London Borough of Brent Council

Data protection audit report

Executive summary
October 2015

Information Commissioner's Office

1. Background

1.1 The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit.

1.2 The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.

1.3 London Borough of Brent Council (LBBC) agreed on 11 February 2015 to a consensual audit of their processing of personal data by the ICO Good Practice Department.

1.4 An introductory teleconference was held on 2 July 2015 with LBBC to identify and discuss the scope of the audit.

2. Scope of the audit

2.1 Following pre-audit discussions with LBBC it was agreed that the audit would focus on the following areas:

a. Security of personal data – The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.

b. Subject access requests - The procedures in operation for recognising and responding to individuals' requests for access to their personal data.

c. Data sharing - The design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.

3. Audit opinion

3.1 The purpose of the audit is to provide the Information Commissioner and LBBC with an independent assurance of the extent to which LBBC, within the scope of this agreed audit, is complying with the DPA.

3.2 The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

Overall Conclusion	
Limited Assurance	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA. We have made one reasonable and two limited assurance assessments where controls could be enhanced to address the issues which are summarised below and presented fully in the 'detailed findings and action plan' in section 7 of this report.

4. Summary of audit findings

4.1 Areas of good practice

- The council's management direction and support for information security is outlined in a number of key policies including an Information Security Policy (ISP) and an Information Risk Policy (IRP) which are owned and approved by the Information Governance Group (IGG). The policies are published on the Information Governance homepage and regular updates are posted on the intranet as reminders and to raise awareness amongst staff.

- The council's intranet sets out the procedure for reporting security breaches and differentiates the process depending on the nature of the breach. This is supplemented by the Security Incident Management Operational Process which outlines the roles, responsibilities and procedures involved for staff in the event of a security incident. Contractors are required to sign a confidentiality agreement which sets out what information can be used for and how it should be handled and are required to adhere to the incident management process set out by the council.

- Privacy Impact Assessments (PIA) are well established at the council and take place prior to the commencement of new or changing systems/processes.

4.2 Areas for improvement

- At present LBBC have not implemented any endpoint controls which would restrict the import and export of data using portable devices, resulting in the risk that an individual could download personal information without authorisation or potentially introduce malware onto the council's network.

- There is currently no formally established programme of data protection or information security related refresher training in place, with the last training of this nature being delivered via e-learning in 2012. Staff who commenced employment at the council prior to the last refresher training in 2012 may not have had data protection or information security refresher training for a significant period of time.

- LBBC reported a 64% subject access compliance rate during 2014. This increased to 78.6% during January to May 2015, and LBBC are targeting 80% during 2015 and 95% for 2016.

The ICO believes this latter target is more appropriate and LBBC should seek to attain this as soon as possible. LBBC should also ensure that they prioritise requests which are in danger of falling outside the statutory 40 calendar day period.

- LBBC have aimed to raise awareness of data sharing policies through a combination of methods which include e-learning and use of the intranet. Despite this, awareness of specific data sharing policies and / or guidance amongst operational staff was low, with interviewees unable to make reference to specific policies.

- There are inconsistencies in the use and completion of the Data Sharing Agreement (DSA) template and no specific provisions within the DSAs viewed as part of the audit to distinguish between fact and opinion within shared data. In addition not all the DSAs and supporting procedural documentation specify retention periods for shared data or prescribe that the recipients of shared data must destroy or return that data once the relevant purpose is served or any relevant retention period expires.

5. Audit approach

5.1 The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

5.2 The audit field work was undertaken at Brent Civic Centre between 8 and 10 September 2015.

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of London Borough of Brent Council.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.