Title: Information Governance Update

Report of the Divisional Director of Finance

Open Report For Information
Wards Affected: All Key Decision: No

Report Author: Contact Details:
Rupert Hay-Campbell Tel: 020 8227 3190
ICT and Information Governance Officer E-mail: rupert.hay-campbell@lbld.gov.uk

Accountable Divisional Director: Jon Bunt, Divisional Director of Finance

Accountable Director: Graham Farrant, Chief Executive

Summary:
This report provides an update on Information Governance issues in the Council. It includes statistics on Freedom of Information requests and Data Protection Subject Access requests. The report also sets out work that has been completed in the past year by the Information Governance board.

Recommendation(s)
The committee is recommended to:

(i) Note the data on Freedom of Information requests and Data Protection Act subject access requests

(ii) Note the work that has been on going to improve Information Governance in the Council

(iii) Note the planned actions for 2013

(iv) Note that the internal audit recommendations for the Council’s Data Quality policy will be deferred until resources become available

Reason(s)
To provide the Public Accounts and Audit Select Committee with an update on the Council’s Information Governance work.
1. Introduction and Background

1.1. The previous Information Governance report provided data up to September 2011. This report provides data up to September 2012, but it includes data for the whole financial year 2011/12 for comparison.

1.2. Corporate Complaints and Members Case work are no longer covered by the Information Governance report, as these were covered in a separate report that was presented to PAASC on 22 September 2012.

1.3. The risks associated with Information Governance are identified as corporate risks (CR 10) and an action plan remains in place to mitigate the risks.

1.4. The Information Commissioner’s Office (ICO) continues to make use of its powers to fine organisations responsible for the loss of personal data. The ICO has now fined 19 local councils a total of £1,885,000 (the single biggest fine was £250,000) and was recently quoted as saying “there is an underlying problem with data protection in local government”.

1.5. Effective Information Governance will be key to how the Council responds to the Government’s code of recommended practice on Data Transparency. The Department of Communities and Local Government (DCLG) has been consulting on making the code of recommended practice a legal requirement.

1.6. This report is divided into four main sections:
   - Information Management & Security
   - Freedom of Information requests
   - Data Protection Act Subject Access requests
   - Data Quality

1.7. The report concludes by setting out the planned Information Governance activities for the year ahead.

2. Information Management & Security

2.1. Significant work has taken place in 2012 to build an electronic corporate library. The aim of this library is to ensure that the many documents and policies generated across the Council are properly structured and accessible to those staff who need them.

2.2. The corporate library has been implemented as part of the Council’s new intranet system. The corporate library will provide an electronic file plan based upon a nationally defined structure and will be crucial to help ensure that the Council can respond effectively and efficiently to Freedom of Information requests in the future.

2.3. Work has been ongoing to raise awareness of good information governance practices. Posters based on material made freely available by the Information Commissioner’s Office have been distributed across the Council. The “Managing Information” online training course was made available on the Council’s new i-Learn system in October 2012. The following table shows the uptake of this course:

<table>
<thead>
<tr>
<th>Total enrolled</th>
<th>2173</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total &quot;completed&quot;</td>
<td>504</td>
</tr>
<tr>
<td>Total &quot;incomplete&quot;</td>
<td>79</td>
</tr>
<tr>
<td>Total &quot;not attempted&quot;</td>
<td>1589</td>
</tr>
</tbody>
</table>
2.4. All staff are required to take this course annually and additional messages will be sent to staff and managers in January 2013 to remind them of this obligation. Data will be provided to departments on a regular basis detailing how many staff within the department have completed the training.

2.5. New Information Governance pages have been created on the Council’s Intranet. These pages will continue to be refined and updated to reflect issues that are identified by staff.

2.6. The Council has successfully retained its accreditations for the Public Sector Network (PSN) and the NHS N3 networks. These crucial connections are vital to support partnership working with central government, other local authorities and the NHS.

2.7. Information security incidents continue to be reported and investigated internally to ensure that lessons are learnt. The latest information on security incidents is shown in the table below:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bogus email / phone call</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Attempted hack</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Computer / laptop stolen</td>
<td>3</td>
<td>11</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Confidential information disclosure</td>
<td>1</td>
<td>8</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>Papers left on printer / public area</td>
<td>2</td>
<td>5</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>RSA token lost / stolen</td>
<td>1</td>
<td>7</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Security pass issue</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unsecure email sent</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Improper storage of information</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Password mis-management</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>IT permissions incorrect</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>USB memory device lost / stolen</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>No breach</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td><strong>16</strong></td>
<td><strong>38</strong></td>
<td><strong>25</strong></td>
<td><strong>17</strong></td>
</tr>
</tbody>
</table>

2.8. Under-reporting of security incidents remains a concern. Staff will be reminded of the importance of reporting any issues for investigation during the year ahead.

2.9. Trends are being observed with:

- The Council’s MFD printers where items are being scanned and emailed to the wrong internal recipient. It is expected that this issue will be addressed through the planned use of ID badges to log on to the printers.

- Emails being sent to the wrong internal recipient. The Information Governance board will be considering these cases to identify any actions that can be taken to reduce the risk of this type of problem occurring in the future.

2.10. The Council self-reported one issue to the Information Commissioner’s Office (ICO). This involved the unauthorised release of information from the Council’s housing system. The ICO confirmed that they considered the release of information to be a breach of the Data Protection Act but they were not planning to take further action against the Council.

**ICO Complaints**

2.11. There have been three complaints made by members of the public to the Information Commissioner’s Office in the past year relating to the unauthorised releases of personal data:
- A social worker left details in a report which were inappropriately shared with the client. The ICO found that the Council had breached the Data Protection Act but took no further action. Breach occurred: September 2011; complaint to ICO: November 2011; complaint closed: August 2012.

**Response from department:** It is now accepted good practice that children who are adopted have this explained to them as soon as they are considered able to deal with the information. However this would not have been the case in the 1950s when the service user concerned was adopted by the complainant.

This situation arose because of an administrative error when we moved from paper files to all electronic records in social care around 2004/5. The service user’s previous surname was entered on the main client records. A small dedicated team undertook the process of creating new records on an electronic system from paper files and scanning previous documents into the new system. Their work was meticulous and carefully supervised by an experienced member of staff who was trained and well versed in the requirements of the Data Protection Act as it applies to Social Services clients. There were appropriate controls in place.

The social worker concerned was not aware of the previous adoption and unwittingly used the name on the records in error. The particular set of unfortunate circumstances that led to this particular Data Breach is extremely unlikely and there is a very low risk of it occurring again.

- The parking service enclosed the wrong photo of a vehicle when sending a penalty charge notice to the owner. The ICO found that the Council had breached the Data Protection Act but took no further action. Breach occurred: July 2011; complaint to ICO: May 2012; complaint closed: July 2012

- The parking service sent details of the wrong penalty charge notice to a member of the public and the Parking Appeals Tribunal Service disclosing the personal data of a third party. The ICO found that the Council had breached the Data Protection Act but took no further action. Breach occurred: June 2011; complaint to ICO: May 2012; complaint closed: July 2012

**Response from department:** As a result of these two complaints parking services are now moving into a secure office in Barking Town Hall. This office will have a dedicated MFD printer to avoid information from other services being mixed in with responses to PCN’s. Staff are also completing more stringent check sheets to ensure only the correct data is being posted.

3. **Freedom of Information Requests**

3.1. The number of Freedom of Information requests received by the Council continues to rise year on year:

- In 2009/10 the Council received 711 requests
- In 2010/11 the Council received 818 requests
- In 2011/12 the Council received 1159 requests

3.2. The monthly breakdown of the number of requests is shown in the table below:
3.3. In 2011/2012 the Council started monitoring the number of requests that were being responded to within the statutory deadline:

- In 2011/12 the Council responded to 72% of requests within the deadline
- In 2012/13 the Council responded to 75% (to date) of requests within the deadline

3.4. In order to improve the management of Freedom of Information requests, new performance indicators were agreed with Elevate who provide the FoI handling service as part of the B&D contact centre. This new performance indicator measures both how quickly FoI requests are logged and if they are assigned to the correct service area. This data is shown in the table below:

<table>
<thead>
<tr>
<th>Performance Indicator</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Jul</th>
<th>Aug</th>
<th>Sep</th>
<th>Ave</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests correctly handled (Target &gt; 91.42%)</td>
<td>74.29%</td>
<td>91.42%</td>
<td>95.71%</td>
<td>100%</td>
<td>94.28%</td>
<td>100%</td>
<td>92.62%</td>
</tr>
</tbody>
</table>

3.5. Requests are received from a wide range of people. The origin of a request is not logged, as requestors only needs to provide their name and contact details when making requests.

3.6. It is not practical to break down all the requests by origin. However an analysis of the requestors making more than 4 requests has been conducted. By reviewing the requests, they have been manually categorised as shown in the table below:

<table>
<thead>
<tr>
<th>Number of requests</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Media (1 individual)</td>
</tr>
<tr>
<td>8</td>
<td>Local community group (1 individual)</td>
</tr>
<tr>
<td></td>
<td>Not specified (1 individual)</td>
</tr>
<tr>
<td>7</td>
<td>Member of the public – LBBD resident (1 individual)</td>
</tr>
<tr>
<td>6</td>
<td>Media (1 individual)</td>
</tr>
<tr>
<td>5</td>
<td>Solicitors (1 individual)</td>
</tr>
<tr>
<td>4</td>
<td>Member of the public – non-resident (1 individual)</td>
</tr>
<tr>
<td></td>
<td>Commercial (2 individuals)</td>
</tr>
<tr>
<td></td>
<td>Media (2 individuals)</td>
</tr>
<tr>
<td></td>
<td>MP – non-LBBD (1 individual)</td>
</tr>
</tbody>
</table>

3.7. Over the past year work has been undertaken to improve the Council's handling of Freedom of Information requests. The process followed by staff when they receive a request has been reviewed, updated and simplified. Regular meetings of the Council’s network of “Freedom of Information Champions” have restarted.

Financial impact

3.8. Currently information is not collected on the amount of time the council spends on responding to Freedom of Information Requests. It is estimated that, on average,
each request takes one hour to respond to. Using a rate of £25 per hour it is estimated that it cost the council approximately £29,000 to respond to these requests in 2011/12.

3.9. The process for responding to Freedom of Information Requests will be updated to collect an estimate of the amount of time it took to respond to the request. This will allow a more accurate estimate to be calculated in the future.

**Next steps**

3.10. It is planned to implement the new Freedom of Information process from 1 February 2013. Further work is planned to increase awareness of the processes that staff should be following if they receive a request and to ensure that exemptions are correctly applied.

3.11. Work is planned to update the Council’s Publication Scheme and update the Council’s web site to ensure that information made available under the Department of Communities and Local Government recommended code of practice is easily accessible.

4. **Data Protection Act Subject Access Requests**

4.1. The Data Protection Act gives the “data subject” a right to request a copy of the information held about him or her. This is known as a Data Protection Act Subject Access request.

4.2. The Council receives a significant number of Data Protection Act Subject Access requests every year. The month by month breakdown of these requests is shown below:

<table>
<thead>
<tr>
<th>DPA Requests</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Jul</th>
<th>Aug</th>
<th>Sep</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011/12</td>
<td>10</td>
<td>8</td>
<td>15</td>
<td>22</td>
<td>14</td>
<td>9</td>
<td>3</td>
<td>11</td>
<td>9</td>
<td>18</td>
<td>10</td>
<td>10</td>
<td>139</td>
</tr>
<tr>
<td>2012/13</td>
<td>16</td>
<td>15</td>
<td>20</td>
<td>17</td>
<td>6</td>
<td>13</td>
<td>18</td>
<td>13</td>
<td></td>
<td></td>
<td>10</td>
<td>10</td>
<td>118</td>
</tr>
</tbody>
</table>

4.3. **Note:** the number of Data Protection Act Subject Access requests was under reported in 2011. Work during 2012 identified the fact that Subject Access requests for social care clients are logged in a different system. The figures in this report have been updated to include the social care data.

4.4. Although the number of Data Protection Act subject access requests is lower than Freedom of Information requests they are often more complex to respond to.

4.5. A full review of the process for handling Data Protection Act Subject Access requests is planned for 2013. This review will seek to simplify the process and ensure that there is clarity around how requests should be handled – especially from members of staff. The process for requesting a review of the Council’s handling of a Subject Access request also needs to be clarified.

**ICO Complaints**

4.6. There have been two complaints about the Council’s handling of Data Protection Subject Access requests during the 2012:

- A member of staff complained that exemptions had been incorrectly applied to a Data Protection Act Subject Access request. On reviewing the case it was decided that the exemptions no longer applied and the information was released. Complaint to ICO: October 2012; this case is still being considered by the ICO.
• Information was only provided electronically to another member of staff in response to a Subject Access request. On reviewing the case it was decided that the cost of printing and posting the material was lower than the statutory limit set out by the Data Protection Act and the information was therefore released. The ICO upheld the complaint. Complaint to ICO: July 2012; complaint closed: August 2012.

4.7. The Council will be conducting a review of the guidance and processes staff use when responding to Data Protection Act Subject Access. This review will include addressing the issues raised by the above two complaints to the ICO.

5. **Data Quality**

5.1. Responsibility for the Council’s Data Quality policy was taken on by the Information Governance board in 2011. This included responsibility for the following recommendations that were made in an internal audit report in 2011 and which remain outstanding:

- The Data Quality policy should be refreshed so that it is reflective of the current management structures and the resources available
- The policy should be promoted as part of a group of policies concerned with Data Management / Information Governance
- The policy needs to emphasise that Divisional Directors and their managers are responsible for the Data Quality of information upon which they rely, and stress the importance of the accuracy of the data where it is used as the basis for decision making.

5.2. The target date for implementing these recommendations was December 2012.

5.3. Although the importance of data quality is recognised by the Information Governance board, work in 2012 focused on the highest risk areas for the Council, that is information security, Data Protection and Freedom of Information processes. Consequently no work has taken place to implement Internal Audit’s recommendations for the Data Quality policy. When resources become available these recommendations will be addressed.

6. **Conclusions and work plan for 2013**

6.1. The rise in the number of complaints investigated by the Information Commissioner (there were none in 2011) has highlighted issues with the procedures that staff are using when responding to Data Protection Act Subject Access requests and Freedom of Information requests.

6.2. The following actions are planned for 2013:

- Freedom of Information workshops for Group Managers
- Publication of all Freedom of Information requests on the Council’s website
- Implement new Freedom of Information process
- Regular Freedom of Information Champions’ workshops
- Provide online Freedom of Information training for staff
- Review the process for handling Data Protection Act Subject Access requests
- Raise awareness of the Council’s new corporate library
6.3. Work will continue to ensure that all staff take the online Managing Information training course and to continue to raise awareness of the importance of protecting the Council’s information.

**Background Papers Used in the Preparation of the Report:**


**List of appendices:**

None