Shared Internal Audit Service
Hertfordshire in Partnership

## Final Internal Audit Report

# East Herts Council
# Data Protection

## December 2015

| | |
|---|---|
| **Issued to:** | Neil Sloper – Head of Information, Customer and Parking Services<br>Alasdair McWilliams – Digital Media and Information Manager<br>Neil Prior – Information Officer |
| **Copied to:** | Adele Taylor – Director of Finance and Support Services<br>Chris Gibson – Head of Governance and Risk Management<br>Audit Committee Members<br>Finance Portfolio Holder |
| **Report Status:** | Final |
| **Reference:** | E3208/15/001 |
| **Overall Assurance:** | Substantial |

**INDEX**

# 1 EXECUTIVE SUMMARY

## Introduction

1.1 Internal Audit provides the Council with an independent and objective opinion on the organisation's governance arrangements, encompassing internal control and risk management, through the completion of an annual risk-based internal audit plan. This audit derives from the approved 2015/16 Internal Audit Plan for East Herts Council (EHC).

1.2 The Data Protection Act 1998 (DPA) regulates information relating to living individuals who can be identified from that information (referred to as personal data) either as it stands on its own or when combined with other information that is also available. This applies to both electronic and paper based information.

1.3 The DPA has eight principles which, in summary, require personal data to be:

1. processed fairly and lawfully;
2. obtained and processed only for one or more specified lawful purposes;
3. adequate, relevant and not excessive in relation to the specified purpose(s);
4. kept accurate and up to date;
5. retained for no longer than necessary in relation to the specified purpose(s);
6. processed in accordance with the rights of the individual (data subject);
7. kept safe and secure;
8. not transferred outside the EEA unless adequately protected.

1.4 The purpose of this audit was to assess the appropriateness and effectiveness of internal controls that are in place in relation to data protection and to evaluate compliance with them across service areas in order to provide assurance that EHC is able to meet the statutory responsibilities under the DPA.

1.5 The audit scope of data protection can be broken down into six potential areas as described by the Information Commissioner's Office (ICO). This was discussed with the Head of Information, Customer and Parking Services to determine the specific two areas of focus for this audit as follows:

1.6 **Governance Arrangements**

- formally highlighted risks in corporate and service risk registers, accountability in job descriptions and organisational management structures, policies, procedures and other controls that are in place to support compliance with the DPA.

1.7 **Security of Personal Data**

- organisational and technical measures that are in place (excluding network security which is under the remit and responsibility of the ICT Shared Service with Stevenage Borough Council) and how they are complied with to ensure there is adequate security for personal data held in manual or electronic form, including ownership, physical security and in respect of third party contracts.

## Audit Opinion

1.8 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.

1.9 For definitions of the assurance levels, please see Appendix A.

1.10 Our findings and opinions in respect of each of the two Risk Areas covered by this audit are summarised as follows:

### Governance Arrangements

1.10.1 It is evident from our findings that, over the past two years, EHC have looked to strengthen the governance structure around Data Protection compliance. This includes having a clear formalised framework confirming roles and ownership of Data Protection risks at senior management level with the Chief Executive designated as the Senior Information Risk Owner. As part of this framework, independent scrutiny and assurance is provided by the Corporate Business Scrutiny Committee.

1.10.2 A risk driven action plan formally captures both: key corporate risks; and Data Protection risks identified within service areas with relevant actions or recommendations to address them. This has been in place since 2013 and is providing an appropriate mechanism for helping manage and monitor the Data Protection risks from both an operational and strategic perspective. The Head of Information, Customer and Parking Services is responsible for completing an annual DP review and provides a report to the Corporate Business Scrutiny Committee to update them on the implementation of the Council's Data Protection action plan.

1.10.3 Service areas are required by the Information Management Team to review their risks annually and actively confirm they have not changed or revised them as necessary. We see this as good practice to help service areas consider and take responsibility for managing their Data Protection risks as part of normal operations.

1.10.4 During our audit we have also seen evidence of new / revised Data Protection policies being agreed and active promotion and support for Data Protection compliance across the Council by the Information Management Team.

### Security of Personal Data

1.10.5 A Data Management Review of the ICT Shared Service was carried out by SIAS in 2014 and provided substantial assurance with one 'merits attention' recommendation around the finalisation of draft policies and procedures.

1.10.6 On the basis that it covered roles and responsibilities, the security of data and data management policies, we have placed reliance on the work we did in respect of the Data Management Review and have not repeated any of the fieldwork or testing for the purposes of our current Data Protection audit.

**Summary of Recommendations**

1.11 We have not made any recommendations as a result of our audit.

**Annual Governance Statement**

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

## 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 Arrangements | | | | | |
| Security of Personal Data<br>(as per Data Management Review audit report - 2014) | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **Overall** | | | | | |

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

| 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. |