APPENDIX G

Internal Audit FINAL Report

Records Retention

Governance Opinion

Adequacy of System	Satisfactory
Compliance	Satisfactory
Organisational Impact of findings	Minor

Report Issued	19/08/2021
Audit Committee schedule	

Executive Summary

1. Background

1.1 The Council produces, receives and retains records that are both hard copy and electronic in the process of conducting its daily business. Records are retained in compliance with its statutory duty to comply with legislation and for its own business purposes.

1.2 Data retention law has changed as a result of the UK leaving the European Union. As of January 2021 UK organisations that process personal information need to comply with the UK General Data Protection Regulations (GDPR) and organisations are required to create a data retention policy to help manage the way personal information is handled and stored. The retention of sensitive information for too long even if stored securely and not misused may still be a violation of the regulations and requirements. No one piece of legislation explicitly requires a Retention and Disposal Schedule however the following legislation does make stipulation in relation to the retention of information:

- Information Management Service, Retention and Disposal Schedule April 2021 v6.0,
- Freedom of Information Act - code of practice Section 46 (FOIA),
- Data Protection Act 2018 (DPA18),
- The General Data Protection Regulations (GDPR),
- Public Records Act 1953.

1.3 A records retention policy should provide a set of guidelines that help the Council keep track of how long information must be kept and how and when information is destroyed when no longer required. The policy should also outline the purpose of processing the data in order to justify the data retention period.

1.4 The Lord Chancellor's Code of Practice for Records Retention provides guidance to English Councils on the types of records that could be kept for each service to ensure compliance with Section 12 of the code on the management of records to meet likely business needs and be compliant with legislative requirements.

The guidance describes how long records need to be kept before destruction or transfer to archives and shows the need to:

- Control the process to ensure it is compliant with legislation,
- Manage disposal in line with Data Protection Rules,
- Identify records containing personal or specific information quickly,
- Improve access to relevant documents and remove old ones,
- Reduce storage back-up systems,
- Improve access requests under the Freedom of Information Act and Environmental Information Regulations.

1.5 Corporate records including emails and attachments must be managed in accordance with the Council's retention policy, which has been recently refreshed (June 2021), and includes a specific email retention policy (June 2021).

1.6 All staff have a responsibility to comply with the Retention and Disposal Policy and Schedule in order to ensure the proper management of information throughout the life cycle and to evidence our commitment to fair processing. The Policy, Insight and Communications team must ensure there is support, advice and guidance to responsible service managers and to ensure corporate compliance with the retention schedule to meet the Councils business requirements and be fully compliant with legislation.

2. Scope of Audit and Approach

2.1 Scope

This audit sought to review the Council's Records Retention Policies and procedures to provide assurance that the Council's record retention arrangements are compliant and meets legislative requirements and best practice. The audit will check the robustness of record retention processes and management to provide assurance that:

- Retention schedules are complete and compliant.
- The Policy is being implemented correctly across the Council,
- Records are retained for the required duration, not retained for longer than required, are properly disposed of and are fully accessible to meet Freedom of Information and Environmental Information Regulations, and Data Protection Act requests to comply with the Information Commissioners Office requirements.
- Controls maintained in the Customer and Communities directorate ensure corporate compliance with the retention schedules.

2.2 Approach

The audit will be undertaken through review of documentation and records and discussion with team members, with testing to verify processes and effectiveness of controls. The audit process involved us: -

- Undertaking video interviews with relevant officers, to ascertain the procedures in place for managing risk;
- Evaluating whether the procedures in place provided for an adequate and effective level of control;
- Testing, where appropriate, that the controls identified were operating in practice;
- Reviewing procedures for efficiency and, where appropriate, identify opportunities to make improvements to processes.

2.3 Acknowledgment

We would like to thank all the members of staff consulted, for their assistance and co-operation during this review.

3. Internal Audit Opinion and Main Conclusions

3.1 Internal Audit Opinion

3.1.1 The assurance given to the system design is SATISFACTORY because systems operate to a moderate level with some control weaknesses that present medium risk to the control environment.

3.1.2 The assurance given for compliance is SATISFACTORY because the control environment has mainly operated as intended although errors have been detected that could be prevented/mitigated. The risks associated with the current use of manual processes (documents and spreadsheets) will be mitigated by moving to automated compliance. The O365 project work in progress with ICT colleagues.

3.1.3 The organisational impact of the findings is MODERATE because the weaknesses identified during the review have left the Council open to medium risk (medium impact on the organisation as a whole).

4. Main recommendations

Based upon the information provided and the test results,

a) Management should strengthen overarching governance on record retention, to ensure compliance and consistency across Council Services by developing a robust, embedded living automated records management system within the Office 365 environment. **(MAP 1).**

b) Consideration should be given to increase managers' awareness of the Record Retention requirements and their responsibilities and introduce periodic Record Retention specific training and record retention training for staff as part of the induction training. The work with ICT to implement an online solution will require colleagues to undertake training and review policies on a regular basis and on request to respond to issue -Meta compliance. **(MAP 2).**

c) Although training resources are already deployed and issues are reviewed as they arise, consideration should be given to strengthen the monitoring of corporate compliance and take appropriate corrective action where the policy and/or procedures are not being followed by Service managers, particularly in managing the destruction of records that are no longer required. **(MAP 3).**

d) Review the Document Retention Schedule to reflect the current functions and activities of the council and provide additional guidance to service managers on record retention requirements. Move to the IRM functional classification and build in SharePoint as a living EDRMS with automated retention and deletion schedules to be in line with best practice and legislation. **(MAP 4).**

Detailed Findings

4. Assurance Area – Policy & Procedures

Control Objective – to provide assurance that there is a Records Retention Policy in place and it is comprehensive and fit for purpose.

4.1 The Records Retention Policy has recently been approved by the Information Governance Board, having been updated in June 2021. A review date is also planned for 2024. The Policy is distributed to managers and is accessible to all staff on the shared drives. The Policy clearly defines roles and responsibilities for all staff across the Council.

4.2 The Record Retention Policy and Intranet Guidance (June 2021) is robust and covers information security, record retention, record destruction and archive schedules, and data protection/data sharing. The Policy is compliant with the legislative requirements of the Council and follows the guidance provided by the Information Commissioners Office (ICO).

4.3 Information on the intranet provides quick guide for all staff as to what files should be retained and for how long. Information is created and held for many reasons, some statutory e.g Audit, Finance, regulatory and business purposes, and are generally managed according to good practice guidelines. Record retention schedules enables staff to refer to and sets out what should be retained, for how long and whether to destroy or transfer the records when the retention is completed. There is reference to the Local Government Association interactive guidance tool for the retention of different types of files and MKC has subscribed to this guidance on the LG Inform website.

4.4 Records Retention guidance was maintained on a spreadsheet which shows a Corporate Retention Schedule of corporate file types. The detail on the worksheets showed Corporate File Types and that some information can be destroyed without reference to the Council's Record Retention Schedule; other records are retained permanently as historic archives; the schedule identifies the records to be preserved to archives. There is also an MKC Email retention Policy attached which details how long emails should be retained. A recent exercise to cull all emails over 1 year old has taken place to comply with the email retention policy.

4.5 The guidance specifically makes reference to the ICO Section 46 code of practice on record retention management and the Lord Chancellor's Code of Practice documents.

5 Assurance Area – Administration & Management.

Control Objective – To provide assurance that administration and management of record retention is robust and compliant with the Policy.

5.1 Three functions were selected from the MKC Retention Schedule for review:

1. **Administration** – including records in respect of customer complaints, Health & Safety Fire, Freedom of Information.
2. **Finance** - including records in respect of Payroll, Invoices and Budget.
3. **Information** – including records relating to Procurement and Emails.

5.1.1 **Administration** –

Records were being retained in compliance with the records retention schedule/Policy and were stored either directly by the system, on the shared drive or via email. Staff were aware of the Policy and the requirements although no specific training had been provided in this respect.
Record retention schedules were available for staff to refer to and sets out what should be retained, for how long and whether to destroy or transfer the records when the retention period has-expired.
There was reference to the Local Government Association interactive guidance tool for the retention of different types of files and MKC has subscribed to this guidance on the LG Inform website.
There is a large spreadsheet showing Records Retention guidance which shows a Corporate Retention Schedule of corporate file types, the reason for retention and the period of retention after which the records can be destroyed. There was also detail of Corporate File Types which shows that some information can be destroyed without reference to the Council's Record Retention Schedule; other records were retained permanently as historic archives; the schedule identifies the records to be preserved to archives. There is also an MKC Email retention Policy attached which details how long emails should be retained.

Archived documents are stored with Iron Mountain, a contractor commissioned to securely store and destroy the records on behalf of the Council. A monthly Iron Mountain report for April was reviewed and showed what records are stored at Iron Mountain and by which department. Destructions are carried out annually as per the destruction date on 31/3/year placed on each box by the manager putting the boxes into storage. Iron Mountain send the Facilities team a list of what has reached its destruction date by each department which is checked and then approval is given for the boxes to be destroyed as per the contract (not audited). Monitoring is carried out using a system called Techforge which holds all the information on.

Three administration areas were tested as follows:

a) Customer Complaints - The Customer Services Manager was contacted and provided evidence that Customer Service delivery complaints are recorded on Granicus Service through the "Contact Us" process aligned with MKC policy for managing official complaints - records are accessed by logging into the appropriate dashboard. Information communicated by email to one of the shared service inboxes were being retained in line with the MKC IT policy for the retention of emails. Complaints were being retained for 3 years as per the requirements. Access to records was found to be secure and controlled.

b) Health & Safety – for example Fire Safety - The Health and Safety team were contacted, and Internal Audit was shown how health and safety records are generated, received and stored. The process for how the team interacts with service managers who are responsible for their health and safety records was reviewed.

The Health and Safety Team receives and stores, for example, incidents and accidents reports. These are reported by employees via the Health and Safety section on the Council's staff intranet page. Once reported there is an auto-generated pdf document that is sent to the responsible manager and the Health and Safety Team in their team inbox. All incidents and accidents are logged by the Health and Safety team onto a password protected excel spreadsheet for capturing details from the reports, tracking required follow up actions, and for allowing for generation of statistical data. The incident and accident reports are retained indefinitely and are not deleted, but the Health and Safety team are faced with difficulties when copies of the pdf documents are requested as retrieval is a slow process from the inbox.

Any records that form part of an investigate carried out following an incident or accident are stored within the network P:/ drive in an investigations folder. Where reports are made under the requirements of RIDDOR, the records of these are also stored within the P:/ drive. In both cases, all information is retained indefinitely and is not deleted. The Records Retention Policy is being complied with in this aspect and records are retained according to and for various legislative requirements (i.e. RIDDOR and The Limitation Act).

Responsibility for retaining the health & safety forms/records sits with the responsible service manager. The Health & Safety team do carry out audits to ensure the health & safety requirements are being met and, where identified, ensure actions are followed up. Whilst there is reliance on the responsible managers to manage the retention of prime records, Managers are required to produce documents when requested/audited by the Health & Safety team and records are being produced when requested and therefore meet the requirements. Access to records was found to be secure and controlled.

c) Freedom of Information. Testing from the recent FOI audit showed records recorded on FIRSTEP are retained for a minimum of 2 years and are readily accessible to the FOI team. No evidence was provided regarding a destruction schedule but the FIRSTEP system data is managed in accordance with the guidelines. Records were found to be retained in compliance with minimum retention periods but reliance on systems purging and periodic file reviews rather than a structured destruction plan. Access to records was found to be secure and controlled.

5.1.2 **Finance**:- Finance records are retained for at least the minimum retention period in compliance with the Council's retention schedules. No hard copy records are kept other than the old hard copies pre-ERP that were archived. Destruction dates were noted on each box, but no monitoring has taken place. No formal regular review had been undertaken recently, of documents on the shared finance drive- the last review was 2 years ago. Records are retained in compliance with minimum retention periods but reliance on systems purging and periodic file reviews rather than a structured destruction plan. Records can be retrieved quickly, and staff are aware of storage locations and what is in storage. Access was found to be secure and is adequately controlled.

Electronically stored documents are retained for longer than the requirement and there is no structured control over the destruction of records that are not required. No training has been provided to the finance team on record retention. Finance records are retained on ERP, only records since 2018 retained so no purge has taken place (7 years) yet. No hard copies are retained.

Three Finance areas were tested as follows:

a) **Budget:** A Finance Business Partner was contacted, and evidence was provided that showed budget papers are held electronically, some are saved corporately, and others held by the service finance teams. No paper records are retained. Records are retained mainly to comply with statutory regulations and others are kept for business reasons. It was confirmed that Finance staff were familiar with the guidance but there was no formal process documented for the retention of records. Documents are held on the finance drive; paper copies were sent to storage several of years ago with destroy dates on them. No list of records in storage is available to finance staff but all records could be past the destroy date now. Documents are secure on the Finance drive and are easily accessed by finance staff with permissions. When the Finance drive was created two years ago a review of documents took place but there is no regular review of documents. Training on record retention is on induction for new staff on use of the Finance drive/folders but there is no specific training on retention of records. Budget papers are retained for 6 years, last purge 2 years ago i.e not regular. Records are held securely and can be retrieved quickly when required.

b) **Invoices:** Responsible officers in both Cambridge County Council and Milton Keynes Council were contacted. In Cambridge CC accounts payable invoices are system generated documents such as remittance advices and purchase orders which are retained in ERP. Records are retained for statutory purposes. Invoices received are scanned into pdf format and imported into ERP. Paper copies are retained until the reconciliation for imported invoices and images is completed c.24 hours, then they are destroyed. Training had been provided to those staff who open post and scan invoices regarding retention and reconciliation of data imported into ERP. No ERP data was migrated when the system went live in 2018 and data purge is scheduled for 7 years. Records are held securely and can be retrieved quickly when required.

c) **Payroll** – The HR Transactional Services Manager in West Northampton County Council confirmed that all payroll related information is retained for audit/statutory/regulatory and business reasons. Files are held on share point by West Northants Council or sent to document archive with a destruction date on them. HMRC data is kept for 4 years and pension information held indefinitely. Access to files is by restricted to preserve security. Share point and other files tested were not older than the required timescales. Training is provided by team leaders and is not formally delivered.

5.1.3 Information:

Of the two areas tested there were formal regular review of shared drive documents. Records are retained in compliance with minimum retention periods but there is a reliance on systems purging and periodic file reviews rather than a structured destruction plan. Records can be swiftly recovered from storage and staff are aware of storage locations and what is in storage. Access was found to be secure and is adequately controlled.

Electronically stored documents are retained for longer than the requirement and there is no structured control over the destruction of records that are not required. No training has been provided

Two areas were tested as follows:

a) **Procurement:**

It was confirmed that records are retained electronically but are not formally controlled in terms of their destruction. Staff had not received any training on records retention, and all documents were pertaining to an individual tender including emails approvals, tender specifications terms & Conditions, evaluations and award decisions were being retained. Records were retained for business reasons.
There was no direct control of documents retained and not destroyed. Instead, these were archived within project folders saved locally on shared folders on the :L drive and on the e-Tendering portal provider platform.
As at the date of the Audit, there was no record of retention or destruction dates on the project folders. Access to the folders is limited to the procurement team. There has been periodic destruction of tender docs that are 10+ years old but the review is not a regular task, more like an annual review of files on the local drive folders. Monitoring is limited as there is no formal structure for the destruction of documents. No member of the procurement team has received any training on the retention of documents. The team plan to introduce training for the team and will develop a retention schedule and manage it.

b) **Emails:**

No testing was carried out as part of this audit – the Corporate IT Email retention policy was introduced in June 2021 and there is already in place action to purge emails after 12 months and is being enforced.

5.2 The Record Retention Schedule was compared to other similar sized Local Authorities for example Coventry County Council of similar size to Milton Keynes Council. It was found that the MKC Records Retention Schedule was not as robust as Coventry County Council and could be strengthened to show a more comprehensive coverage of services which will improve the guidance provided to managers on record retention applicable to their service area. **(See MAP 4).**

6 Assurance Area – Compliance

Control Objective – To provide Assurance that the Council is compliant with its legislative requirements and MKC Document Retention Policy.

6.1 Testing confirmed that records are being retained in compliance with the policy and procedures and legislative requirements. Managers are aware what records are retained and where they are stored. Other than records held on managed systems there is generally no system in place to manage record retention, storage and disposal. Records are in some cases being retained for longer than necessary.

6.2 The Information Governance Board (IGB) has noted that records can't always be recovered quickly and there are inconsistencies in the way record retention is managed across the services and this is a finding in areas tested. There is an awareness of the retention schedule and of the procedures, but testing showed that although training has been delivered in the last 12 months, and is available on request and given where issues are identified, there is a need for more formal specific record retention training to reinforce the training briefly touched on during staff induction.

6.3 The Record Retention Policy and guidelines is compliant with the legislative requirements and the guidance provided by the Information Commissioner's Office (ICO). Testing confirmed that the areas tested have retained records for at least the statutory or the defined periods within the Corporate File Types retention schedule.

6.4 A discussion with the Head of Customer Data and insight highlighted that it's not possible to give 100% assurance of compliance without an automated piece of technology monitoring every keystroke. However, there is in place an updated suite of policy and guidance documents and planned training activity. There is training and guidance material signposted on the intranet. The current state of and future plans for retention were discussed and Information Governance Board (IGB) reports to the Security Management Committee responding to concerns raised relating to the handling of FOI and record retention management. The importance of there being a correct regime to manage information is clearly understood and there is now an email retention policy (June 2021). The Retention schedule has been reviewed in line with the Institute of Records Management best practice.

6.5 The IG team have provided enhanced templates to services to ensure that they are capturing appropriate records and applying correct treatments for storage retention and disposal, the retention schedule is also attached. It has been recognised by the IGB and the Council that records management in some services needs improvement (for example, Planning Service). Records are retained in compliance of the guidance but have not always been stored in such a way as to make it easy to identify and simple to retrieve and disclose if required. There is now a checklist for the IG team to work to and clearly defined IG team responsibilities. The IG team are working with Planning to introduce a defined agreed process when requests on planning related information is requested. Proactive steps are being taken working with ICT colleagues to exploit tools to create a robust embedded living automated records management system within the office 365 environment for completion by 30 April 2022 **(See MAP 1, 2 and 3).**

7 Assurance Area – Security

Control Objective – To provide assurance that records are stored securely with appropriate restricted access.

7.1 Across all areas tested records were found to be stored on systems that have secure access controls and within local drives that are restricted to the relevant team's access permissions. The responsibility for the security sits with the local system administrators, business systems team or IT or individual teams for the locally stored records. Each officer is responsible for the retention of its records in accordance with the policy and schedule of retention and of its security.

Management Action Plan

Likelihood	H	S	I	E
	M	S	I	E
	L		S	I
		L	M	H
		Impact		

The Agreed Actions are categorised on the following basis:	
Essential	Action is imperative to ensure that the objectives for the area under review are met.
Important	Requires action to avoid exposure to significant risks in achieving objectives for the area under review.
Standard	Action recommended enhancing control or improving operational efficiency.

Ref	Issue	Recommendation	Management Comments	Priority	Officer Responsible	Due Date
1	Manual process in place for managing retention and deletion reliance on officers understanding and following excel retention schedule Lack of a robust, embedded, living automated records management system within the Office 365 environment to effectively corporately manage record	Strengthen the overarching governance, to ensure compliance and consistency across Council Services, by developing a robust, embedded living automated records management system within the Office 365 environment.		Important	Lisa Beckett – Head of Customer Data and Insight.	30 April 2022

Ref	Issue	Recommendation	Management Comments	Priority	Officer Responsible	Due Date
	retention across the Council.					
2	Insufficient manager awareness and training of staff responsible for the retention of records within Council Services.	Increase manager awareness of the Record Retention requirements and their responsibilities and consider introducing periodic Record Retention specific training and introduce the record retention requirements of all staff at induction training.		**Standard**	Lisa Beckett – Head of Customer Data and Insight	31 October 2021
3	Insufficient Corporate controls to ensure compliance with Record Retention Schedule.	Monitor corporate compliance and take appropriate corrective action where the policy and/or procedures are not being followed by Service managers, particularly in		**Important**	Lisa Beckett – Head of Customer Data and Insight	30 April 2022

Ref	Issue	Recommendation	Management Comments	Priority	Officer Responsible	Due Date
		managing the destruction of records that are no longer required.				
4	Document Retention Schedule is not Comprehensive.	Review the Retention Schedule to reflect the current functions and activities of the Council to increase the guidance to managers. Move to the IRM functional classification and build in SharePoint as a living EDRMS, with automated retention and deletion schedules, in line with best practice and legislation.		Important	Lisa Beckett – Head of Customer Data and Insight	30 September 2021

milton keynes council

Audit reference number

Distribution List

CLIENT:	**Sarah Gonsalves - Director of Customer and Communities**
Full Report Issued for Action:	Lisa Beckett – Head of Customer Data and Insight
Full Report Issued for Information:	Hazel Lewis – Head of IT & Print Yvonne Okonjo – Corporate Information Officer. Natasha Hutchin – Deputy Head of Finance Deputy S.151 Officer.

Issue Date: 07/07/2021

Audit Committee Date: tbc

This audit and report has been prepared in line with the LGSS Internal Audit Manual and has been subject to appropriate review.

LGSS Chief Internal Auditor Approval:	Duncan Wilkinson
Quality Reviewed:	David Lamb/Jacinta Fru
Lead Auditor:	Alan Bacon