valid business need. There are secure storage facilities for the retention of paper documents and the Council has documented the security measures and storage controls for each information asset as part of its information asset register.
- The Council has a document retention schedule in place, which was last reviewed in February 2020. The retention schedule includes defined and enforced mandatory minimum retention periods, which are based on Information and Records Management Society guidelines, the Council's requirements and are in line with current legislative and regulatory requirements. Through discussions with information asset owners, we confirmed awareness of the retention schedule and maintenance of appropriate records of all information kept in on-site storage facilities for archiving purposes.
- There are defined procedures in place for the disposal and destruction of information, which include identification, recording and authorisation procedures and there are appropriate on-site facilities for confidential waste and for the storage of confidential information. Confidential waste is securely shredded once a week on site by Shred Station, an external contractor, in line with the Council's defined procedures.

## KEY FINDINGS:

We identified the following areas of improvement:

- The Council's Document Retention and Data Protection policies were found to be out of date at the time of the audit and do not include the procedures for the management of the Council's digital records (Medium – Finding 1)
- The Council has not defined and communicated the responsibilities of information asset owners (Medium – Finding 2).

## CONCLUSION:

Based on our review we have raised two medium level recommendations to improve the Council's information management arrangements.

Overall, the Council has a sound system of internal controls and maintains an appropriate document retention schedule and information asset register. However, the absence of defined responsibilities for the information asset owners and the gaps identified in the Council's information management policies and defined procedures could undermine its ability to manage information assets appropriately and in line with current legislation.

Consequently, we conclude moderate assurance over both the design of the Council's information management controls and their operational effectiveness.

## DETAILED FINDINGS

RISK: THE COUNCIL DOES NOT HAVE APPROPRIATE POLICIES AND PROCEDURES IN PLACE FOR INFORMATION GOVERNANCE AND RECORD MANAGEMENT

| Ref | Significance | Finding |
|---|---|---|
| 1. | Medium | Document Retention and Data Protection Polices<br><br>The Council has a Document Retention Policy in place, which provides a corporate framework for governing management decisions on retention and disposal of paper and other non-digital records. The Council also has a Data Protection Policy in place to ensure that personal information held by the Council is treated lawfully, in an accountable manner and in compliance with the Data Protection Act 2018.<br><br>However, both policies were found to be out of date at the time of the audit and were last reviewed in February 2018. Whilst the Document Retention Policy has been presented to the Strategy and Resources Committee in November 2020, we found that the Data Protection Policy has not been reviewed.<br><br>Where information management policies are incomplete or out of date there is an increased risk that the Council's information will not be managed in line with its strategic objectives, best practice and current legislation and regulations. |

RECOMMENDATION:

1.1. Management should review and update the Council's Data Protection Policy to ensure that it remains in compliance with the Data Protection Act 2018, is relevant to the Council's needs and is in line with the Council's strategic objectives.

1.2. The revised policies should be approved and communicated to members of staff and arrangements should be put in place for reviewing the policies on a routine basis.

MANAGEMENT RESPONSE:

Agreed in principle during audit closing meeting with Emma Holmes (Data Protection Officer) and Annette Cardy (Resources Specialist Services Manager).

The Document Retention Policy was approved by the Council's Strategy and Resources Committee on 24 November 2020.

Details of revised policies will be provided to all managers and staff.

Policies will be reviewed annually.

Responsible Officer: Emma Holmes, Data Protection Officer

Implementation Date: 31 March 2021

| RISK: | THE COUNCIL DOES NOT HAVE APPROPRIATE POLICIES AND PROCEDURES IN PLACE FOR INFORMATION GOVERNANCE AND RECORD MANAGEMENT | |
|---|---|---|
| Ref | Significance | Finding |
| 2. | Medium | Responsibilities of Information Asset Owners<br><br>The Council has a defined information asset register in place, which identifies the information asset owners for each of the Council's information assets.<br><br>However, we found that the responsibilities of the information asset owners have not been defined and communicated to the relevant members of staff and there is no requirement in the Council's information management policies for the information assets to be reviewed on a regular basis by the information asset owners.<br><br>Where the responsibilities of information asset owners have not been defined and communicated there is an increased risk that the Council's information will not be managed in line with its strategic objectives and best practice. |

RECOMMENDATION:

2.1. Management should define the responsibilities of information asset owners, which should include, but not be limited to:

- Knowing who has access to the information assets and why
- Monitoring access to information assets and maintaining a log of access requests made
- Reviewing risks to the confidentiality, integrity and availability of the information assets on at least an annual basis
- Approving and minimising the transfer of the assets
- Ensuring that the assets are appropriately protected and that their value to the Council is fully exploited.

MANAGEMENT RESPONSE:

Agreed in principle during audit closing meeting with Emma Holmes (Data Protection Officer) and Annette Cardy (Resources Specialist Services Manager)

Detailed Guidance notes on responsibilities and policies will be provided to all IAO setting out their role and responsibilities.

The Council began an annual review of the Information Asset Register in 2020 and this will continue. Data Protection Officer will require confirmation that these have been reviewed.

Responsible Officer: Emma Holmes, Data Protection Officer

Implementation Date: May 2021

# OBSERVATIONS

## CONFIDENTIAL WASTE CONTRACT WITH SHRED STATION

The destruction of confidential waste is managed by Shred Station, an external third party, which carries out weekly on-site shredding of all confidential documents and archived documents that have reached their destruction date. The contractor provides the Council with a collection note at each visit, identifying the number of bins collected for onsite destruction.

The confidential waste contract was put in place in January 2013 for an initial duration of two years and we observed that the contract has been rolled over annually since then, but has not been officially reviewed since its inception. We noted through discussions with management that the contract will be market tested at the end of the current financial year.

## DOCUMENT RETENTION- DIGITAL RECORDS

We found that the Document Retention Policy only defines the procedures for the management and retention of paper records and does not include the procedures relating to the management of the Council's digital records, including access controls, review and retention requirements and disposal arrangements.

The Council's Document Retention Policy was updated in December 2020 so that it defines the digital record management and retention procedures to ensure that digital records are subject to the same retention schedules and scrutiny as paper and other non-digital records: 'The retention schedule refers to all information, regardless of the media in which it is stored, i.e. manual files, computer files, tapes, microfiche, etc.'

## STAFF INTERVIEWED

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.

| | |
|---|---|
| Annette Cardy | Resources Specialist Services Manager |
| Emma Holmes | Data Protection Officer |

| 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

## PURPOSE OF REVIEW:

The purpose of this audit is to assess the design and effectiveness of the Council's information management controls and the processes for the storage, retention and destruction of paper documents to support compliance with the Council's retention schedule and current legislation.

## 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 key risks associated with the area under review are:

- The Council does not have appropriate policies and procedures in place for information governance and record management
- The Council does not have a full understanding of the information that it holds, why it holds it, what it is used for and its value
- Personal confidential information is not stored securely and access to information is not appropriately and effectively controlled
- Information and document retention is not compliant with the requirements of the GDPR and users cannot access information as and when it is required
- Information is not securely disposed of and/or destructed when it is no longer required.

## SCOPE OF REVIEW:

The following areas will be reviewed as part of this audit:

- Policies and guidance documents relating to information governance and records management, including the procedures for identifying, assessing and resolving data security breaches and for establishing the lawful basis for collecting, processing and storing personal information
- The Council's information asset register, which should classify the Council's information assets in line with governing regulations and should be reviewed on a regular basis
- The arrangements for ensuring that access to information is restricted only to those that have a valid business need and the storage facilities for the retention of paper records
- The Council's retention schedule, including the frequency with which it is reviewed and how compliance is monitored at Departmental level, and how members of staff are made aware of the Council's information and document retention requirements
- Whether there are appropriate on-site facilities for confidential waste and whether the contractual arrangements for the disposal and/or destruction of records are regularly reviewed and include information governance clauses.

However, Internal Audit will bring to the attention of management any points relating to other areas that come to their attention during the course of 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.

FOR MORE INFORMATION:

**Greg Rubins**

Greg.Rubins@bdo.co.uk