Shared Internal Audit Service
Hertfordshire in Partnership

Final Internal Audit Report

Stevenage Borough Council - Information Management (Storage and Retention)

October 2016

Issued to:	Paul Froggatt – Borough Solicitor Andy Christophi – Corporate Facilities and Compliance Manager Jenny Body – Digital Communications Officer Fariha Ayyub – Senior Corporate Solicitor David Traylor – Information Officer
Copied to:	Richard Protheroe – Head of Service (Chief Executive's Unit) Andy Sowden – Interim Head of Property and Estates Scott Crudgington – Chief Executive Clare Fletcher – Assistant Director (Finance)
Report Status:	Final
Reference:	S5003/16/001
Overall Assurance:	Substantial

INDEX

1. EXECUTIVE SUMMARY

Introduction

1.1 Internal Audit provides Stevenage Borough Council ('the Council') with an independent and objective opinion on the organisation's governance arrangements, encompassing internal control and risk management, by completing an annual risk-based audit plan. This audit forms part of the approved 2016/17 Internal Audit Plan for the Council.

1.2 Whilst the main focus of this audit is on information in paper documents, the key assurance area of 'Governance' also covers digital information.

1.3 Policies and procedures for the retention of information need to support local government, accounting and anti-fraud related requirements. In addition, there is a need to comply with relevant legislation in relation to information management, primarily the Data Protection Act 1998, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004. The Council's retention schedule formally defines the expectations and requirements for information retention, including the period of storage until destruction.

1.4 Non-compliance with the Council's retention schedule and relevant supporting policies and procedures may incur additional resource and material costs for the Council in respect of searches, retrieval and storage. Any breach of the information management legislation may cause reputational damage to the Council and, if personal data is involved, a potential fine of up to £500,000 may be imposed by the Information Commissioner's Office.

1.5 From 25 May 2018, the EU General Data Protection Regulation (GDPR) will affect every organisation that processes EU residents' personally identifiable information. The GDPR will supersede national laws such as the Data Protection Act 1998 (DPA), and the Regulation mandates considerably tougher penalties than the DPA: breached organisations can expect fines of up to 4% of annual global turnover (N.B. turnover, not profit) or €20 million – whichever is greater.

1.6 Article 37(5) of the GDPR states that Data Protection Officer (DPO's) must be appointed for all public authorities and certain companies and that a DPO may act for a group of authorities or companies. The GDPR does not specify precise credentials for a DPO, but does require that they have "expert knowledge of data protection law and practices." The GDPR states that the role of a DPO may be allocated to an existing employee or can be contracted externally, but a DPO must be able to operate independently and report to the highest level of the organisation, i.e. board level.

1.7 Article 39 of the GDPR defines the minimum tasks expected of a DPO. This includes informing the organisation about their legal obligations, monitoring compliance with the GDPR and other DP laws, managing internal DP activities, advising on DP impact assessments, training staff, conducting internal audits and being first point of contact.

1.8 The purpose of this audit was to review the governance framework for information management and the processes for the storage, retention and destruction of paper documents to support compliance with the Council's retention schedule, the current legislation and the forthcoming GDPR.

Overall Audit Opinion

1.9 Based on the work performed during this audit, we can provide overall **Substantial Assurance** that there are effective controls in operation for those elements of the risk management processes covered by this review. These are detailed in the Assurance by Risk Area Table in section 2 below.

1.10 For definitions of the assurance levels, please see Appendix B.

1.11 In response to a previous outstanding data protection related recommendation, the Council are currently completing a review of the corporate Data Protection Policy and the supporting Guide for Staff documentation published on the intranet. This is formally included as part of a programme of 'significant enhancement activity' the Council has identified and planned for 2016/17 as a result of a self-assessment of their corporate governance arrangements.

1.12 Any general review of data protection should include records management and, in particular, the policies and procedures for the retention and disposal of data and paper documents as this is a key part of compliance with the DPA. To ensure this is covered, we have made a recommendation in this respect.

1.13 Another 'enhancement activity' planned by the Council for delivery in 2016/17 is a programme of training in relation to data protection. Members and the Senior Management Team received training at the beginning of 2016 and a schedule of officer training is being established. On this basis, we have not raised a specific recommendation regarding training with the expectation that the activities identified and planned by the Council will be fully completed in 2016/17.

1.14 The maintenance and security of the main off-site paper document storage facility at Shephalbury Park depot is managed by the Corporate Facilities and Compliance Manager whilst authorisation of retrievals and deposits of storage boxes by service areas is administered by the Digital Communications Officer, including the maintenance of a comprehensive register with details of the boxes in storage.

1.15 Whilst this joint arrangement has worked well since the deletion of the Records Manager role several years ago, we encourage the confirmed intention for the Corporate Facilities and Compliance Manager to take over full control of all aspects of paper document storage, access and destruction as soon as it is possible for this to be achieved. We have made a recommendation in this respect.

1.16 A full audit of all boxes containing paper documents in the main storage facility has not been completed for several years. There is also a second secure storage facility on the Shephalbury Depot site with further boxes that need to be reviewed and the contents potentially destroyed. Therefore, to ensure there are no DPA compliance issues with any of the paper documents being retained in storage, we have made a recommendation that a full audit is carried out.

1.17 Several hundred storage boxes that have passed their recorded retention date have been returned to their respective owners for confirmation that the contents can now be destroyed. However, in many cases, a response is still awaited, so there are potentially paper documents in those boxes being retained in breach of the DPA. We have made a recommendation in this respect.

Summary of Recommendations

1.18 We have made five recommendations, one of which is classified as 'Medium' priority and four as 'Merits Attention'.

1.19 Our 'Medium' priority recommendation is as follows:

a) Retention - full audit of all paper documents currently in storage.

1.20 Our four 'Merits Attention' recommendations are as follows:

a) Governance - full review of Retention Guidelines and Records Management Policy.
b) Governance – DPA compliance monitoring reports for Senior Management.
c) Storage - management of all paper document storage by Property and Estates.
d) Disposal – authorisation for destruction of paper documents identified for disposal.

1.21 For further details of our recommendations, please see the Management Action Plan at Appendix A.

Annual Governance Statement

1.22 This report provides good levels of assurance to support the Annual Governance Statement.

Audit Commentary

Governance – Corporate Risk Register

1.23 Information management is not currently included in the Council's Corporate Risk Register.

1.24 By including information management in the Council's Corporate Risk Register, it would highlight its relevance across all the Council's services and operations. In this respect, it would underline the impact of any non-compliance with the Data Protection Act 1998 (DPA), including responses to Subject Access Requests, plus requests received under the Freedom of Information Act 2000 (FOI) and the Environmental Information Regulations 2004 (EIR).

1.25 However, the Council are currently satisfied that this is not necessary as all information management related concerns are well managed, including the provision of appropriate training, to sufficiently mitigate the potential reputational and financial risks of any breaches of the DPA and to ensure compliance with the FOI and EIR. The emergence of risks in relation to information management would be managed by the Corporate Governance Group and the Corporate Risk Group.

1.26 On this basis and acknowledging that, to date, the Council has not had any issues of non-compliance with the DPA in particular, we have not raised a formal recommendation to include information management in the Council's Corporate Risk Register at this time.

2. ASSURANCE BY RISK AREA

2.1 Our specific objectives in undertaking this work, as per the Terms of Reference, were to provide the Council with assurance on the adequacy and effectiveness of internal controls, processes and records in place to mitigate risks in the following areas:

Risk Area	None	Limited	Moderate	Substantial	Full
Governance (paper-based and digital information) – accountability, strategic oversight and operational responsibilities for retention of information; inclusion of information management in corporate risk register; formally agreed and maintained retention schedule.					
Storage (paper documents) – policies and procedures for storage and archiving; off-site locations and accommodation; management and security of storage facilities; access arrangements.					
Retention (paper documents) – policies and procedures to support retention schedules; staff and Member awareness and understanding of retention requirements; monitoring of compliance with the retention schedule.					
Disposal (paper documents) – agreed and formally maintained policy; identification and authorisation procedures for disposal/destruction; on-site facilities for confidential waste; contractual arrangements for disposal/destruction.					

Overall					

2.2 For definitions of the assurance levels, please see Appendix B.

No.	Finding / Associated Risk	Priority	Recommendation	Management Response	Target Date
1.	**Governance** - formally agreed and maintained retention schedule Whilst there are appropriate documents in place in respect of the Council's 'Record Retention Guidelines' and 'Records Management Policy', these have not been maintained or reviewed for over eleven years. <u>Associated Risk</u> Without clear corporate policies, robust supporting procedures and appropriate operational management, with oversight and regular monitoring by Senior Management, the storage and retention of paper documents containing personal data may not be compliant with the DPA. This may result in damage and distress to individuals, reputational damage to the Council and regulatory action being taken with a potential fine of up to £500,000.	Merits Attention	We recommend that the Council's 'Record Retention Guidelines' (including the 'Introduction' document) and the 'Records Management Policy' (with the supporting guide for 'The Records Disposal Review Process') are fully reviewed and refreshed with all Heads of Service, formally approved at Director level and actively promoted to all Council Officers and Members.	**Responsible Officer:** Borough Solicitor **Agreed Action:** A full review and any necessary revisions of the Council's Record Retention Guidelines and Records Management Policy (and any supporting guidance or other relevant documentation) will be undertaken over the next six months in liaison with all Heads of Service. Regular updates will be provided to the Council's Corporate Governance Group who will be monitoring progress.	31 March 2017

No.	Finding / Associated Risk	Priority	Recommendation	Management Response	Target Date
2.	**Governance** - accountability, strategic oversight and operational responsibilities The organisational framework and operational procedures are in place to support the delivery of the Corporate Data Protection (DP) policy and Retention Schedule. However, no regular formal update reports are provided to Senior Management (or to Members) in respect of their oversight and accountability for compliance with the Data Protection Act 1998 (DPA), including the storage and retention of personal data. <u>Associated Risk</u> Without clear corporate policies, robust supporting procedures and appropriate operational management, with oversight and regular monitoring by Senior Management, the storage and retention of paper documents containing personal data may not be compliant with the DPA. This may result in damage and distress to individuals, reputational damage to the Council and regulatory action being taken with a potential fine of up to £500,000.	Merits Attention	We recommend that appropriate DP compliance monitoring reports are issued monthly to Senior Management and Members and are reviewed as necessary. These reports should include updates about actions and issues in relation to digital and paper storage and retention to ensure that files are not being held for longer than necessary and are being deleted / destroyed in a timely way. These updates should form part of the same monitoring reports as those in relation to the similar recommendation we made in our report for the recent audit of Data Protection (see recommendation 3 in our Final Report issued 19 August 2016).	**Responsible Officer:** Information Officer **Agreed Actions:** Reporting requirements will evolve as the document retention schedule is compiled and refined as an on-going project. In the meantime, appropriate DP compliance reports will be provided to the Council's Corporate Governance Group for monitoring and review purposes and escalation where necessary.	By end 2017 31 December 2016

No.	Finding / Associated Risk	Priority	Recommendation	Management Response	Target Date
3.	**Storage** - management and administration of storage facilities Once the Digital Communications Officer has fully completed and tested the central register of all boxes of paper documents held in storage, the agreed intention is that it will be handed over to the Corporate Facilities and Compliance Manager so they will then become the Council's single central point of contact and control for paper document storage and retention. However, no timescale has been formally established for this to happen. <u>Associated Risk</u> The storage and retention of paper documents containing personal data may not be compliant with the DPA. This may result in damage and distress to individuals, reputational damage to the Council and regulatory action being taken with a potential fine of up to £500,000.	Merits Attention	We recommend that an agreed timescale is formally established, and monitored, for the transfer from the Chief Executive's Unit to the Property and Estates service area of the overall management and administration of all aspects of the storage, retention and destruction of paper files.	**Responsible Officer:** Corporate Facilities and Compliance Manager **Agreed Actions:** Complete the audit of all boxes in storage and update the central register. (Digital Communications Officer) Complete all identified disposals. (Facilities Team) Upload the updated central register to an online system (IT in liaison with Digital Communications Officer) Roll out training to all staff. Transfer of full responsibility and operational control for storage, retention and destruction of paper files to Facilities Team.	31 March 2017

No.	Finding / Associated Risk	Priority	Recommendation	Management Response	Target Date
4.	**Retention** - compliance with retention schedule A full audit of all boxes containing paper documents in the main storage facility has not been completed for several years. There is also a second secure storage facility on the Shephalbury Depot site containing further boxes that need to be reviewed and the contents potentially destroyed. <u>Associated Risk</u> The storage and retention of paper documents containing personal data may not be compliant with the DPA. This may result in damage and distress to individuals, reputational damage to the Council and regulatory action being taken with a potential fine of up to £500,000.	Medium	We recommend that, in conjunction with all Heads of Service, a full audit is carried out of all paper documents currently in storage to ensure that what continues to be retained has confirmed ownership with an agreed destruction date that is compliant with the Council's 'Record Retention Guidelines' and with the DPA. Also ensuring that the CRC Register is fully complete and accurate in respect of the details for whatever paper documents are retained. The audit will need to include all units on the Shephalbury site or elsewhere that are being used for the storage of any of the Council's paper documents.	**Responsible Officer:** Heads of Service and Digital Communications Officer **Agreed Actions:** Continuation of the review process that has already started, to include obtaining responses from all Heads of Service (or their designated officers) confirming ownership and appropriate destruction dates for boxes that have originated from their service area. It will also encompass a full audit by the Heads of Service of the contents of the boxes held in either of the storage units on the Shephalbury depot site. The central register will be updated as necessary by the Digital Communications Officer to ensure it remains fully complete and accurate.	30 November 2016

No.	Finding / Associated Risk	Priority	Recommendation	Management Response	Target Date
5.	**Disposal** - authorisation for disposal/destruction Several hundred storage boxes that have passed their recorded retention date have been returned to their respective owners for confirmation that the contents can now be destroyed. However, in many cases, a response is still awaited so, potentially, there are paper documents in those boxes being retained in breach of the DPA. <u>Associated Risk</u> The storage and retention of paper documents containing personal data may not be compliant with the DPA. This may result in damage and distress to individuals, reputational damage to the Council and regulatory action being taken with a potential fine of up to £500,000.	Merits Attention	We recommend that the required authorisation from all respective Heads of Service is pursued as a priority, and escalated where necessary, to ensure that the paper documents that have been previously identified for potential disposal can be confirmed as such and arrangements made for their immediate destruction.	**Responsible Officer:** Corporate Facilities and Compliance Manager **Agreed Actions:** Outstanding authorisations from Heads of Service (or their designated officers) for the destruction of boxes will be pursued urgently and, if necessary, escalated to the relevant Director. Consideration will be given to revising the Council's disposal policy to say that, in future, the confirmed destruction date for each storage box will be sufficient authorisation for the contents to be automatically destroyed when the date is reached without any further reference to the respective owner.	30 November 2016

Levels of assurance	
Full Assurance	There is a sound system of control designed to achieve the system objectives and manage the risks to achieving those objectives. No weaknesses have been identified.
Substantial Assurance	Whilst there is a largely sound system of control, there are some minor weaknesses, which may put a limited number of the system objectives at risk.
Moderate Assurance	Whilst there is basically a sound system of control, there are some areas of weakness, which may put some of the system objectives at risk.
Limited Assurance	There are significant weaknesses in key control areas, which put the system objectives at risk.
No Assurance	Control is weak, leaving the system open to material error or abuse.

Priority of recommendations	
High	There is a fundamental weakness, which presents material risk to the objectives and requires urgent attention by management.
Medium	There is a significant weakness, whose impact or frequency presents a risk which needs to be addressed by management.
Merits Attention	There is no significant weakness, but the finding merits attention by management.