AGENDA ITEM: 9 Pages 1 – 19

Meeting	Cabinet Resources Committee
Date	19 July 2010
Subject	**Independent investigation into data loss incident**
Report of	Leader of the Council Deputy Leader of the Council/Cabinet Member for Education, Children and Families
Summary	This report summarises the findings and recommendations of the independent investigation undertaken as a result of a data loss at the Council in March 2010.

Officer Contributors	Jeff Lustig, Director of Corporate Governance Robert McCulloch-Graham, Director of Children's Service
Status (public or exempt)	Public
Wards affected	All
Enclosures	Appendix – Final Report of Investigation (June 2010)
For decision by	Cabinet Resources Committee
Function of	Executive
Reason for urgency / exemption from call-in (if appropriate)	Not applicable

Contact for further information: Alice Bolton, alice.bolton@barnet.gov.uk, 020 8359 3057.

1. RECOMMENDATIONS

1.1 That the findings and recommendations of the independent investigation be noted

1.2 That officers are instructed to implement the recommendations of the report across the Council.

2. RELEVANT PREVIOUS DECISIONS

2.1 None.

3. CORPORATE PRIORITIES AND POLICY CONSIDERATIONS

3.1 Ensuring that personal data is effectively and appropriately safeguarded and used by all Council services will help to improve the reputation of the Council as a trusted public body, acting in the best interests of residents and service users. Enabling staff to use and share data securely and appropriately is essential in order to provide high quality, personalised and targeted services to service users. This will help to meet the corporate priority of 'Sharing opportunities, sharing responsibilities'. Helping staff to work effectively and efficiently will contribute to the corporate priority of 'Better services for less money'.

4. RISK MANAGEMENT ISSUES

4.1 If the identified recommendations are not implemented, there is a risk that a further data loss could occur. There would also be a reputational risk to the Council if the recommendations of the independent investigation are not complied with.

4.2 The Information Commissioner's Office is also able to impose a fine on the council if it believes the correct steps are not being taken to prevent further data loss.

4.3 Any loss of personal data, particularly relating to children or vulnerable adults, carries an associated safeguarding risk. Ensuring that all recommendations from the independent investigation are implemented will ensure that this risk is minimised.

5. EQUALITIES AND DIVERSITY ISSUES

5.1 The proposed course of action has been considered and does not have any adverse equalities implications on specific groups.

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

Finance

6.1 Some of the recommendations may have associated resource implications. These will be met from existing budgets where possible.

7. LEGAL ISSUES

7.1 The Data Protection Act 1998 establishes a framework designed to safeguard personal data and to enable access to data by 'data-subjects'. Any organisation that 'processes' personal data must notify with the Information Commissioner, comply with the Act and handle the personal data in accordance with the data protection principles set out in the Act.

7.2 The Information Commissioner has power to impose sanctions for non-compliance with the Act and its principles.

8. CONSTITUTIONAL POWERS

8.1 The Council's constitution in Part 3, Responsibility for Functions, paragraph 3.6 sets out the terms of reference of the Cabinet Resources Committee including to develop and recommend to Cabinet for adoption an e-Government strategy and associated ICT policies and strategies[1].

9. BACKGROUND INFORMATION

9.1 In March 2010, a large volume of unencrypted data containing information about pupils in Barnet schools was stolen as a result of a burglary at a member of staff's home address. The Council learned about this on Monday 15 March and reported the loss to the Information Commissioner's Office (ICO). The Council subsequently took a set of remedial actions and as part of its commitment to affected parents indicated it would establish an independent review of the incident.

9.2 An independent review was commissioned that was tasked with establishing whether the data loss was an isolated incident or indicative of a wider set of problems across the Council.

9.3 The review process involved examining council policies and procedures and interviewing staff in the Children's Service and in the Corporate Governance directorate.

9.4 The report found that there were two factors that combined directly to give rise to the data loss. Firstly data security did not have the level of priority that it needed and secondly staff and management awareness of data protection was not sufficient to minimise the risk of losing personal data. The report also outlines a number of areas of good practice.

9.5 A number of recommendations were made and these are listed below. The main priority areas in the recommendations are to raise staff and management awareness of data protection, to improve management control systems and to refine HR processes to support data protection.

Recommendation	Priority next 6 Months	Priority next 12 months
1. Develop the roles of Senior Information Risk Officer (SIRO) and Caldicott Guardian to ensure the development of appropriate governance and confidentiality processes within the Children's Service (CS).	**X**	
2. Develop similar SIRO and Caldicott arrangements within Adult Social Care if not already in place.	**X**	
3. Appoint a SIRO for the Council. This is a Local Government Association (LGA) recommendation. It has a specific role in terms of information risk that could be incorporated into an existing senior manager role.	**X**	

[1] Data Protection comes within the ICT strategies.

Recommendation	Priority next 6 Months	Priority next 12 months
4. Clarify the Information Asset Owner for the information systems in each directorate. The role will include overall responsibility for data quality and data handling though specific actions may be delegated.		**X**
5. Implement Data Protection (DP) awareness training for all new starters and annual refresher training for staff that handle personal data.	**X**	
6. Ensure that job descriptions for posts that handle personal data explicitly address DP issues.		**X**
7. Update HR policies to ensure that they emphasise the importance of good data protection practice and the seriousness of failing to comply.		**X**
8. Implement and publicise mechanisms for bringing concerns about information risk to the attention of senior managers. This is also an ICO audit recommendation.	**X**	
9. Take the opportunity provided by the election of new councillors to provide a member briefing on DP issues.	**X**	
10. Review the storage for personal information on Council premises away from the NLBP to ensure that it is secure.	**X**	
11. Ensure that photographs are securely stored and have the required authorisation for use.	**X**	
12. Ensure that lockable storage of personal paper records kept on site can always be locked.		**X**
13. Ensure that personal data on the Apple Mac computers held by youth service is securely stored.	**X**	
14. Maintain the current tight controls on removable storage and review the approval process to ensure that exceptions are considered speedily.		**X**
15. Make the use of secure email mandatory for those teams that exchange a high volume of personal data.		**X**
16. Brief staff and managers on the use of shared drives with appropriate access conditions to improve data quality.		**X**
17. Where teams or sections process a high volume of personal information include a DP target in the manager's annual appraisal.		**X**
18. Review the role of DP link Officers in the light of the recommendations of this report and the ICO audit report.	**X**	
19. Review and consolidate the reporting arrangements for Freedom of Information (FOI), Subject Access Requests (SAR) and DP in the light of the recommendations of this report and the ICO audit report.	**X**	

Recommendation	Priority next 6 Months	Priority next 12 months
20. Use the Information Governance Toolkit in Children's Services and in Adult Social Care. This is also a recommendation of the ICO audit.		**X**
21. Move to an Electronic Records and Document Management System (ERDMS) solution for those areas of the Children's Service using paper based systems as soon as resources allow.		**X**
22. Conduct Privacy Impact Assessments (PIA) on new systems.		**X**
23. Develop an Information Strategy for the Council that gives a clear direction of travel.		**X**
24. While paper records are in use, ensure that management systems are in place to monitor adherence to the policy on Retention of Documentation and Destruction of Files.		**X**
25. Develop compliance testing on DP policies by directorates and report annually through the corporate SIRO to the Corporate Director's Group.	**X**	
26. Update existing data protection policies and address data security issues arising from remote working; include an owner, version control, a date of issue and review date as recommended by the ICO audit.		**X**

9.6 Prior to this data loss incident, the council had already been working on a voluntary basis with the Information Commissioner's Office (ICO) audit team to improve data protection and information security across the council.

9.7 The ICO were satisfied with the prompt actions taken by the Council subsequent to the loss of pupil data, and with the undertaking given as to the future steps the Council would take; the ICO therefore did not judge that any enforcement action was required as a result of this incident. A further audit will be carried out by the ICO later in the financial year to assess progress against the recommendations.

10. LIST OF BACKGROUND PAPERS

10.1 None.

Legal – SS
CFO – DM

Investigation into Data Loss at Barnet Council March 2010

Final Report

June 2010

Background
This investigation came about because a large volume of unencrypted pupil data had been stolen as a result of a burglary at a member of staff's home address. The Council learned about this on Monday 15 March and reported the loss to the Information Commissioner's Office (ICO).

After the incident a number of immediate steps were taken:

- Letters were sent to the parents of the children advising them of the data loss; a telephone helpline was set up and manned by Children's Services (CS) including senior staff, to deal with calls from those affected.
- A risk assessment on all the children was carried by the Head of Safeguarding to determine whether any additional support was required.
- All staff were reminded via email of the data protection policies and told where to find them on the council intranet. Those CS staff deemed to be high risk in terms of data protection (DP) attended a mandatory face to face briefing and were shown where the relevant policies can be found.
- A check of all 2130 laptops was begun to confirm that they were encrypted; as a result 600 were later encrypted to bring them up to the corporate standard.
- DVD/CD drives and USB ports on all laptops were disabled.
- Staff were required to bring in all removable storage they had been using. A total of 814 non encrypted media (memory sticks and CDs) were received.
- The member of staff who had the data at the time of the loss was suspended and a disciplinary investigation was begun.
- The Chief Executive commissioned an independent review that was tasked with establishing whether the data loss was an isolated incident or indicative of a wider set of problems. The Terms of Reference are in appendix 1.

The Council had invited the ICO to carry out an audit on the effectiveness of Data Protection governance and internal controls and processes within the Council. The audit was carried out in February and March this year prior to the incident and focused on Human Resources and Children's Services.

Methodology
In order to carry out the review I examined Council procedures and documents including the following policies: Internet and Email Policy, Information and Security Policy, acceptable Usage Policy, Data Protection Policy, Password Policy and Password Selection. I also read relevant internal audit reports: Data Protection Act 1998 February 2009, Working with Partners August 2009 and Data Security and Handling February 2010.

Staff were made available for interview and notes were sent to those interviewed so that they had the opportunity to check for accuracy. I saw a total of 15 people in individual interviews and a further 6 people in a focus group of CS staff.

There has been full and constructive cooperation from the staff I have talked to in Children's Services and Corporate Governance.

I have consulted the ICO document library for examples of good practice. A link is provided in appendix 2. This was helpful as a check that all the relevant areas for improvement were considered. The draft ICO audit report was published as my investigation began; where the areas identified for improvement were similar to mine I have taken account of the recommendations of that audit.

The Local Government Association (LGA) produced guidance for local government in its report 'Local Government Data Handling Guidelines' published in 2008. The Information Commissioner writes in his foreword to the guidelines:

'In investigating any apparent breaches of the Data Protection Act by councils we will look to see whether these guidelines have been implemented effectively and take this into account in assessing whether councils are meeting their obligations.'

I have therefore taken account of those guidelines in formulating my findings and recommendations.

Data Loss Incident

There were two factors that combined directly to give rise to the data loss. Firstly data security did not have the level of priority that it needed and secondly staff and management awareness of data protection was not sufficient to minimise the risk of losing personal data.

There were exceptions to that lack of awareness especially in the Research and Information Management Team and in the Safeguarding Service in Children's Services and in the Performance and Organisational Development Team in Corporate Governance. Checking systems were in place such as the Internal Control List, but they were not sufficiently robust to give the Council assurance that data protection policy and procedures were being followed consistently and safely.

As well as the factors already mentioned, there were general factors that contributed to the incident, in summary:

1. Data security at the time of the incident did not have the priority it needed.
2. Awareness training on DP was not generally available for new starters and there was no programme of refresher training for existing staff
3. There was relatively little compliance testing on adherence to DP policies.
4. Alternatives to putting personal data on to removable storage were available but not sufficiently used.

1. Data security did not have the priority it needed
   - There was no encryption on most memory sticks and CDs used to take data off site
   - The results of the recall of unencrypted removable storage were that 814 items were handed in. While it is not clear that all of those media were used for storing personal data, the number does support the view that protecting electronic data was not a high priority at the time.
   - Staff interviews confirmed that this lack of priority was not unusual in the CS at the time. All staff felt that data security had not had as high a profile as it needed.
   - The Information Security Policy states that removable storage should be 'protected and stored securely' but is not explicit about encryption.

2. Awareness training on DP is not generally available for new starters and there is no programme of refresher training for existing staff.
   - The absence of regular refresher training on DP for all staff handling personal data means that staff across the Council are less likely to adopt consistent good DP practice.
   - Induction is the responsibility of the starter's manager and so depends on those managers' understanding of DP policies. There was not at the time of the incident a general induction programme within CS though one is now planned.
   - The main exception is that Safeguarding staff undertake common core training and this includes direct reference to the provisions of the Data Protection Act.

3. There was relatively little compliance testing on adherence to DP policies.
    - There is an Internal Control Checklist that includes questions about information risk. On its own it was not able to pick up problems in data protection and needs to be supplemented by further checks on compliance.
    - Staff interviewed reported that prior to the incident there was little checking on adherence to data protection policies. Managers were aware that staff were using removable media to store personal data but no checks were made on how secure those media were.
    - It was difficult to find policies on home working which suggests that they were not likely to be effective as a guide to action.
    - Some policies have yet to be updated to reflect the new requirements for data security introduced since the data loss in March. It is also difficult to tell how up to date policies are in general as they do not have start or review dates.

4. Alternatives to removable storage were available but not used.
    - It is believed that the removable storage that was lost was due to be handed over to a colleague. The handover could have been achieved more securely by the use of a shared drive. Shared drives can limit access to files containing personal data to specific users with rights to see that data. Staff reported a lack of use of that facility at the time of the incident.
    - All staff who need to work remotely can do so through the use of VPN or Citrix. In combination with shared drives this allows personal data to be used from different locations by groups of staff with rights to see such data.
    - Staff can also use a 'briefcase' facility on their laptop computer that enables them to synchronise standalone work with the network drive. This is useful when remote access is not possible as is the case with Barnet House used by social care staff to see clients and attend conferences.

Other Findings

Good practice in data protection is likely to be ever more essential to confidence in local government as technology continues to shape the relationship between local councils and citizens.

However, the recent recurrence of data protection problems at HMRC is a timely reminder of how difficult it can be to avoid mistakes with personal data. Recently HMRC reportedly sent information on tax credits to the wrong people and in some cases to neighbours rather than the correct individual.

The findings below arise from interviews with staff and from a desktop review of the DP policies. They address security and awareness issues, and have contributed to the recommendations later in the report.

The findings are set out under the headings adopted by the LGA report referred to earlier:

- People
- Places
- Processes
- Procedures

Some of these findings show areas of good practice as well as opportunities for improvement.

People

1. CS has identified two senior managers to fulfil the roles of Caldicott Guardian and Senior Information Risk Officer (SIRO) for the directorate. An initial meeting of an Information Governance Board has been arranged to discuss working arrangements. This development is welcome as it provides senior management oversight of data protection issues. The plan is for quarterly meetings to ensure that security and handling of personal information within CS comply with policy and procedures.

2. CS runs training courses attended by all social workers and administrators who use ICS and WISDOM and produces training materials that include advice on how to send personal data securely. Those materials are available on the Intranet and are of good quality; they are reported to be well used though specific statistics on usage are not currently available.

3. Some staff want to see a quicker and more consistent response to exception requests for removable storage. In the light of recent experience with the approval process, it may be that some requests for exceptions to the removable storage ban could in future be decided on a class basis.

4. The culture of desktop computers with documents stored on individual hard drives seems to have led to storage on a personal network drive instead of or as well as shared drives. The resulting lack of access to a sole 'version of the truth' can lead to sub-optimal decisions where up to date information is essential. It also creates the conditions for duplication of data and impaired data quality. This is an area where refresher training could help.

5. Corporate Governance had been concerned about potential weaknesses in data protection so commissioned internal audit to investigate the Data Protection Act (February 2009). Unfortunately the ICO audit found that the audit still had 5 out of 6 recommendations outstanding; this was due to other work taking priority at the time.

6. At present CS are not making use of the Information Toolkit developed by the NHS. Version 7 of the toolkit has been written specifically for social care organisations to ensure high standards of practice. Although not mandatory for children's social care, the toolkit has been regularly updated and reflects the latest Cabinet Office requirements to improve the management of information risk.

7. The Council has not yet appointed a corporate SIRO as recommended by the LGA guidelines on data handling in local government. The primary responsibility would be to provide an annual written statement of the security and use of business assets. This responsibility could be attached to an existing senior role.

8. The Council has a system of DP Link Officers (LO) across directorates. The ICO audit found that not all recommendations of internal audit about the LO role had been implemented and that seniority of people filling the role appeared to vary across the Council. I found that the perception of CS staff is that this role is mainly for FOI requests rather than for advice on wider DP issues.

Places

9. Access to the Council offices on the North London Business Park (NLBP) site is well controlled and there is security on site; within the buildings a swipe card is required to enter offices from lifts and stairwell areas.

10. Those children's centres and youth provision that are the direct responsibility of the local authority adhere to corporate policy on data security. There are a few instances in youth provision where Apple Mac computers are used that are not encrypted. There are practical difficulties to be resolved about security as the users of the service use their own memory sticks to copy multimedia work they have done on the Apple Macs.

11. Security of personal information on school premises is the responsibility of the school as data controller and that includes some children's centres. Schools have been advised of the need to encrypt laptops and removable storage. Guidance notes on data protection have been produced and are nearly ready to circulate. A briefing meeting on data protection has recently been held with secondary heads and a similar briefing has been arranged for primary heads.

12. Where services hold photographs, procedures are in place for permission to publish them. However, it is unclear how secure storage of photographs is in some youth service premises although the staff focus group produced examples of good practice.

Processes

13. Secure electronic transfer of files is now well established between schools and the Council's Research and Management Information Team. This is a process that appears to work well although there are technical limits on file size that the Council may have to address in the future.

14. CS has introduced secure file transfer arrangements for annual returns by Early Years providers including childminders which contain sensitive personal data. This year for the first time CS insisted for data security reasons that all annual returns were made by this method.

15. CS Research and Information Management Team (REMIT) challenge examples of poor practice in transferring personal data. For example if such data is sent by unsecure email they will discuss alternative secure methods of dealing with the information.

16. The use of secure email is starting to roll out across the Council. When implemented this will make it easier to transfer securely small amounts of personal information where it is not appropriate to send by file transfer. At present the implementation is voluntary so progress depends on the willingness of services and sections to volunteer.

17. Paper files are used extensively in some areas of CS, in particular the SEN Team. The team stores paper on site as well as at the archive in Hendon and reports some problems with the maintenance of lockable storage. Data security has a high priority but the implementation of a full electronic record management system would make the service more efficient and would improve data security. The Service relies on reports from many professionals outside of the Council so to move to a fully electronic mode of operation would require considerable negotiation.

18. The position on records in children's social care is that WISDOM is the main (electronic) record for children. However the service keeps some documents such as passports or letters from parents. Older paper files are in the process of being scanned into electronic form and that should be finished later this year.

Procedures

19. All staff that take laptops off site are required to complete an authorisation form that is countersigned by the service director and lodged with HR. The individual retains a copy that has to be produced on demand. As at 19 May 742 forms had been lodged with HR.

20. Staff who can make a business case for using removable storage have to submit a written request for approval by the service director. Within CS these requests are subject to a challenge process and many have been diverted through the use of alternative processes. As at 19 May 50 requests had been received.

21. The Information Security Policy states in section 15 Staff Responsibilities that, *'All information (flash drives (memory sticks), disks, CD's and paper) must be protected and stored securely at all times and whilst in transit or at home.'* The policy needs to reflect the current standard to use removable storage only where authorised by the service director and then only encrypted storage.

22. The Internet and Email Policy lists a series of Don'ts for email but says nothing about attachments containing personal data. This is an area of potential vulnerability in data quality as well as data security as it creates the possibility of multiple versions of personal information.

23. The Retention of Documentation and Destruction of Files Policy states in section 1.5, *'Staff are not allowed to remove case files or other documents from their or any other office, whether this is to work at home or for meetings, out of their normal place of work. Exceptions may be agreed on a case-by-case basis by the line manager, which should be noted, particularly in relation to timescales'*. Management responsibility is outlined in Section 1.7, *'Managers should have systems in place to record any removal of documentation from the workplace and their return, with appropriate signatures and dates'.* However it is unclear how consistently these requirements are being met.

24. The Home Working Policy contains an FAQ section on the Housing Benefit Pilot where question 40 asks about to DP. The answer states '*It is the employee's responsibility to ensure safety and security of the documentation that is in their custody. During 'core' work hours it is expected that the employee will focus on job and not distracted by visitors to the household. A lockable pedestal is provided if required.'* It would be helpful to produce guidance that deals with occasional remote working including examples of reasonable steps to secure personal data.

25. The Acceptable Usage Policy refers to a Mobile Working Policy that no longer exists. I understand that the issues that were in that policy are now covered in other procedures.

Recommendations

The controls introduced through encryption of laptops and severely restricting the use of removable media should go a long way towards avoiding a similar incident in future. However further measures are needed to ensure that present and future staff and managers are aware of and take action to reduce the risk of losing personal data.

Prior to the data loss the Council relied primarily on individual staff and managers taking responsibility for understanding and following data protection policies. I believe that the Council should now consider how best to rebalance individual responsibility with systematic oversight and compliance testing. Many of my recommendations suggest a way forward in that rebalancing.

The main priority areas in the recommendations are to raise staff and management awareness of data protection, to improve management control systems and to refine HR processes to support data protection. Appendix 3 gives a summary of each recommendation with a suggested timeframe for implementation.

Individually many of these recommendations are small in scale but the cumulative impact should be to shift awareness of information responsibilities and risks in a direction which would make personal data safer. Small scale recommendations are also more likely to be sustainable in a time of major change as Barnet implements its Future Shape programme.

People

1. Develop the roles of Senior Information Risk Officer (SIRO) and Caldicott Guardian to ensure the development of appropriate governance and confidentiality processes within CS. This will help the service to better manage information risks. There are already some useful online resources for these roles and details can be found in appendix 2.

2. Develop similar SIRO and Caldicott arrangements within Adult Social Care if not already in place. Adult Social care is the other major user of personal data about vulnerable people and would benefit from a similar mechanism to the one being developed for CS.

3. Appoint a SIRO for the Council. This is an LGA recommendation. It has a specific role in terms of information risk that could be incorporated into an existing senior manager role. The role is likely to be best placed within the Corporate Governance Directorate as that directorate already has the oversight of corporate risk management.

4. Clarify the Information Asset Owner for the information systems in each directorate. The role will include overall responsibility for data quality and data handling though specific actions may be delegated. This is clear for Children's Services and Corporate Governance. It is included to ensure that similar clarity exists in other directorates.

5. Implement DP awareness training for all new starters and annual refresher training for staff that handle personal data. A logical starting point for refresher training would be those staff with permission to take laptops off site. This will support a culture of DP awareness across the Council.

6. Ensure that job descriptions for posts that handle personal data explicitly address DP issues. This will help build awareness of the importance attached to DP in Barnet from the pre-employment stage.

7. Update HR policies to ensure that they emphasise the importance of good data protection practice and the seriousness of failing to comply. Again this will contribute to awareness and so promote a stronger data protection culture.

8. Implement and publicise mechanisms for bringing concerns about information risk to the attention of senior managers. This is also an ICO audit recommendation. There is a difficult balance to strike here between informality and formal procedure. Much will depend on the effectiveness of awareness training and the way that staff and managers at all levels are able to promote a culture of openness about data problems or near misses.

9. Take the opportunity provided by the election of new councillors to provide a member briefing on DP issues. Councillors already receive a briefing on their role as data controllers and this could extend to inform them of the steps being taken with council staff and managers to raise awareness on data protection.

Places

10. Review the storage for personal information on Council premises away from the NLBP to ensure that it is secure. The main impact is likely to be on youth service provision directly managed by the Council which is potentially less secure than the main site.

11. Ensure that photographs are securely stored and have the required authorisation for use. Written authorisation for the use of photos is already obtained but needs to be updated every 3 years. Storage arrangements should be checked to ensure they are secure; that should include the storage of written permission as well as of the photos themselves.

12. Ensure that lockable storage of personal paper records kept on site can always be locked. This seems to be an issue for the SEN Service which in the longer term could be significantly improved by the use of electronic records. However that will not be easy to achieve as the service relies on reports from a range of professionals outside of the Council all of whom would have to able to comply with common data security standards across agencies.

13. Ensure that personal data on the Apple Mac computers held by youth service is securely stored. Youth service clients currently use removable storage on those machines as part of the work the service does. I understand that alternative solutions to data security are being explored.

14. Maintain the current tight controls on removable storage and review the approval process to ensure that exceptions are considered speedily. The controls will limit the risk of a recurrence of the March incident. It may be possible to speed up decisions on certain types of request in the light of experience.

Processes

15. Make the use of secure email mandatory for those teams that exchange a high volume of personal data. Making this mandatory would improve security of data transfer. There will still be issues to address about personal data sent to parties not on secure email.

16. Brief staff and managers on the use of shared drives with appropriate access conditions rather than personal network drives to improve data quality. Shared drives reduce the need for duplicate data and so contribute to better data quality.

17. Where teams or sections process a high volume of personal information include a DP target in the manager's annual appraisal. This will raise awareness and ensure that improvements in data protection maintain a high profile.

18. Review the role of DP link Officers in the light of the recommendations of this report and the ICO audit report. The role seems to be more effective in dealing with SAR and FOI rather than general data protection queries. This should help to improve clarity of role and seniority required and hence effectiveness.

19. Review and consolidate the reporting arrangements for FOI, Subject Access Requests (SAR) and DP in the light of the recommendations of this report and the ICO audit report. This may have a cost implication if specialist software has to be purchased, but should improve the Council's timeliness in responding to requests.

20. Use the Information Governance Toolkit in Children's Services and in Adult Social Care. This is also a recommendation of the ICO audit. It will help the service to assess the state of progress on implementing DP policies through an annual review. It is a quick win as the tool is readily available.

21. Move to an ERDMS solution for those areas of CS using paper based systems as soon as resources allow. This should improve the operational efficiency of the SEN Service in particular.

22. Conduct Privacy Impact Assessments (PIA) on new systems. The PIA process is recommended by the ICO and is

    "…..a process whereby a project's potential privacy issues and risks are identified and examined from the perspectives of all stakeholders and a search is undertaken for ways to avoid or minimise privacy concerns…."

    For more information see link to the PIA handbook in appendix 2. PIA is now used by central government to help manage information risks arising from proposed new systems. By considering privacy issues at the planning stage it can avoid more costly changes later if privacy problems are identified after implementation.

Procedures

23. Develop an Information Strategy for the Council that gives a clear direction of travel. Such a strategy could also be the basis of an information charter for Barnet. A sample charter can be found in the cabinet office guidelines – see appendix 2.

24. While paper records are in use, ensure that management systems are in place to monitor adherence to the policy on Retention of Documentation and Destruction of Files. The procedure requires managers to have a system to track papers being removed from the office. This could be checked through the normal management supervision process.

25. Develop compliance testing on DP policies by directorates and report annually through the corporate SIRO to the Corporate Director's Group. The ICC checklist process could be fine tuned to deliver this with questions revised to take account of the changes in process due to these recommendations. The internal audit team could also be used to test compliance on a sample basis.

26. Update existing data protection policies and address data security issues arising from remote working; include an owner, version control, a date of issue and review date as recommended by the ICO audit. This will ensure to ensure that they are up to date with current practice.

Hugh Fenwick
SOLACE Consultant

June 2010

Appendix 1 Terms of Reference for Investigation

Background

On Monday 15 March 2010 the Council discovered that as a result of a burglary at a member of staff's home address a large volume of unencrypted pupil data had been stolen.

The Council subsequently took a set of remedial actions and as part of its commitment to affected parents indicated it would establish an independent review of the incident.

Terms of Reference

The Terms of the review are:

- To review the data handling storage and security arrangements within Children's Service, including;
    - Whether existing policies are appropriate and meet appropriate external standards
    - Whether management processes are sufficient and appropriate to ensure policies are effectively followed
    - Whether other processes, including technical processes, are sufficient and appropriate.
    - Whether there is in place an effective culture recognising the importance of data protection
    - Whether existing systems (such as address data tools) effectively support data protection policies
- Establish if the data loss is an isolated incident or indicative of part of a wider set of problems within the Children's service and across the Council as a whole.

Make recommendations to inform:

- Improvements in data protection including handling and storage within the Children's Service and corporately;
- Future staff training and development needs;
- Future arrangements at service and corporate level for monitoring data security;
- Addressing other barriers to effective data protection that the review may identify.

Conduct of the review

To manage the review process the Council will appoint an independent person with relevant experience to steer the review.

The appointed person will have the following resources at their disposal:

- Access to all relevant personnel;
- Access to relevant systems information;
- Funding to access any technical resource the person deems necessary;
- All policy documentation.

Timescale

It is important that this review is completed in a timely fashion given the service and corporate risks such incidents present. Final timings will be by negotiation with the CE and Director of Corporate Governance but a timescale of approximately six weeks is expected.

Nick Walkley
Chief Executive

April 2010

Appendix 2 Useful Resources

Data Handling Procedures in Government Final Report
(Contains a draft Information Charter)
Cabinet Office 2008
http://webarchive.nationalarchives.gov.uk/20100416132449/http://www.cabinetoffice.gov.uk/media/65948/dhr080625.pdf

ICO Document Library on Data Protection
Information Commissioner's Office
http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx

Information Governance Assessment Version 7
(IG Toolkit)
NHS Connecting for Health 2009
https://www.igt.connectingforhealth.nhs.uk/Getting%20Started%20-%20SC%20organisations_2009.pdf

Local Government Data Handling Guidelines
Local Government Association 2008
http://www.lga.gov.uk/lga/aio/1587602

Privacy Impact Assessment Handbook
Information Commissioner's Office
http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

Resources for Caldicott Guardians
NHS Connecting for Health
http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott/caldresources

The Caldicott Guardian Manual
Department of Health 2010
http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/@ps/documents/digitalasset/dh_114506.pdf

Appendix 3 Suggested implementation priority for recommendations

Recommendation	Priority next 6 Months	Priority next 12 months
1. Develop the roles of SIRO and Caldicott Guardian to ensure the development of appropriate governance and confidentiality processes within CS.	**X**	
2. Develop similar SIRO and Caldicott arrangements within Adult Social Care if not already in place.	**X**	
3. Appoint a SIRO for the Council. This is a LGA recommendation. It has a specific role in terms of information risk that could be incorporated into an existing senior manager role.	**X**	
4. Clarify the Information Asset Owner for the information systems in each directorate. The role will include overall responsibility for data quality and data handling though specific actions may be delegated.		**X**
5. Implement DP awareness training for all new starters and annual refresher training for staff that handle personal data.	**X**	
6. Ensure that job descriptions for posts that handle personal data explicitly address DP issues.		**X**
7. Update HR policies to ensure that they emphasise the importance of good data protection practice and the seriousness of failing to comply.		**X**
8. Implement and publicise mechanisms for bringing concerns about information risk to the attention of senior managers. This is also an ICO audit recommendation.	**X**	
9. Take the opportunity provided by the election of new councillors to provide a member briefing on DP issues.	**X**	
10. Review the storage for personal information on Council premises away from the NLBP to ensure that it is secure.	**X**	
11. Ensure that photographs are securely stored and have the required authorisation for use.	**X**	
12. Ensure that lockable storage of personal paper records kept on site can always be locked.		**X**
13. Ensure that personal data on the Apple Mac computers held by youth service is securely stored.	**X**	
14. Maintain the current tight controls on removable storage and review the approval process to ensure that exceptions are considered speedily.		**X**
15. Make the use of secure email mandatory for those teams that exchange a high volume of personal data.		**X**
16. Brief staff and managers on the use of shared drives with appropriate access conditions to improve data quality.		**X**

Recommendation	Priority next 6 Months	Priority next 12 months
17. Where teams or sections process a high volume of personal information include a DP target in the manager's annual appraisal.		**X**
18. Review the role of DP link Officers in the light of the recommendations of this report and the ICO audit report.	**X**	
19. Review and consolidate the reporting arrangements for FOI, SAR and DP in the light of the recommendations of this report and the ICO audit report.	**X**	
20. Use the Information Governance Toolkit in Children's Services and in Adult Social Care. This is also a recommendation of the ICO audit.		**X**
21. Move to an ERDMS solution for those areas of the Children's Service using paper based systems as soon as resources allow.		**X**
22. Conduct Privacy Impact Assessments (PIA) on new systems.		**X**
23. Develop an Information Strategy for the Council that gives a clear direction of travel.		**X**
24. While paper records are in use, ensure that management systems are in place to monitor adherence to the policy on Retention of Documentation and Destruction of Files.		**X**
25. Develop compliance testing on DP policies by directorates and report annually through the corporate SIRO to the Corporate Director's Group.	**X**	
26. Update existing data protection policies and address data security issues arising from remote working; include an owner, version control, a date of issue and review date as recommended by the ICO audit.		**X**