AGENDA ITEM: 9 Page nos. 32 - 83

Meeting	Audit Committee
Date	7 December 2010
Subject	**Data Protection Audit**
Report of	Director of Corporate Governance
Summary	This report seeks approval of the Data Protection External Audit Report and Action Plan

Officer Contributors	Sian Hughes – Governance and Service Development
Status (public or exempt)	Public
Wards affected	All
Enclosures	Appendix A – ICO Report Appendix – Action Plan
For decision by	Committee
Function of	Council
Reason for urgency / exemption from call-in (if appropriate)	Not applicable

Contact for further information: Jeff Lustig, Director of Corporate Governance -Tel: 020 8359 2008

1. RECOMMENDATIONS

1.1 To approve the Information Commissioner's Office (ICO) Data Protection Audit Report and the Council's Action Plan.

2. RELEVANT PREVIOUS DECISIONS

2.1 None.

3. CORPORATE PRIORITIES AND POLICY CONSIDERATIONS

3.1 The Council's objectives include the priority 'Better Services with Less Money'. Good governance arrangements are central to the delivery of that priority objective, and meeting our statutory obligations under the Data Protection Act is a key element of good governance.

4. RISK MANAGEMENT ISSUES

4.1 Referred to in the body of the report.

5. EQUALITIES AND DIVERSITY ISSUES

5.1 Effective Data Protection arrangements are necessary to ensure that the Council is meeting its equalities and diversity obligations and objectives.

6. USE OF RESOURCES IMPLICATIONS (Finance, Procurement, Performance & Value for Money, Staffing, IT, Property, Sustainability)

6.1 Addressing the Council's Data protection responsibilities and putting in place mitigating actions to reduce the risk of non compliance is central to the effective use of resources.

7. LEGAL ISSUES

7.1 Referred to in the body of the report.

8. CONSTITUTIONAL POWERS

8.1 None.

9. BACKGROUND INFORMATION

9.1 Background to the DP Audit Report

9.1.1 From April 2010 new powers were given to the Information Commissioner's Office (ICO) to impose substantial fines (of up to £500,000) on organisations that breach the Data Protection Act (DPA). This came about largely as a result of a series of high profile 'personal data loss' cases across the country and the need to put greater pressure on organisations to meet their statutory obligations.

9.1.2 In response to this, it was important for the Council to assess how effective its DP policies and practices were, and to what extent it was meeting the statutory requirements of the DPA. To assist in this process, the ICO were asked to carry out an independent Data Protection Audit. This was a voluntary

audit (for which there was no charge), but one that we were keen to undertake in order to have an expert opinion on where we needed to focus our efforts in order to ensure we were fully compliant.

9.1.3 The draft Audit Report was completed in July 2010, along with the recommendations to address the areas of concern (appendix A).

9.1.4 The ICO recommended a follow up audit in six months time to assess to what extent the Council has put in place measures to mitigate the risks identified.

9.2 Key Improvements

9.2.1 The Audit highlights a number of key areas where the Council needs to concentrate its efforts:

- Risk Management – to ensure all directorates have sufficient support and guidance to identify and respond to DP risks
- Roles and Responsibilities – to identify and formalise corporate (Governance Team), directorate (Link Officers) and individual roles/responsibilities for DP
- Policies and Procedures – to ensure all the DP and data security policies are up to date, version controlled and accessible via the Councils' intranet pages
- Potential Breaches – to ensure the Council has an Incident Reporting Procedure and that staff know how to report a potential breach of the Act
- Awareness and Training - to ensure all staff across the Council understand their responsibilities are equipped with the essential knowledge to process data in accordance with the principles of the Act
- Responding to Requests for Personal Data – to ensure all staff receiving Subject Access Requests (SARs) understand the statutory process and timescales for responding to these, and the consequences of not doing so

9.3. Action Plan

9.3.1 The Action Plan (appendix B) sets out the key actions and progress that has already begun in addressing these areas.

9.3.2 To address one of the critical areas of concern, a communications and awareness raising campaign was launched in October, part of which was a number of briefing sessions (31 in total) – aimed at all staff across the Council.

9.3.3 The sessions were led for us by PDP, who are one of the leading external providers of DP training. They have the most comprehensive range of professional compliance training and all their courses are accredited by the Law Society. Their brief was to deliver the key DP messages as clearly and succinctly as possible and to ensure that staff were clear on what practical measures they needed to take process personal data in accordance with the Act.

9.3.4 The response to these sessions has been very positive in that they have clearly raised a great deal of interest (and concern) about DP issues and

about some the more recent challenges that go with the territory of partnership working, contracted-out services and other third party arrangements.

9.3.5 There is still a great deal to do over the next few months to ensure we are able to demonstrate real progress in putting in place some of the revised and new policies, procedures and practices. The Governance Team will be prioritising this work in preparation for the follow up Audit, which is expected to take place in January/February 2011.

10. LIST OF BACKGROUND PAPERS

10.1 None.

Legal: JEL

London Borough of Barnet Council

Data Protection Audit Report

v1.0

Auditors: Kai Winterbottom, Audit Team Manager
Christine Eckersley, Compliance Auditor
Claire Chadwick, Compliance Auditor
Paul Hamnett, Compliance Auditor

Distribution:

Final Report: Nick Walkley Chief Executive,
Jeff Lustig Director of Corporate Governance,
Sian Hughes Performance and OD Manager.

Report Issued: 29 June 2010

Contents

1. Background

1.1 During October 2009 the Information Commissioner concluded its review of a complaint relating to a Freedom of Information (FOI) request made to London Borough of Barnet. The review and a subsequent internal investigation conducted by the council, identified failings in the way the council had responded to and handled the request. An interest was expressed in further support from the Information Commissioner in respect of its handling of personal data.

1.2 The Director of Corporate Governance provided a full response to the Information Commissioner, detailing implemented changes and initiatives targeted at improving the councils handling of FOI responses.

1.3 The Information Commissioner may with the consent of the data controller assess any processing of personal data for the following of good practice and shall inform the data controller of the results of the assessment DPA s51(7).

1.4 Input was sought from the Council's Governance Team on the 15 January 2010 to inform a suitable scope for the audit which is intended will provide both the council and the ICO with an assurance as to the effectiveness of Data Protection Governance and internal controls and processes within the council.

1.5 The selected focus for the audit was the Human Resources and Children's Services directorates. In addition a review was conducted of the councils archiving unit at Mill Hill.

1.6 Subsequent to the completion of the audit fieldwork and outside the scope of the audit the ICO was informed by the Director of Corporate Governance of a significant security breach involving personal data. A USB data stick and CD containing unencrypted personal data regarding children and ex pupils of schools has been stolen from the home of a Children's Service employee. At the time of submitting this report the member of staff has been suspended pending internal investigation and the theft is the subject of an independent investigation. The breach will be independently addressed by the ICO's enforcement department.

In addition the council has implemented a number of retrospective controls to mitigate the risk of any further breaches. These include restrictions on removing laptops from council premises, removal of the ability to use USB sticks and the ability to write to CD. A detailed response has been provided to the ICO on the 29 April and will be updated on the 14 May 2010.

2. Audit Opinion

2.1. The purpose of the audit is to provide Barnet Council and the Information Commissioner with an assessment of how the Borough Council is meeting its data protection obligations

2.2. The recommendations made are primarily around enhancing processes and procedures although some proposed actions, such as those related to the handling of subject access requests, are necessary to achieve compliance.

Overall Conclusion	
Very Limited Assurance	On the basis of the work that we have performed we consider that the arrangements in place at Barnet Council at the time of the audit, with regard to data protection governance and controls, provide very limited assurance that processes and procedures are in place and being adhered to. There is therefore a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment. It should be recognized that in certain key areas the council has already identified opportunities which should improve its compliance with data protection regulations and good practice. The ICO also recognizes that some of the opportunities identified have not yet been approved/implemented and in other cases changes to policy procedure and structures are not yet embedded. We have made 2 No assurance and 2 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' section 7 of this report along with management responses.

3. Summary of Audit Findings

3.1 Areas of Good Practice.

3.1.1 The council has approved and adopted a Corporate Code of Governance in line with the CIPFA/SOLACE standards.

3.1.2 The Corporate Governance function has a documented Risk Management system which informs and populates the Corporate Risk Register and mandates the production of a risk register for each directorate which includes data protection concerns.

3.1.3 The Corporate Governance Director has clearly identified data protection governance and risks as an area requiring development and actively encouraged the involvement of the ICO to inform this process. Corporate Governance staff are attuned to data protection risks and are already addressing many of the key findings identified within this report.

3.1.4 It is reported that the Director of Corporate Governance will be further supported by the creation of an 'Assistant Director' role with responsibility for risk management and audit.

3.1.5 The process for dealing with recruitment and selection demonstrated a level of adherence to the recommended measures in the ICO's Employment Practices Code.

3.2 Areas for Improvement.

3.2.1 The Governance and Service Development Team in its current structure is embryonic. There is considerable pressure on the single Corporate Governance staffing resource available, to provide adequate support for Subject Access Requests and FOI requests. This is impacting the council's ability to respond to requests in a timely manner.

3.2.2 The Council currently has no formal reporting and measurement of compliance with its data protection responsibilities. Although internal audits have been completed for data protection and information security.

3.2.3 The Governance and Service Development Team were unclear as to what data protection training if any, is

provided to new starters. Personnel responsible for responding to subject access requests had not received appropriate training to support them in their role. (For example awareness of subject access procedures by those questioned was 30%, just 39% of staff questioned were aware of the statutory time limit of 40 days for the provision of a response to a SAR). The ICO would expect that personnel responsible for responding to subject access requests receive basic data protection training and receive appropriate guidance specific to their departments in how to handle, document and respond to requests.

3.2.4 Just 36% of Council staff questioned reported that they would report subject access requests to Link Officers, just 14% of staff would inform the link officer when the response to a SAR was sent out. As a consequence such requests will not have been updated on the database resulting in inaccurate management information.

3.2.5 The current FOI/SAR data base does not provide the Corporate Governance team with adequate and accurate management information, to provide an assurance of the council's compliance with its subject access responsibilities.

3.2.6 The council is not complying with its responsibility to respond to subject access requests within 40 days. Several subject access requests reviewed were significantly overdue with no action plan to resolve them. Several factors are contributing towards this; there is no effective monitoring of subjects access requests received, procedures for issuing subject access packs in some cases create unnecessary delays, personnel are not prioritising response to requests to enable them to respond within 40 days and the follow up procedures to prevent responses exceeding 40 days are ineffective.

4. Audit Approach

4.1. The audit was conducted following the Information Commissioner's Data Protection Audit Methodology and comprised an Adequacy Audit which reviewed documented policies and procedures and the Compliance Audit which involved an on-site visit and interviews with Barnet Council personnel.

4.2. An introductory meeting was held on the 15 January 2010 with the Corporate Governance team to establish an appropriate scope for the audit. It was agreed that the audit would be conducted within the Human Resources and Children's Services Directorate's.

4.3. Barnet Borough Council provided the Information Commissioner's Audit Group with access to policies, procedures, governance reports and internal audit reports relevant to the scope of the audit in preparation for the on site audit visits.

4.4. All interviews took place with staff on the main council premises at North London Business Park on the 22, 23 February and the 2, 3 March 2010. In addition a review was conducted of the council's archiving unit at Mill Hill.

5. Audit Scope

5.1 Following pre audit discussions with the Director of Corporate Governance and other members of the Governance Team, Information Assurance and I.T, it was agreed that the review would focus on the following areas:

a. Data protection governance within London Borough of Barnet with reference to its statements on internal controls, risk management strategy and risk registers.

b. Processes and procedures to manage the collection, access, content and movement of personal data, both manual and electronic, within the Human Resources; Recruitment and Selection, Disciplinary and Leavers functions and Children's Service. Including a review of the weeding and retention of records.

c. The effectiveness of the methods used to develop and maintain the awareness by staff within the identified directorates, of their responsibilities and accountabilities for data protection in their daily duties and behaviours.

d. The processes and systems in place to ensure subject access requests are dealt with in line with legislation and London Borough of Barnet procedures, with specific reference to both public and staff requests.

6. Audit Report Grading

6.1 Audit reports are graded with an overall assurance opinion, and any issues and associated recommendations are classified individually to denote their relative importance, in accordance with the definitions in the table below.

Colour Code	Internal Audit Opinion	Recommendation Priority	Definitions
	High assurance	Minor points only are likely to be raised	The arrangements for data protection compliance with regard to governance and controls provide a high level of assurance that processes and procedures are in place and being adhered to and that the objective of data protection compliance will be achieved. No significant improvements are required.
	Reasonable assurance	Low priority	The arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements and appropriate action has been agreed to enhance the likelihood that objective of data protection compliance will be achieved.
	Limited assurance	Medium priority	The arrangements for data protection compliance with regard to governance and controls provide only limited assurance that processes and procedures are in place and are being adhered to. The achievement of the objective of data protection compliance is therefore threatened.
	Very Limited assurance	High priority	The arrangements for data protection compliance with regard to governance and controls provide very limited assurance that processes and procedures are in place and being adhered to. There is therefore a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

7. Detailed Findings & Action Plan

7.1 Findings and recommendations flowing from the audit will be risk categorised using the criteria defined in Section 6. The rating will take into account the impact of the risk and the probability that the risk will occur.

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
7.1	**Data protection governance within London Borough of Barnet with reference to its statements on internal controls, risk management strategy and risk registers.**			
a.	The lack of a robust and consistent process for evaluating the effectiveness of the application of policies and procedures for managing data protection raises the risk that personal data may not be processed and managed in compliance with the DPA 1998, causing adverse impacts on individual's privacy with the potential for causing damage and distress to individuals.	• The Council have an Internal Control Checklist which is assessed annually. This process is co-ordinated by the Risk Manager and can inform the annual internal audit planning and is also available to external audit. • The ICO audit team did not review the internal control checklist during the audit and so are unable to comment on whether this checklist adequately covers data protection issues. • Based on the work completed 2008/09 the Head of Internal Audit identified Data Protection compliance as one of the key areas for improvement.		

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
a.		• In January 2009 the General Functions committee (responsible for approval of the constitution, structure and policies) approved the implementation of new or updated policies for Acceptable Usage, Data Protection, Information Security, Email and Internet and Passwords. • These policies have been provided to audit for review and appear to be fit for purpose however the majority are neither dated nor version controlled. • The council has a documented Risk Management framework which informs and populates the Corporate Risk Register and mandates the production of a risk register for each directorate.	1.1 When any policy is created or updated it should be allocated an appropriate owner, version controlled and dated and allocated an appropriate review date.	**Appendix A, 1.1 Owner Corporate Governance Implementation date, October 2010**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
a.		• The corporate risk register demonstrates that DP issues are recognised within the Risk Management System by highlighting six risks involving data protection; for example, risk numbers 6. The failure to discharge CRB checks. 22. The implementation of the WISDOM EDRM system 23. Implementation of the ICS system. 30. Poor data quality through failure to effectively use the ICS system. 31. Out of hours access to electronically held data 32. Significant increase in number of referrals.		

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
a.		• However, it was reported that the detail in risk registers varied between directorates and that it was unclear whether all directors clearly understood the relationship between issues, risks and residual risks. • By way of example risk 22 on the corporate register was reviewed. This revealed that the residual risk had been classified as 'risk removed' when the underlying activity continues. • The Director of Corporate Governance reports directly to the Chief Executive and has Data Protection oversight. It was stated that data protection governance will be further supported with the appointment of an Assistant Director responsible for Risk Management and Audit.	1.2 Barnet should ensure that all directorates receive sufficient guidance and support for the effective operation of the risk register 1.3 The Council should ensure that guidance and support is sufficient to equip those responsible with the necessary skills to; • Identify data protection issues • Identify data protection risks • Consider appropriate mitigating actions • Understand when to close risks	**Appendix A, 1.2** **Owner, Corporate Services / Audit / Risk to address** **Implementation date,** **Appendix A, 1.3** **Owner, Corporate Services / Audit / Risk to address** **Implementation date,**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
a.		• The intention is that this appointment will assist in improving communication between Audit and Risk Management. • Internal Audit conducted an audit into the arrangements for complying with data protection and submitted a report on the 16 February 2009, where they provided a no assurance rating. • A follow up review was conducted in March 2009 where agreed actions were reviewed to confirm the Councils progress against the six recommendations. • Of the six recommendations only one action has been fully implemented (Data Protection policy redraft). • Given the time elapsed since the audit report, the ICO would have expected further progress.		

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
a.		• Further recommendations around defining roles and responsibilities for Link and Data Protection Officer and data collection and processing have been partially implemented. • Whereas the risks around monitoring DPA compliance, management information and SARs have yet to be fully addressed pending further discussion. Further findings in these areas can be found under their relevant risks. • A paper was submitted to the Council Directors on 4 August 2009 (although year is not stated on document) entitled 'A review of Information Governance and Complaints'. This identified Data Protection as an area of concern due to the lack of visibility, ownership and consistency of policies.	1.4 The council should ensure that in regard to data protection issues recommendations made by Internal Audit or Corporate Governance receive timely consideration and implementation of mitigating actions. 1.5 Ensure the recommendations from the DP internal audit report are fully addressed with appropriate mitigating actions in a timely manner.	**Appendix A, 1.4** **Owner, Directors/Link Officers/SIRO's** **Implementation date, From September 2010** **Appendix A, 1.5** **Owner, Gov Team/Directors** **Implementation date, August 2010.**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
a.		• Directors agreed on the 4 August 2009 to set up a small team within Corporate Governance with responsibility for FOI, EIR, DP, SARs and Complaints. • The roles and structure of the Governance and Service Development Team have been approved but have yet to be formalised although a paper has been submitted which documents the structure and reporting lines. • The Director of Corporate Governance presented a 'Review of Data Protection Arrangements' paper to Directors on the 5 January 2010. This highlighted the loss or theft of mobile devices, ease of reference of policies and procedures, data protection related roles and responsibilities and staff awareness as key issues.	1.6 Sign off and implement the Governance and Service Development Team roles, structure and reporting lines as documented. 1.7 Identify and publicise clear DP contact(s) in Corporate Governance.	**Appendix A, 1.6** **Owner, Director of Corporate Governance** **Implementation date, September 2010** **Appendix A, 1.7** **Owner, Governance team** **Implementation date, September 2010**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
a.		• In February 2010, a draft internal audit report was submitted to Corporate Governance on Information Security. A 'no-assurance' rating was provided. • A network of Link Officers coordinated by Corporate Governance has been established and each directorate has a nominated officer. • The Link Officer role is to provide support for SAR requests and data protection guidance. The small team within Corporate Governance holds quarterly Link Officer meetings. • The role and identity of link officers were not always recognised within their own departments.	1.8 Corporate Governance should review the Link Officer role and incumbents to identify whether they possess sufficient seniority, authority and visibility within their departments.	**Appendix A, 1.8** **Owner, Governance team / Directors** **Implementation date, June 2010**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
a.		• The Governance and Service Development team has created a quarterly email/intranet bulletin publication (evidenced) which is issued to all staff to reinforce the key messages of the Link Officer meetings. • The council's intranet is currently being rebuilt. However, Information Governance intranet pages have been restructured to make them more accessible to staff and are now available via the home page of the intranet (evidenced by audit). • The council currently has no formal incident reporting procedure that may adequately encompass data protection and information security risks.	1.9 Ensure all DP related policies including (Acceptable Use, Information Security, Password policy) are clearly accessible through the new intranet site when it is fully operational. 1.10 Implement an incident reporting system to provide the Governance and service Development Team with management information to measure data protection compliance and direct future data protection related initiatives.	**Appendix A, 1.9** **Owner, Corporate Governance/Corporate Services** **Implementation date, October 2010** **Appendix A, 1.10** **Owner, Governance Team** **Implementation date, November 2010**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
a.		• The council does have a whistle blowing process but it was reported that this was unlikely to adequately address data protection issues, though it was unclear why. • The ICO audit team requested a meeting with the Caldicott Guardian. It was reported that there was some confusion within the council in identifying the person who held this responsibility. • However, prior to the audit visit it was identified that the Information Manager (ICS) held this post. Whilst his role is responsible for some Caldicott principles, the role appears to lack the required seniority, breadth of responsibility and professional social care experience advocated by the Caldicott Guardian Manual 2006.	1.11 Review Councils with Social Services Responsibilities (CSSR) guidance and the Caldicott Guardian Manual to decide if a Guardian is required. In the event that a Guardian is required the appropriate seniority and visibility should be attached to the role.	**Appendix A, 1.11** **Owner, Children's Service** **Implementation date,**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
a.		• There was no evidence that the council currently make use of the Information Governance Toolkit. Toolkit is not mandated but has been developed for voluntary use in CSSR's. • It was reported that the Governance and Service Development Team are liaising with colleagues from the Insight team and legal services to provide comments on a draft protocol for data sharing with the NHS trust . • The council appeared to have no mechanisms through which compliance with its data protection responsibilities could be assessed on a regular basis.	1.12 It should consider the implementation of the Information Governance Toolkit for CSSRs. 1.13 The council should ensure that it develops, implements and communicates a clear policy regarding data sharing (including guidance on developing protocols), which appropriately addresses data protection compliance and 'ICO Framework Code of Practice for sharing personal information'. 1.14 The council should have a system through which it can monitor its performance against its data protection responsibilities.	**Appendix A,1.12** **Owner, Children's Service** **Implementation date,** **Appendix A, 1.13** **Owner, Corporate Governance/Corporate Services** **Implementation date, October 2010** **Appendix A, 1.14** **Owner, Governance team** **Implementation date, from now ongoing**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
7. 2	**Processes and procedures to manage the collection, access, content and movement of personal data, both manual and electronic, within the Human Resources: Recruitment and Selection, Disciplinary and leavers functions and Children's Socials Services directorate. Including a review of the weeding and retention of records.**			
b.	A failure to provide and implement proper procedures for the processing of personal records raises the risk of inaccurate, excessive and out of date data causing damage and distress to individuals.	**Children's Service** • Children's Service case work documents are scanned onto WISDOM. The paper originals are then shredded, with the exception of certain legal documents which have to be retained (birth certificates, passports and court papers). • WISDOM is a system used to deliver electronic data records management (EDRM). • A risk has been highlighted on the corporate register, relating to problems with records identified as missing on WISDOM. This occurred during the back scanning exercise. All documents but 3 have been identified and correctly indexed.	. 2.1 The council should ensure that appropriate scanning procedures have now been implemented and that these ensure that personal information is held securely.	**London Borough of Barnet have decided that recommendations 2.1-2.11 will be owned by the HR Director; an action plan will be presented to the Directors Group and subsequently reported to the ICO after agreement.**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
b.		• Although the council has a 'Records Retention and Disposal guidelines' document. It was unclear what operational procedures the service has introduced to weed electronically held records on WISDOM. • WISDOM has the functionality to support automatic records archiving and deletion however this function is not currently 'switched on'. It was reported that discussion is ongoing as to how to address records retention within EDRM. • Full case records were being retained on the shared 'H drive' in addition to WISDOM. It was established that this was due to a distrust of WISDOM and perceived difficulties in accessing WISDOM on line.	2.2 Individual departments should clearly identify and communicate • Who is responsible for archiving and deleting records; • That procedures apply to both electronic and manual records. • When this should be done; and • Any audit trail or log that should be maintained to support this activity. 2.3 The council should closely monitor the duplication of client records to shared drives. It should further ensure that staff understand the consequences for non compliance with documented procedures when handling personal data.	

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
b.		• Social workers view and update cases on the Service ICS system. All Children's Service staff can search the ICS system for any open or closed case. • It was reported however that the ICS system does have audit trails, though it was reported that no one currently monitors this. • Any absence of monitoring of ICS system usage raises the risk that browsing and inappropriate disclosure or download of confidential records will not be identified. • Warning markers are used on ICS to alert social workers of key information relating to a client. The warning markers may identify various situations (such as violent clients or relatives, dangerous dogs on the premises).	2.4 The council should investigate whether all children's service personnel require access to all open and closed records. 2.5 The council should implement a proportionate system of monitoring or audit of access to ICS records, based on risk analysis. 2.6 The council should ensure: • That the decision to apply a marker about an individual is based on a specific incident or set of circumstances or expression of clearly identifiable concerns by a professional.	

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
b.		• The ICS system currently flags warning markers for review every 6 months. It was reported however that markers are not being reviewed in accordance with this schedule. • The admin team hold a copy of the manual 'legal file' which contains the original documents such as passports, birth certificates, and court papers. • These files are securely stored, while the case is active, under the control of the Admin Manager.	• The decision should be based on objective and clearly defined criteria in line with a clear and established policy and review procedure. • Senior nominated personnel in the service are responsible for making these decisions. Decisions should be reviewed regularly. *(ref ICO Good Practice Note –Use of Violent Warning Markers)*	

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
b.		• Once closed, fostering and adoption files are currently stored at Barnet House prior to the scanning and archiving process. • It was reported that the closed files stored at Barnet House are not locked away which raises the risk of inappropriate disclosure, loss or damage to records. • The archivist at the Mill Hill depot has a documented archiving process which is followed in Children's Service. • When historic records (such as previously closed cases) are required, they can normally be extracted within 24hrs.	2.7 The council should implement appropriate access controls for the files in storage at Barnet House to ensure their security	

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
b.		• An archive request form is used to extract records however there did not appear to be any validation or authorisation of requests within Children's service. • Although the council has a 'Records Retention and Disposal Guidelines' document. The Archivist reported difficulties in obtaining approval to destroy records once the destruction date had been reached. • Delays are also caused through the need for Children's Service to review the content of files to ensure that records were not destroyed that may be required in connection with more recently opened cases concerning the same individuals.	2.8 Requests for extraction of records from archive should be approved by line management. 2.9 The archivist should be suitably empowered and supervised to destroy records in line with documented and agreed retention schedules. 2.10 Directorates should document procedures for linking files (to update historic information where appropriate) to ensure that records for recently opened cases are complete.	

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
b.		• Day to day procedures for departmental shredding of documents requiring disposal, were not appropriate for the size and the length of time it takes to shred certain documents • During the audit it was noted that blue sacks were also in use for the disposal of confidential waste. Sacks which have to be requested sit on the floor and are not secured whilst awaiting collection. **Human Resources** • HR provides services to Barnet Council and to the schools in the surrounding area. • The recruitment application process demonstrated good adherence to best practice documented within the ICO's Employment Practices Code.	2.11 The council should implement an effective and appropriately secure method of handling confidential waste.	

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
b.		• Retention schedules are documented by the council's draft 'Records Retention and Disposal guidelines v0.001' and apply to categories of information. • Personnel interviewed however were not aware of any applicable retention policy relating to personal data they processed and held on local or shared drives. • There were no requirements to record collections of records held within teams. Ownership and management of these records was therefore unclear. • Some roles that the Resources team deal with require psychometric testing to be completed. The raw data (not just the summary) is kept on the HR file.	2.12 The council should formalise the guidelines and ensure that key managers and personnel understand how the data they handle is covered by the categories in the retention guidelines and schedules, *(As identified by the Governance Director in his 'Review of Data Protection Arrangements' paper, 5 January 2010).*	**London Borough of Barnet have decided that recommendations 2.12-2.17 will be owned by the Children's Service Director, an action plan will be presented to the Directors Group and subsequently reported to the ICO after agreement.**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
b.		• Access to psychometric records did not appear to be restricted and no additional security was applied to them. • Checks (references, CRB checks, etc) are only completed when the information is required after a job offer has been accepted. • There was a suggestion that records may be reviewed for obsolete information when personnel request access to their records. The ICO does not consider this activity to be good practice and could also be a breach of the 5th DPA principle.	2.13 Due to the potential for answers to be taken out of context, the ICO recommends that the access to raw data for psychometric testing should be restricted to an appropriately qualified member of staff. 2.14 HR should further ensure that psychometric records are reviewed after a suitable time to ensure they are still relevant.	

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
b.		• Information available by right to an individual is to information that the council holds at the time of the request, rather than the information that it is supposed to hold. • In removing information on the receipt of a request there is a risk that they are failing to adequately comply with the right of individuals. • There is a further risk that such activity could be regarded as deliberate in an attempt to avoid disclosure, thereby risking possible criminal prosecution. • HR holds all manual staff records centrally. Managers have to supply a valid business reason if they want to view any of the information held on staff records and such requests are considered on a case by case basis.	2.15 In addition to complying with documented retention policies and procedures, HR should ensure that all key personnel are aware that records should not be removed or deleted in response to a subject access request.	

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
b.		• Where disciplinary action (warnings, written, or final) are recorded on personnel records, there are clear policies in place for the weeding of the information. HR staff thought that there was no clear policy for what should be retained on the file when investigations do not result in action. • The Employee Lifecycle team handles work that deals with any form of change in relation to an active HR file. Work is dealt with using three systems depending on what needs to be amended; 'HR Connect' through which work is received 'WISDOM' which holds the central HR record of copies of documents; and 'SAP', which mainly deals with the Payroll	2.16 (See above recommendation 2.3)	

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
b.		• There was a duplication of employment related letters on the WISDOM system (which has only recently gone live) and the team drive. • Duplication of personal data presents a risk that information will not be managed effectively. (For example will all sets of information be appropriately updated)?	2.17 *(see recommendation 2.3)*	

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
7.3	**The effectiveness of the methods used to develop and maintain the awareness by staff within the identified directorates, of their responsibilities and accountabilities for data protection in their daily duties and behaviours.**			
C.	A failure to ensure an appropriate awareness by staff of their individual responsibilities for handling personal data raises the risk that privacy considerations are overlooked resulting in non compliant behaviour.	• The council are currently constructing a new Council intranet; there is a link to the old intranet where Corporate Governance pages are still located. • There is also a link to online induction training, although the content could not be reviewed by the ICO Audit team without a login. • The council has an induction programme and 18 week assessment procedure, which has 'Information Technology Security Issues and Data Protection' as a checklist item. • It was believed however that this training was left to the individual managers to cover with new starters.	3.2 Individual departments should be asked to review data protection content of induction training, with line managers. The council should have a corporate induction process which appropriately covers data protection matters, supplemented where required by local requirements.	**Appendix A, 3.2 Owner, Human Resources/Governance Team Implementation date, August 2010**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
C.		• Link officers received training provided by Amberhawk during March 2009. However Corporate Governance do not have an attendance list and due to staff turnover are unclear how many of the current group of link officers attended this. • Further dates have been scheduled in May and November 2010 (in addition to FOI training in March) to repeat this training for new and existing Link Officers as a refresher exercise. • The most recent versions of the Data Protection Policy, SAR procedure, SAR staff guidance and SAR Pack are located on the Corporate Governance intranet pages and reasonably easy to locate.		

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
C.		• No decision has yet been made on how to deliver training to all personnel. It was reported that an e learning package may be the preferred option however concerns exist as to its effectiveness. • Other than its publication on the intranet, no further activity has been undertaken to promote the new Data Protection Staff Guide and Policy within the council. • Staff interviewed advised that they had received some data protection training. Only 50% of staff questioned felt that they had received enough data protection training to support them in their role.	3.3 It is likely that training and awareness may be best achieved through a combination of approaches. The council should ensure that it implements a strategic cohesive approach to data protection and information security training from new starter through to refresher and role specific training. 3.4 The Governance Team should promote the guide within the intranet and through its quarterly communications.	**Appendix A, 3.3** **Owner, Governance Team /Communications/External input** **Implementation date, December 2010** **Appendix A, 3.4** **Owner, Governance team** **Implementation date, from now ongoing**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
C.		• Review of ICO complaints has revealed that the absence of a Data Protection Officer has caused the public some confusion. • Staff did provide examples of DP related guidance; communications provided quarterly by Corporate Governance, (for example, security of referrals to the police an update covering internal FOI reviews, security of personal data and logging of SAR requests). • Although there was a lack of data protection training across the directorates visited, there was a strong awareness of confidentiality of information.	3.5 In the absence of a clearly identifiable Data Protection Officer the Council should ensure that all staff are aware of whom their Link Officer is and how they can be contacted. In addition to this the website and policies should be updated to provide a clearly identifiable data protection contact for members of the public.	**Appendix A, 3.5** **Owner, Governance Team / Directors** **Implementation date, September 2010**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
7.4	**The processes and systems in place to ensure Subject Access requests are dealt with in line with legislation and London Borough of Barnet procedures, with specific reference to both public and staff requests.**			
d.	A failure to ensure Subject Access Requests are dealt with appropriately raises the risk that individuals rights to information may be compromised resulting in non compliance with the requirements of the Data Protection Act.	• The council's website states that the Information Governance Officer should be contacted in the event of a personal information request; no mention is made of what is required and the SAR pack is not available online. • Some directorates routinely respond in the first instance by sending a SAR pack out, even if they already have enough information for a valid SAR. • There was an inconsistency in approach to SARs between directorates. For example, a directorate may use their own pack and charge a fee while another may use the standard SAR pack and charge no fee.	4.1 Full guidance as to how to make a valid SAR should be readily available to the public i.e. on website. 4.2 Link Officers should be made aware that the provision and completion of a pack should not delay the provision of requested information response to compliance with a request within 40 days.	**Appendix A, 4.1** **Owner, Governance team / Directors** **Implementation date, December 2010** **Appendix A, 4.2** **Owner, Governance team / Directors** **Implementation date, December 2010**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
d.		• Link officers typically, will not be responsible for collating the information and responding to the request. This usually lies with the individual (e.g. social worker in Children's Services) receiving the request. • Requests should be logged on the central 'FOI Logging' database. The council has recognised that the current database is not fit for purpose as it does not reliably provide adequate management information. • There is no effective monitoring of the SAR log to ensure that requests are dealt with on time. • Where requests are 'cross cutting' (require data from more than one directorate) or complex they will be dealt with within the Corporate Governance team	4.3 Implement as a matter of urgency a means of reliably tracking and recording SARs (and FOI requests). The database should clearly identify • When request was received, pack sent and response provided; • Provide reminders prior to statutory due dates; • Indicate who is responsible; • Evidence senior manager or Corporate Governance review (where appropriate); • Document exemptions relied upon; • Document summary of information redacted	**Appendix A, 4.3 Owner, Governance team / Directors Implementation date, December 2010**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
d.		• During the audit the SAR log provided by the Children's Service was reviewed. For the period 15/07/09 – 26/01/10, 5/25 cases responded to had exceeded the statutory 40 day time limit. A further 7/25 cases remained open outside the 40 day period; this demonstrates non compliance with the sixth principle of the DPA 98. • Not all requests are reported to the Link Officer. The ICO can therefore have no assurance that the council can demonstrate that it is complying with its subject access responsibilities under the DPA. • In Children's Service 8 individual SAR cases were reviewed with the social worker responsible for responding to the request.	4.4 The council must ensure that it complies with all requests within the statutory time frame of 40 days. 4.5 The council should document a clear universal process that applies to all directorates and clearly describes individual responsibilities. 4.6 They should further ensure that all directorates adopt the process.	**Appendix A, 4.4-4.6 Owner, Governance Team / Directors Implementation date, December 2010** **Appendix A, 4.4-4.6 Owner, Governance Team / Directors Implementation date, December 2010** **Appendix A, 4.4-4.6 Owner, Governance Team / Directors Implementation date, December 2010**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
d.		• In 1 case the response had been provided outside the 40 day period and the remaining cases were unresolved outside the 40 day period; demonstrating non compliance with the sixth principle. • It was reported that the Link Officer responsible for subject access requests in HR had not received any requests. • Staff responsible for responding to requests reported that they had received little if any DPA training and that no training had been provided in handling and responding to subject access requests. • It was also noted that the corporate SAR report for the period did not reconcile with the Children's Services own log.	4.7 Clear guidance and support should be delivered to Link Officers and individuals who respond to SARs within departments. Training should provide practical examples and discuss how to apply relevant exemptions. 4.8 The SAR database should provide adequate Management information for directorates and the Governance Team at a corporate level to effectively manage performance.	**Appendix A, 3.3 Owner, Governance Team / Communications / External input Implementation date, December 2010** **Appendix A, 4.3 Owner, Governance team / Directors Implementation date, December 2010**

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
d.		• During the time spent within HR it was noted that although requests have not been logged as SARs, HR do process and respond to subject access requests. • In HR just 2 cases had been reported for the period reviewed. In both cases a complaint had been made to the ICO and upheld as compliance unlikely. Both cases had: Exceeded the 40 day time limit and in 1 case were still open (112 days). Involved an inappropriate application of an exemption under the DPA 1998. • The ICO guidance on handling SAR states that in many cases the best way of responding to requests may be through treating them as business as usual.		

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
d.		• It was evident that HR employees did not recognise requests received in the normal course of business as subject access requests. Due to their own SLAs such requests were being handled within the 40 day time limit. • Although directorate personnel reported that they receive follow up calls from Link Officers to remind them of deadlines, this activity is clearly ineffective. • There was evidence that a lack of clearly prescribed processes for handling and responding to requests were contributing to the delays in providing the information requested.	See recommendations (4.5/4.6) 4.9 It is imperative that Link Officers have the appropriate seniority and competence to perform the role.	**Appendix A, 4.9** **Owner, Governance Team / Directors** **Implementation date, June 2010**

The agreed actions may be subject to a follow up audit to establish whether they have been implemented.

7.6 Any queries regarding this report should be directed to Kai Winterbottom, ICO Audit Group.

7.7 During our audit, all the employees that we interviewed were helpful and co-operative. This assisted the audit team in developing an understanding of Barnet Council, their policies and procedures. The following staff members were particularly involved in organising the audit:

- Sian Hughes, Performance and OD Manager
- Jeff Lustig, Director of Corporate Governance

DATA PROTECTION ACTION PLAN

Actions arising out of the ICO Audit

FINDINGS	Report Recommendation:	Owner:	Timescales:	Completion By:	Progress	Comments
In January 2009 the General Functions committee (responsible for approval of the constitution, structure and policies) approved the implementation of new or updated policies for Acceptable Usage, Data Protection, Information Security, Email and Internet and Passwords. These policies have been provided to audit for review and appear to be fit for purpose however the majority are neither dated nor version controlled.	**1.1:** When a policy is created or updated, it should be allocated an appropriate owner, version controlled, dated and given an appropriate review date	Information Gov Council	From now	End Oct 10	In Progress	Work is on-going on a programme of Information Management projects. A review/update of DP and data security policies is underway to create a more streamlined policy framework with overall ownership/version control being with the Governance Team
However, it was reported that the detail in risk registers varied between directorates and that it was unclear whether all directors clearly understood the relationship between issues, risks and residual risks.	**1.2:** Barnet should ensure that all directorates receive sufficient guidance and support for the effective operation of the risk register	Corporate Services/Risk to address			In Progress	Training and new system rolled out, with ongoing support - each directorate having a named 'risk officer' Risk Management Strategy to be published within 'Key Documents' on the intranet
By way of example risk 22 on the corporate register was reviewed. This revealed that the residual risk had been classified as 'risk removed' when the underlying activity continues.	**1.3:** The Council should ensure that guidance and support is sufficient to equip those responsible with the necessary skills to identify DP issues, identify DP risks, consider appropriate mitigating actions and understand when to close risks	Corporate Services/Audit/Risk to address			In Progress	Further guidance will be provided Link Officers in the InfoGov newsletters
Whereas the risks around monitoring DPA compliance, management information and SARs have yet to be fully addressed pending further discussion. Further findings in these areas can be found under their relevant risks.	**1.4:** The Council should ensure that in regard to DP issues recommendations made by Internal Audit or Corporate Governance receive timely consideration and implementation of mitigating actions	Directors/Link Officers/SIRO's	From September '10	On-going	In Progress	These will be actioned as part of this plan
A paper was submitted to the Council Directors on 4 August 2009 (although year is not stated on document) entitled 'A review of Information Governance and Complaints'. This identified Data Protection as an area of concern due to the lack of visibility, ownership and consistency of policies.	**1.5** Ensure the recommendations from the DP Internal Audit report are fully addressed with appropriate mitigating actions in a timely manner	Gov Team/Directors	From now	End Dec 2010	In Progress	These will be actioned as part of this plan
The roles and structure of the Governance and Service Development Team have been approved but have yet to be formalised although a paper has been submitted which documents the structure and reporting lines.	**1.6:** Sign off and implement the Governance and Service Development Team roles, structures and reporting lines as documented (this is a reference to the CDG reports of August and October 09)	Director of Corporate Governance	ASAP	01-Dec-10	In Progress	The restructure is now progressing as part of a wider Corporate Governance restructure
	1.7: Identify and publicise clear DP contacts in Corporate Governance	Governance Team	ASAP	30-Sep-10	In Progress	Intranet and Internet to be updated. Also to be communicated as part of the awareness campaign and via the InfoGov Newsletter
The role and identity of link officers were not always recognised within their own departments.	**1.8:** Corporate Governance should review the Link Officer role and incumbents to identify whether they possess sufficient seniority, authority and visibility within their departments (**4.9:** it is imperative that Link Officers have the appropriate seniority and competence to perform the role)	Gov Team/Directors	From now	End June 2010	Completed	Directors have reviewed and confirmed their Link Officers. This will be regularly reviewed
The council's intranet is currently being rebuilt. However, Information Governance intranet pages have been restructured to make them more accessible to staff and are now available via the home page of the intranet (evidenced by audit).	**1.9:** Ensure all DP related policies including Acceptable Use, Information Security and Password are clearly accessible through the new intranet site when it is fully operational	Governance Team / Corporate Services	From now	End Oct 2010	In Progress	Now published within 'Key Documents'. IS and the Governance Team have agreed an urgent review/update of all 'IS' policies relating to DP including data security and transfer. This review will be led by the Governance Team
The council currently has no formal incident reporting procedure that may adequately encompass data protection and information security risks.	**1.10:** Implement an incident reporting system to provide the Governance and Service Development Team with management information to measure DP compliance and direct future DP related initiatives	Governance Team	From Aug 2010	End Nov 2010	In Progress	Risks are captured through the new risk management process/system. Work has begun on an Incident Reporting procedure

FINDINGS	Report Recommendation:	Owner:	Timescales:	Completion By:	Progress	Comments
The ICO audit team requested a meeting with the Caldecott Guardian. It was reported that there was some confusion within the council in identifying the person who held this responsibility.	**1.11:** Review 'Council's with Social Services Responsibilities (CSSR) guidance and the Caldecott Guardian manual to decide if a guardian is required. In the event that a Guardian is required the appropriate seniority and visibility should be attached to the role (**1.12:** consideration should also be given to the implementation of the Information Governance Toolkit for CSSRs)	Children's	From June 2010	01-Aug-10	Completed	The service has set up a Data Governance Group that has the Caldicott Guardian and Risk Officer as members. Clear guidelines have been written regarding the different roles. The group will cover all aspects of data protection and data security.
There was no evidence that the council currently make use of the Information Governance Toolkit. Toolkit is not mandated but has been developed for voluntary use in CSSR's.	**1.12** It should consider the implementation of the Information Governance Toolkit for CSSRs.	Children's	From June 2010	The work of the DGG will be ongoing	Completed	See comments above - The Information Governance Toolkit has been used to inform the work of the Data Governance Group
It was reported that the Governance and Service Development Team are liaising with colleagues from the Insight team and legal services to provide comments on a draft protocol for data sharing with the NHS trust .	**1.13:** The Council should ensure that it develops, implements and communicates a clear policy regarding Data Sharing (including guidance on developing protocols), which appropriately addresses data protection compliance and 'ICO Framework Code of Practice for sharing personal information'	Governance Team	From now	End Dec 2010	In Progress	Work has begun of Sharing Protocols and guidance for services on data sharing arrangements and the drafting of those arrangements
The council appeared to have no mechanisms through which compliance with its data protection responsibilities could be assessed on a regular basis.	**1.14:** The Council should have a system through which it can monitor its performance against its data protection responsibilities	Governance Team	From now	ongoing	Not Started	Work is on-going on a programme of Information Management projects. A review/update of DP and data security policies is underway to create a more streamlined policy framework with overall ownership/version control being with the Governance Team
A risk has been highlighted on the corporate register, relating to problems with records identified as missing on WISDOM. This occurred during the back scanning exercise. All documents but 3 have been identified and correctly indexed.	**2.1** The council should ensure that appropriate scanning procedures have now been implemented and that these ensure that personal information is held securely.	Children's	From June 2010	01-Dec-10	Completed	Information Systems working practices are continuously under review. The specific point regarding Wisdom is being addressed
Although the council has a 'Records Retention and Disposal guidelines' document. It was unclear what operational procedures the service has introduced to weed electronically held records on WISDOM.	**2.2** Individual departments should clearly identify and communicate • Who is responsible for archiving and deleting records; • That procedures apply to both electronic and manual records. • When this should be done; and • Any audit trail or log that should be maintained to support this activity.	Children's	From June 2010	01-Dec-10	In Progress	This is link with item 2.9. Procedures are being reviewed and will then be communicated to all staff
Full case records were being retained on the shared 'H drive' in addition to WISDOM. It was established that this was due to a distrust of WISDOM and perceived difficulties in accessing WISDOM on line.	**2.3** The council should closely monitor the duplication of client records to shared drives. It should further ensure that staff understand the consequences for non compliance with documented procedures when handling personal data.	Children's	From June 2010	01-Mar-11	In Progress	A review of the shared areas and the use of the 'H' drive is taking place across the whole Children's Service. The outcome will be to rationalise the use of shared areas to ensure data protection and security best practice is followed
Social workers view and update cases on the Service ICS system. All Children's Service staff can search the ICS system for any open or closed case.	**2.4** The council should investigate whether all children's service personnel require access to all open and closed record**s.**	Children's	From June 2010	01-Dec-10	Completed	Information Systems working practices are continuously under review. The specific points in the ICO audit are being addressed. Not all Children's Service staff have access - only those staff with a username and password. A review of user accounts requested
It was reported however that the ICS system does have audit trails, though it was reported that no one currently monitors this.	**2.5** The council should implement a proportionate system of monitoring or audit of access to ICS records, based on risk analysis.	Children's	From June 2010	01-Dec-10	Completed	The Data Governance Group will be monitoring access on a monthly basis
Warning markers are used on ICS to alert social workers of key information relating to a client. The warning markers may identify various situations (such as violent clients or relatives, dangerous dogs on the premises).	The council should ensure: • That the decision to apply a marker about an individual is based on a specific incident or set of circumstances or expression of clearly identifiable concerns by a professional.	Children's	From June 2010	01-Dec-10	In Progress	Information Systems working practices are continuously under review. The specific points in the ICO audit are being addressed

FINDINGS	Report Recommendation:	Owner:	Timescales:	Completion By:	Progress	Comments
The ICS system currently flags warning markers for review every 6 months. It was reported however that markers are not being reviewed in accordance with this schedule.	The council should ensure: • The decision should be based on objective and clearly defined criteria in line with a clear and established policy and review procedure. • Senior nominated personnel in the service are responsible for making these decisions. Decisions should be reviewed regularly. (ref ICO Good Practice Note –Use of Violent Warning Markers)	Children's	From June 2010	01-Dec-10	In Progress	Information Systems working practices are continuously under review. The specific points in the ICO audit are being addressed
It was reported that the closed files stored at Barnet House are not locked away which raises the risk of inappropriate disclosure, loss or damage to records.	**2.7** The council should implement appropriate access controls for the files in storage at Barnet House to ensure their security	Children's	From June 2010	01-Dec-10	Completed	All case files have now been moved to secure storage at NLBP. The duty staff at Barnet House will be provide with lockable storage for their duty case work
An archive request form is used to extract records however there did not appear to be any validation or authorisation of requests within Children's service.	**2.8** Requests for extraction of records from archive should be approved by line management.	Children's	From June 2010	31-Mar-11	In Progress	A review of the current archiving process is being undertaken. This will include updated procedures which will be communicated to all staff. This particular action will also be linked to 2.8
Although the council has a 'Records Retention and Disposal Guidelines' document. The Archivist reported difficulties in obtaining approval to destroy records once the destruction date had been reached.	**2.9** The archivist should be suitably empowered and supervised to destroy records in line with documented and agreed retention schedules.	Children's	From June 2010	31-Mar-11	In Progress	A review of the current archiving process is being undertaken. This will include updated procedures which will be communicated to all staff. This particular action will also be linked to 2.8
Delays are also caused through the need for Children's Service to review the content of files to ensure that records were not destroyed that may be required in connection with more recently opened cases concerning the same individuals.	**2.10** Directorates should document procedures for linking files (to update historic information where appropriate) to ensure that records for recently opened cases are complete.	Children's	From June 2010	31-Mar-11	In Progress	Action on this is linked to 2.8 and 2.9
During the audit it was noted that blue sacks were also in use for the disposal of confidential waste. Sacks which have to be requested sit on the floor and are not secured whilst awaiting collection.	**2.11** The council should implement an effective and appropriately secure method of handling confidential waste.	Children's	From June 2010	01-Aug-10	Completed	The large number of sacks during the visit were due to the pending move of the Children's Service to the ground floor. The amount of confidential waste that normally needs to be destroyed is dealt with using free standing shredders
Personnel interviewed however were not aware of any applicable retention policy relating to personal data they processed and held on local or shared drives.	**2.12** The council should formalise the guidelines and ensure that key managers and personnel understand how the data they handle is covered by the categories in the retention guidelines and schedules, (As identified by the Governance Director in his 'Review of Data Protection Arrangements' paper, 5 January 2010).	HR	From 1 Aug 2010	End Dec 10	In Progress	HR have redrafted a Managers Induction Pack. The Governance Team have inputted to the DP aspects of the pack The Records Retention & Disposal Guidelines are under review and work is underway with departments to update. HR have already completed this work
Access to psychometric records did not appear to be restricted and no additional security was applied to them.	**2.13** Due to the potential for answers to be taken out of context, the ICO recommends that the access to raw data for psychometric testing should be restricted to an appropriately qualified member of staff.	HR	From 1 Aug 2010	End Aug 2010	Completed	This report finding was inaccurate Psychometric testing is always carried out by an agency and only for certain staff groups
	2.14 HR should further ensure that psychometric records are reviewed after a suitable time to ensure they are still relevant.	HR	From 1 Aug 2010	End Aug 2010	Completed	Psychometric tests are used purely for the purpose of appointment and are not referred to or use after appointment has taken place. Therefore reviewing of this information is not required.

FINDINGS	Report Recommendation:	Owner:	Timescales:	Completion By:	Progress	Comments
Information available by right to an individual is to information that the council holds at the time of the request, rather than the information that it is supposed to hold.	**2.15** In addition to complying with documented retention policies and procedures, HR should ensure that all key personnel are aware that records should not be removed or deleted in response to a subject access request.	HR	From 1 Aug 2010	End Jan 2011	In Progress	All HR staff have been reminded of the basics of Subject Access and Data Protection responsibilities (completed) Purging of employee files is being undertaken as part of transferring records from paper to electronic media (via WISDOM Project) (scanning on-going, scheduled to complete in January 2011)
Where disciplinary action (warnings, written, or final) are recorded on personnel records, there are clear policies in place for the weeding of the information. HR staff thought that there was no clear policy for what should be retained on the file when investigations do not result in action.	**2.16** (See above recommendation 2.3) The council should closely monitor the duplication of client records to shared drives. It should further ensure that staff understand the consequences for non compliance with documented procedures when handling personal data.	HR	From 1 Aug 2010	End Nov 2010	Completed	All HR Staff have been reminded of Data Protection Policy and their own responsibilities under the Policy & Act The HR Management Team have been requested to review all records held on Shared Drives including ensuring all those that have access are identified and those who should not have access are removed
Duplication of personal data presents a risk that information will not be managed effectively. (For example will all sets of information be appropriately updated)?	**2.17** (see recommendation 2.3) The council should closely monitor the duplication of client records to shared drives. It should further ensure that staff understand the consequences for non compliance with documented procedures when handling personal data.	HR	From 1 Aug 2010	End Nov 2010	Completed	All HR Staff have been reminded of the Data Protection Policy and their own responsibilities under the Policy & Act The HR Management Team have been requested to review all records held on Shared Drives including ensuring all those that have access are identified and those who should not have access are removed
The council has an induction programme and 18 week assessment procedure, which has 'Information Technology Security Issues and Data Protection' as a checklist item. It was believed however that this training was left to the individual managers to cover with new starters.	**3.2:** Individual departments should be asked to reviews DP content of induction training with line managers. The Council should have a corporate induction process which appropriately covers DP matters, supplemented where required by local requirements	HR / Governance	From 1 June '10	End Dec 2010	In Progress	HR have renewed the license for the e-learning induction, which covers DP quite comprehensively. Thought to be given to the process for ensuring new starters are sent a link and log in details. HR/Governance Team are working on the contract template for new starters to make sure the references to DP responsibilities is made more explicit
No decision has yet been made on how to deliver training to all personnel. It was reported that an e learning package may be the preferred option however concerns exist as to its effectiveness.	**3.3:** The Council should ensure that it implements a strategic cohesive approach to DP and information security training from new starter through to refresher and role specific training	Gov Team/Communications/external input		End Nov 2010	In Progress	Awareness campaign due to be completed at the end of December. Posters (inc giant posters), screen savers, plasma screen presentation, intranet articles and DP training sessions for all staff have been underway during October/November. A further plan of action will address emerging issues
Other than its publication on the intranet, no further activity has been undertaken to promote the new Data Protection Staff Guide and Policy within the council.	**3.4:** The Governance And Service Development Team should promote the DP staff guide within the intranet and through its quarterly communications			Ongoing	In Progress	The DP Policy and Guidance now accessible through 'Key Documents'. First team will promote through the communications campaign. This will also be the subject of more detailed articles in the InfoGov newsletter
Review of ICO complaints has revealed that the absence of a Data Protection Officer has caused the public some confusion.	**3.5:** in the absence of a clearly identifiable DP Officer the Council should ensure that staff are aware of whom their Link Officer is and how they can be contacted. In addition to this the website and policies should be updated to provide a clearly identifiable DP contact for the public	Gov Team/Directors	ASAP	1 Sept '10	In Progress	Link Officers have been confirmed by Directors and work to publicise the Governance Team has started in earnest through the 31 DP sessions
The council's website states that the Information Governance Officer should be contacted in the event of a personal information request; no mention is made of what is required and the SAR pack is not available online.	**4.1:** Full guidance as to how to make a valid SAR should be readily available to the public i.e. on the website (**4.4:** The Council should document a clear universal process that applies to all directorates and clearly describes individual responsibilities and that **4.6:** they should ensure all directorates adopt the process)	Gov Team/Directors	From now	End December '10	In Progress	A new Subject Access Request pack for members of the public and revised, updated and enhanced guidance for Link Officers is underway - with a view to publishing by the end of December. InfoGov newsletter to also pick up the key points

FINDINGS	Report Recommendation:	Owner:	Timescales:	Completion By:	Progress	Comments
Some directorates routinely respond in the first instance by sending a SAR pack out, even if they already have enough information for a valid SAR.	**4.2:** Link Officers should be made aware that the provision and completion of a pack should not delay the provision of requested information response to compliance with a request within 40 days (**4.4:** The Council must ensure it complies with all requests within the statutory timeframe of 40 days)	Gov Team/Directors	From now	End December '10	In Progress	Reminders to Link Office via the InfoGov newsletter, and guidance pack and through the performance monitoring framework
Requests should be logged on the central 'FOI Logging' database. The council has recognised that the current database is not fit for purpose as it does not reliably provide adequate management information.	**4.3:** Implement as a matter of urgency a means of reliable tracking and recording of SARs. The database should satisfy a number of key criteria as listed in the report	Gov Team/Directors	Underway	End December '10	In Progress	After extensive work the internal Customer Relations Management system is not a viable system and too costly to develop to meet the requirements of DP An alternative system has been identified. Directors have agreed in principle - a development bid to be submitted for its implementation (from January) and its ongoing maintenance
During the audit the SAR log provided by the Children's Service was reviewed. For the period 15/07/09 – 26/01/10, 5/25 cases responded to had exceeded the statutory 40 day time limit. A further 7/25 cases remained open outside the 40 day period; this demonstrates non compliance with the sixth principle of the DPA 98.	**4.4** The council must ensure that it complies with all requests within the statutory time frame of 40 days.	Governance Team		Nov-10	In Progress	Reminders to Link Officers via the InfoGov newsletter, and guidance pack and through the performance monitoring framework
Not all requests are reported to the Link Officer. The ICO can therefore have no assurance that the council can demonstrate that it is complying with its subject access responsibilities under the DPA.	**4.5** The council should document a clear universal process that applies to all directorates and clearly describes individual responsibilities. **4.6** They should further ensure that all directorates adopt the process.	Governance Team		End Nov 2010	In Progress	A new Subject Access Request pack for members of the public and revised, updated and enhanced guidance for Link Officers is underway with a view to publishing by the end of December. InfoGov newsletter to also pick up the key points
Staff responsible for responding to requests reported that they had received little if any DPA training and that no training had been provided in handling and responding to subject access requests.	**4.7:** Clear guidance and support should be delivered to Link Officers and individuals who respond to SARs within departments. Training should provide practical examples and discuss how to apply relevant exemptions	Governance Team		End Nov 2010	Not Started	Subject Access Requests covered briefly in the DP session but more detailed training is planned for Link Officers in early 2011 to focus more specifically on those requests for personal data
It was also noted that the corporate SAR report for the period did not reconcile with the Children's Services own log.	**4.8:** The SAR database should provide adequate management information for directorates and the Governance and Service Development Team at a corporate level to effectively manage performance	Governance Team		End Nov 2010	Not Started	After extensive work the internal Customer Relations Management system is not a viable system and too costly to develop to meet the requirements of DP An alternative system has been identified. Directors have agreed in principle - a development bid to be submitted for
It was evident that HR employees did not recognise requests received in the normal course of business as subject access requests. Due to their own SLAs such requests were being handled within the 40 day time limit.	See recommendations (4.5/4.6)			End Nov 2010	Not Started	A new Subject Access Request pack for members of the public and revised, updated and enhanced guidance for Link Officers is underway with a view to publishing by the end of December. InfoGov newsletter to also pick up the key points
Although directorate personnel reported that they receive follow up calls from Link Officers to remind them of deadlines, this activity is clearly ineffective.	**4.9** It is imperative that Link Officers have the appropriate seniority and competence to perform the role.			End Nov 2010	Completed	This has been addressed with Directors and the list has been reviewed