



CIVILSERVICE

Information Management Assessment

Department for Children Schools and Families

July 2009



The National Archives

<u>PART ONE: EXECUTIVE SUMMARY</u>	<u>2</u>
<u>PART TWO: INTRODUCTION</u>	<u>8</u>
<u>PART THREE: ACTIVITIES CARRIED OUT BY THE ASSESSMENT TEAM</u>	<u>11</u>
<u>PART FOUR: HIGHLIGHTS AND AREAS FOR IMPROVEMENT</u>	<u>15</u>
<u>APPENDIX ONE: SUMMARY OF RECOMMENDED ACTIONS</u>	<u>41</u>
<u>APPENDIX TWO: GLOSSARY</u>	<u>44</u>

PART ONE: EXECUTIVE SUMMARY

1. The Department for Children, Schools and Families (DCSF) is a forward-thinking department that values innovation and creativity. Information is key to achieving this agenda, but our assessment found that information is not truly valued as an asset. DCSF's emphasis appears to be on information protection, not exploitation. Our assessment found that information owners are not always taking full responsibility for the information they are responsible for, except in the challenge of embedding the security agenda across the organisation.
2. If DCSF does not truly value its information, there are real risks to the organisation: it may be unable to meet its objectives under the Children's plan; the effectiveness of evidence-based business decisions will be compromised; statutory obligations will not be met, and valuable information will not be kept.
3. DCSF has a core of committed and professional staff with responsibility for Knowledge and Information Management (KIM). This team reports through to several boards which have oversight of distinct areas of information management. DCSF should have a strategic Knowledge and Information Management Board with responsibility for championing information management across the organisation.
4. DCSF is currently reviewing its approach to information management. It is addressing many of the issues identified above through the Information Work Place (IWP) programme. This programme has the potential to set a new standard across government. It is a major piece of work which incorporates a new departmental Intranet, Team Sites, MySites and Records Centre. It is through this system that the department will be able to capture and manage its future electronic information. There are many promising aspects to the plans, including the automation of metadata to ease the burden on end-users, and it is hoped that this more user-friendly environment will encourage and enable staff to derive the most value from their information, sharing work across teams. However, the technical solution alone will not suffice and strong governance and leadership, including robust policies, guidance and training, will be needed to ensure the IWP programme's success. Visible measures and outcomes in this area

would also add real benefit in raising the priority of information management.






5. Although information assurance is defined as one of the top three risks to the department, information management is not defined as a risk on the corporate risk register. It is a sub risk. Information risk and not information assurance should be the governing principle, with good information management practice embedded in the business. Whilst DCSF has made a good start in tackling the information assurance agenda, there are gaps in the department's assessment of, and management of, wider information risk. For example, whilst DCSF may be confident that key information is protected, it needs to be confident that it is managing the risk of not retaining the evidence of key decisions or of failing to share critical information across the organisation, or with key partners.
6. The assessment found evidence of management of information security, but not of wider information risk. There was little evidence that the risks of not sharing or exploiting information, or of failure to capture key information, were understood or managed. Good information management will lead to better policy, greater efficiency and better accountability.
7. DCSF have not clearly defined which of its information assets have business value. Many staff currently either keep everything or use their common sense to determine what should be kept. This strategy is not sustainable in the long term. The risk of losing, or providing inadequate protection, or not being able to find core business information or records of key decisions is both significant and substantial. There is also a real risk of DCSF being exposed to possible legal challenge and the reputational risk which this engenders.
8. DCSF is recognised internally as having a culture that is averse to mandating, or being overly prescriptive, in how internal business is conducted. This has an impact on a number of areas, including training and on the IT systems used for storing information. The majority of training in 2009, other than information security, is not mandatory; therefore, many staff either did not attend or were unaware

of the training opportunities. Furthermore, there is a policy of no classroom training. Online training requires people to prioritise training in their busy schedules. There is a key risk that staff will not prioritise information management training and therefore be unable or unaware of how to meet their responsibilities.






9. People trained to do particular roles are not always replaced when they leave, leaving gaps in knowledge and training. This lack of knowledge transfer leads to a loss of valuable knowledge and experience.
10. The widespread sharing of knowledge and information is not yet at a mature level. There is no system to help staff share the information they hold. At present, it depends on previous contacts rather than a need to know. This could lead to poor decisions made without access to the full facts and also duplication and a lack of efficiency as information is not easy to find or its actual existence is not known.
11. It is The National Archives assessment that if DCSF implement the recommendations contained in this IMA report that they will be well placed to achieve this transformation.

12. Risk Matrix

Governance and Leadership

Strategic management		
Business objectives		
Management controls		
Resourcing		
Risk management		


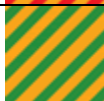

Records Management

Creation		
Storage		
Appraisal, disposal and transfer		
Sustainability of digital records		
Management		

Access

FOI/Data Protection		
Re-Use		
Security		






Compliance

Staff responsibilities and delegations		
Policies and guidance		
Training		

Change management		
-------------------	---	--

Culture

Commitment		
Staff understanding		
Knowledge Management		

Key to Colour Coding	
	Best Practice
	Good
	Satisfactory
	Development Needed
	Priority Attention Area

PART TWO: INTRODUCTION

Information Management Assessments

13. The Information Management Assessment (IMA) Programme is the best practice model for government departments wishing to demonstrate a high level of commitment to managing their information. The assessment process ensures that government departments meet the required standards for effective collection, storage, access, use and disposal of information. The IMA programme:
 - enables the Head of Profession for Knowledge and Information Management (KIM) to assess the effectiveness of the function in departments;
 - sets out the capability of departments to meet their KIM challenges and obligations;
 - assures the Accounting Officer that departments are equipped to deliver their information management responsibilities; and
 - helps Accounting Officers plan for future information management developments.
14. The National Archives leads information management across government. The IMA Programme is a key element of that function. The programme's goal is to deliver measurable improvements in information management across government by providing robust, independent validation of the standards and integrity of the information management processes and capability within departments.
15. The IMA Programme is aimed at core government departments. To be admitted to the Information Management Assessment programme, an organisation will:
 - make a public commitment to the IMA programme; and
 - see the commitment successfully independently verified.
16. Once a Permanent Secretary has declared the commitment, the underlying administrative and decision-making processes of the

organisation are examined to verify that they support the IMA commitment.

17. This report sets out the findings, conclusions and recommendations of The National Archives' IMA Assessment of the Department for Children, Schools and Families (DCSF).

The Business of the Department for Children, Schools and Families (DCSF)

18. The Department for Children, Schools and Families (DCSF) was created on 28 June 2007, following the demerger of the Department for Education and Skills (DfES).
19. The department aims to make the UK the best place in the world for children and young people to grow up.
20. DCSF is responsible for all issues affecting people up to the age of 19 including child protection and education. It is led by the Secretary of State for Children, Schools and Families, Ed Balls and the Permanent Secretary, David Bell.
21. The Department currently employs an estimated 2,620 staff. Estimated Government expenditure on education in 2007-08 was £77.7 billion.
22. DCSF aims to deliver a step change in education provision and integrated support to all children and their families and to support Government's long-term ambitions to eradicate child poverty by 2020.
23. Delivery of these priorities will be driven by Departmental Strategic Objectives to:
 - secure the well-being and health of children and young people;
 - safeguard the young and vulnerable;
 - ensure an excellent education for all our children and young people;
 - keep them on the path to success; and

- provide more places for children to play safely.
24. DCSF leads delivery of the cross-governmental Public Service Agreements (PSAs) to improve the health and well-being of children and young people, improve children and young people's safety, narrow the gap in educational achievement between children from low income and disadvantaged backgrounds and their peers, raise the educational achievement of all children and young people and increase the number of children and young people on the path to success.

Information Management at the Department for Children, Schools and Families

25. The records management service at the Department for Children Schools and families is managed by the Information and Records Management Team who are based in Runcorn, Cheshire. The Team's responsibilities include; producing information and records management policies and procedures, managing the storage of paper records, review, selection and transfer of records to The National Archives and oversight of the Electronic Documents and Records Management system (Meridio).

PART THREE: ACTIVITIES CARRIED OUT BY THE ASSESSMENT TEAM

Methodology

26. The underlying purpose of the assessment is to establish whether the key elements of the department's commitment to the IMA programme and their own Information Management (IM) priorities are achieved. A range of standard processes, systems and documentation were examined to determine if this was the case. This approach was based on a matrix model, as shown below, which takes essential business outcomes, and shows how work in each of the areas of activity demonstrates compliance.

27. The department is divided into a number of key business areas, relating to how the organisation is managed, governed, its vision and key business objectives, especially pertaining to information management. Key services across the range of DCSF business groups were assessed. The key business areas were considered according to a risk assessment carried out prior to the on-site visit. This was based on:
 - the findings of the pre-assessment questionnaire;
 - previously identified strategic risks; and
 - information management or skills issues raised by DCSF themselves.

28. The key business areas, and the areas of assessment focus, fall under the following headings:

<i>Business Area</i>	<i>Assessment Focus</i>
Governance	Strategic direction, business objectives and performance indicators Management controls Capability Risk management Data Handling Processes
Records Management	Creation, storage, appraisal, disposal, transfer, security, management, sustainability of digital records
Access	Access to and re-use of government information Websites and equivalents
Compliance	Staff responsibilities and delegations Policies and guidance Intranet Skills/Training Effects of changes in government policy or legislation
Culture	The commitment to effective information management Staff understanding of information management risks Application of Policies and Guidance Knowledge Management

Activities Undertaken

29. The Assessment Team:

- examined key policy and practice documentation relating to training, skills and processes;
- interviewed staff members from across the organisation;
- tested the processes used; and
- reviewed the website and intranet.

These activities are described in more detail below.

Documentation Review

30. The department provided documentation in support of their information management objectives and the IMA commitment, which was reviewed prior to the on-site assessment.

People and Practices

31. The Assessment Team interviewed a range of staff, at all levels, who are involved in policymaking, interpretation and the practice of managing information. These interviews were used to determine how people in the organisation work and the impact of information management on them.

Process Testing

32. A sample review of the day-to-day business processes was used to identify possible procedural gaps. This included electronic records management systems, retention schedules and general guidance and working instructions.

Intranet review

33. A review of the department's Intranet was carried out to assess ease of use, utility of the information contained on it and to determine how up to date it was.

Website Review

34. A review of the organisation's website was conducted to establish the transparency of information relating to Freedom of Information, Data Protection, contact details and complaints procedures.

Risk Assessment

35. The department's risk framework and associated information statements and policies were assessed to ensure information, knowledge and records management compliance.

Data Handling

36. The department's data handling was reviewed in a limited context or "light touch" within the IMA process and only where there is an immediate effect on the process being reviewed.

The Assessment Team

37. Each IMA is carried out by the Standards Team within The National Archives, with a team of external reviewers assembled to meet the

requirements identified in the pre-assessment planning. The team comprised:

- Standards and Assessment Manager, Doreen Charlton
- Head of Standards, Marcia Jackson
- Standards Adviser, Dan Husbands
- Information Management Consultant, Siân Jones
- Standards Adviser, Matthew Pearce
- Research Adviser, Matt Brown

The DCSF Assessment took place in July 2009, over a period of 5 days. There were also a series of follow up meetings, aimed at identifying potential solutions, in September and October 2009.

Assistance provided by the Department for Children, Schools and Families

38. The Assessment Team is grateful for the co-operation and assistance of all staff within the Department for Children Schools and Families, and especially the Information and Records Management Team for their help in facilitating the assessment.

PART FOUR: HIGHLIGHTS AND AREAS FOR IMPROVEMENT

Governance and Leadership

“I will provide effective leadership on Knowledge and Information Management capability across my Department.”

39. The Department for Children, Schools and Families (DCSF) is a forward-thinking, creative organisation. DCSF has taken up the challenge of embedding the security agenda across the organisation. The Permanent Secretary has established and communicated the priority of information security in DCSF. The visibility and the commitment at a senior level to the security agenda is to be commended.
40. The clarity of the message from senior management was evidenced. The department used a number of ways to promote good information assurance practices, such as alerts on the Intranet which reinforced the message. This has resulted in staff understanding the need for security and why it is a high priority. The department's external accreditation to ISO 27001 compliant Information Security Management Systems demonstrates the level of engagement with information security.
41. However, information security is only a subset of information risk. Whilst this is a good foundation, we saw gaps in the department's assessment of, and management of, wider information risk. For example, whilst DCSF may be confident that key information is protected, is it confident that it is managing the risk of not retaining the evidence of key decisions? Or of failing to share critical information across the organisation, or with key partners? The assessment only found evidence of management of information security, and not of wider information risk, and little evidence that the risks of not sharing or exploiting information, or of failure to capture key information being understood, or managed. The Government's Managing Information Risk¹ report provides guidance on identifying and managing

¹ [Managing Information Risk](#)

information risks within the public sector. This report was published as guidance for boards to sit alongside the Hannigan review of Information Assurance². Once the risks have been identified, this should guide the focus of DCSF's information management activity, which at the moment appears fragmented and disconnected from strategic decision making.

42. DCSF needs to raise the profile of Knowledge and Information Management (KIM). DCSF currently has several boards which oversee distinct areas of information management. It does not have a strategic KIM lead at Board level. The senior-level representative, either a Senior Information Risk Owner (SIRO) or policy area lead, must have responsibility for championing information management across the organisation. Without such a defined role there is a risk that information management is perceived as low priority and a risk that the information management implications connected to policy changes in ICT, security and risk management are not considered in a timely or coordinated manner.

Recommendation 1: In line with the Hannigan Review guidance, DCSF should ensure that they have board representation covering all aspects of information risk, and not just information security

Recommendation 2: The Board should follow the guidance set out in the Information Matters report and consider information risk alongside, and as a contributory part of, other key risks, and give it priority accordingly

43. The department is investing heavily in ICT to support more efficient, streamlined and collaborative working practices. Examples of recent developments include shared Services Implementation and the piloting of the innovative Information Work Place (IWP) project. It is important that these developments are not run solely as ICT projects, but as KIM projects. Information management is a core success criteria for whether IT projects succeed or fail.

² [Hannigan report](#)

44. There is real risk that without a co-ordinated approach to information management, the department may repeat some of the mistakes made during the implementation of its current document management system (Meridio). Although it was introduced nearly five years ago, the Assessment Team found that its usage has been both inconsistent, and in some cases, nonexistent. There are a number of forums/boards where aspects of knowledge and information management are discussed and actioned across DCSF. However, there is little evidence of coordination of activity and policies through these groups. There is a risk that with the multiplicity of avenues to discuss KIM, the approach will be disjointed and uncoordinated. Further consequences could be wasted money and wasted effort.

Recommendation 3: DCSF should consider the formation of an Information Management Board to oversee all aspects of knowledge and information management

45. With the creation of the KIM Board, DCSF must ensure that it sets out clearly for staff how systems are used, who is required to use them and what information is to be kept. This should be underpinned with the support of relevant policies, guidance and protocols. The consequences of not doing this are duplication of effort, lack of corporate memory, poorly evidenced decisions and a lack of consistency and focus.

Recommendation 4: DCSF, in line with the KIM reporting structure, should develop and communicate clear responsibilities for all staff

46. During the implementation of its previous EDRMS, DCSF created the role of Information Manager. This role was pivotal in cascading training to users, identifying effective working and managing the corporate file plan. For many reasons, including not replacing Information Managers, technical problems with Meridio, and not mandating the use of the system, the impact of the Information Managers has been eroded or diminished over time and the forums that were instigated to support the role have ceased.
47. DCSF has informed the Assessment Team that with the piloting and

roll out of the new intranet (“Our Intranet”) and Information Workplace (IWP) programme, DCSF will introduce the role of IWP champions. DCSF must ensure that the champion roles are clearly defined and fully supported, with clear succession planning, through training and coherent practices. There is a risk if this is not considered, the role of IWP champion will be an ineffective waste of investment instead of a key information management link and catalyst for change.

Recommendation 5: DCSF to ensure that the IWP champion roles are clearly defined and fully supported

Risk Management

48. DCSF has a corporate risk register that is the responsibility of the Chief Information Officer’s Group (CIOG). Information assurance is defined as one of the top three risks to the department. Information management is not defined as a risk on the corporate risk register, it is a sub risk. Information risk needs to be seen in the widest sense, as stated in the Hannigan report.
49. There are many information risks that are clear to DCSF that are not being managed. Examples of potential risks are set out in ‘Managing Information Risk’. These include:
 - Lack of comprehensive oversight and control (so anything can go wrong)
 - Critical information is wrongly destroyed, not kept or can’t be found when needed, leading to reputational damage or large costs
 - Inaccurate information (which causes the wrong decision to be made or the wrong action to be taken)
 - Failure to utilise the value of the information asset (leading to a waste of public money)
50. Once risks are defined they should be assessed, appropriately allocated to risk owners and understood by the board in line with the Hannigan Review and ‘Managing Information Risk’.

Recommendation 6: DCSF to define, communicate and mitigate Information Management risk within its corporate and business reporting systems

51. DCSF uses a number of data and information sets that contain personally sensitive information. It has an Information Asset Register (IAR) where all the major information assets are defined. The Assessment Team interviewed a number of information asset owners who were clear on what their responsibilities are as asset owners. This is to be commended.

Records Management

“I will ensure that our information is appropriately captured, described, managed and preserved and that the risks are controlled.”

What to Keep

52. DCSF has for a number of years had an Electronic Document and Records Management (EDRM) system, Meridio. Although this system is available across the entire department, its use has been inconsistent. A number of reasons were cited as to why the EDRMS has not been fully utilised. A primary factor was that users confronted technical problems when initially using the system. Once these were resolved, DCSF did not further require its staff to use the system, therefore compounding the problems that existed.
53. Another contributing factor is that many staff are unclear on what information should be kept. The risk of losing, or providing inadequate protection or not being able to find core business information is both significant and substantial.
54. The majority of staff interviewed indicated that they used common sense when deciding what information was critical to the business. Common sense alone is not a strategy that is sustainable in the long term. It puts the emphasis on the individual to define what is of business value; this is a high risk strategy that DCSF must remedy.
55. The Information Workplace Programme (IWP) is in the pilot stage. This project will identify what business critical information should be kept by DCSF. The National Archives has been involved in early discussions regarding both this project and The National Archives' 'What to Keep' project. This latter project is supporting government departments in strategically deciding what information to keep and for how long. DCSF should make a considered and corporately agreed decision on what information has business value, as without this there is a risk that critical information may not be kept and may be lost, which could have a negative impact on the department's efficiency, reputation and

expose the department to possible legal challenge.

56. The Assessment team have been advised that DCSF have appointed an officer, initially for six months, to address what information has critical business value and to address future legacy information concerns. This demonstrates that DCSF recognises the responsibility it has to ensure there are clear standards on what it defines as information with business value, to equip staff with the tools or material to facilitate keeping core information long term.

Recommendation 7: DCSF should define what information it needs to keep, with the support of The National Archives, and ensure that all staff are aware of this

57. The lack of definition of what should be kept has left many staff to adopt the default position of keeping everything. DCSF is facing a considerable risk that it is creating a store of information that has limited value, or that it is keeping records with potentially sensitive data longer than is necessary. Although retention schedules exist there is little evidence that these are reviewed or enforced. This raft of excess information will hinder effective searches when information is required. Searching is made more difficult by the fact that outside the EDRMS, DCSF estimates that there are 1500 shared drives and 4000 personal drives.³
58. This lack of definition is also reflected in the electronic environment, the primary platform by which information is created in DCSF. The lack of a policy governing the retention, review and disposal of electronic records has had an impact on the efficiency of the organisation and exposes the department to risk. This lack of a policy or guidance relating to the electronic environment puts the department at risk of potentially keeping information that it no longer needs, which is clearly against the requirements contained in the in the data protection legislation and may be subject to Freedom of Information (FOI) disclosure.

³ Information and Records Management Team 2008/9 Review to DCSF Senior Management.

59. The Record Management Policy states that most records are subject to a seven or ten year retention period. In the last five years many documents in Meridio have been created and stored without being assigned a retention or review period. This lack of process has meant that in the majority of cases, documents are retained indefinitely.
60. In one service team this absence has meant that staff are unwilling to make a local decision on whether to dispose of information that contains personally identifiable information. They have therefore continued to retain the information long after its primary purpose as they felt that the decision to dispose of this data was not their responsibility. This is clearly in breach of data protection rules and may open DCSF to legal challenge. It also highlights the continuing potential reputational risks to which DCSF is exposed. The Assessment Team are aware that DCSF are planning to address some of the issues identified above as part of the developing Dataset Strategy.

Recommendation 8: DCSF should revise the records and information management policies to ensure that they include fully the use of digital media

61. The Information and Records Management Team is responsible for producing information and records management guidance for DCSF, all of which is available via the Intranet. Although the guidance is comprehensive, it appears not to have been updated. The size and the resource levels of investment in the team have impacted on the team's ability to be proactive. As a possible consequence of the resource levels, guidance does not fully reflect DCSF's ways of working with reference to electronic documents. There is an established records management policy that covers the retention, review and disposal of registered paper files.
62. DCSF currently has three reviewer roles based in the Information and Records Management Team with responsibility for the review of registered files. The Assessment Team recognise that these are important specialist roles and the department should continue to invest in these roles to enable the department's legacy to be preserved in

The National Archives.

63. There does not appear to be a succession plan in place for the KIM roles within DCSF. Should the incumbents be unable to fulfil their duties in the future this will pose a risk to DCSF's information legacy. For example, there is a risk that the lack of succession plan in the short-term will impact DCSF's ability to address potential statutory changes in accessioning information to The National Archives. The Assessment Team recommends that DCSF review the current resource level to ensure that sustainable resources are available to enable DCSF to fulfil its future obligations.

Recommendation 9: DCSF should review the current resource levels to ensure that it will continue to meet future statutory requirements

64. Aside from Meridio, DCSF also has an electronic correspondence system called Electronic Correspondence Handling Organisation (ECHO), by which the department tracks general correspondence and FOI requests. Documents are scanned into the system but are not subject to a retention and disposal schedule.
65. According to internal DCSF analysis there are also approximately 1500 shared areas containing numerous documents and records. These combined systems contain the majority of the documents created by the department. There is a real risk that if this situation continues, the department will be unable to keep track of the information that it produces.
66. The volume of information with business value continues to grow exponentially and may be lost to the organisation if it is not retained and reviewed correctly. Retaining documents indefinitely, whether on shared areas or ECHO, will impact on the ability of the organisation to retrieve key information when required, as searches will need to be conducted across several systems that hold an increasing amount of information. There is a risk that relevant information will become irretrievable if this situation persists. In addition, there are significant costs in holding too much information in terms of storage, and wasted time for staff and FOI reviewers trying to identify what the important

information is amongst large volumes other less important content. This is neither a sustainable nor an effective way to manage information. The information that the department creates and generates is fundamental to its business.

67. The Assessment Team are aware that DCSF is implementing the IWP project to address some of the issues identified, and that this will be piloted from October 2009.

Sustainability of Digital Records

68. Meridio was introduced in DCSF in 2004. At the time it was intended to be used as the primary method by which the department would store and manage its electronic records. The department has recognised that there are a number of issues which have inhibited the effective use of the Meridio system. It is estimated within DCSF that only forty percent of the department is using the system to manage their documents and records.
69. The Assessment Team was informed that DCSF decided not to mandate the use of Meridio when it was introduced. In addition, the department did not ensure that the guidelines for use were disseminated or that usage of Meridio was monitored and reported corporately. Aligned to this there was a need to ensure that all the support mechanisms were ongoing, such as training, updated guidance and support including the Information Managers networks. This should have included reporting when issues relating to the technical side of Meridio were resolved.
70. The Assessment Team found that in several teams and services, Meridio was not used or had been abandoned after a short period. This was made all the more problematic by the fact that staff continued to have access to alternatives, for example shared file areas, personal drives and hard drives on PCs and laptops.
71. Having alternative areas in which to store information undermines the integrity of any corporate system that is introduced. DCSF need to ensure that it mitigates the risk of non-compliance by not allowing staff

to “opt out” of using corporate systems, except in exceptional circumstances. The risk of them doing so is, of course, a risk to DCSF, and not to the individual.

72. The Information and Records Management Team also provides support for the use of Meridio via a “helpdesk” facility. Through this facility the team promotes good records management disciplines across the department. However, as only forty percent of the organisation currently uses Meridio, their impact is limited.
73. DCSF is currently looking at alternative ways to manage its electronic records and documents. The result of this review is IWP. During IWP’s implementation, DCSF needs to address the legacy issues surrounding the storage of the information already created in Meridio. A migration policy is essential. This will allow for records and documents with business value to be reviewed, migrated and stored so that they can be held for future reference.
74. DCSF is assessing an appropriate method to facilitate the migration of existing records once IWP is embedded in the department. How IWP is used to facilitate a clear migration policy will have a long term impact on DCSF. Without a clear migration policy, there is a risk that information created within the last few years will be lost. This loss of information to the department will impact on its ability to meet its statutory obligations, such as FOI and data protection. It will also impact on how DCSF will meet its obligations in the Children’s Plan, and therefore has the potential to put its reputation at risk.

Recommendation 10: DCSF should develop a migration policy to manage legacy information

Email

75. The DCSF Records Management Policy encourages staff to treat emails as records. Despite this, the Assessment Team found that the recognition or understanding that emails constitute a record was inconsistent. Although some staff were aware of the importance of keeping emails, they were often over-cautious, for instance duplicating

emails by saving them in the shared area or the EDRMS and also printing off copies and placing them in the registered files.

76. DCSF does not presently have a limit on the size of email inboxes. Therefore, staff have access to unlimited storage for their private emails. Although there may be sound business reasons for this decision, it makes it imperative that staff are able to distinguish what emails have business value and which do not, with obsolete information destroyed appropriately. There is a real risk with the potential size of personal email stores that information with business value is lost to the department. One individual interviewed confessed to keeping every single email that they had received in the last ten years. In addition, another individual confessed to having over 6000 emails in their personal area. These emails are only accessible by the owner. DCSF staff are also able to convert emails to .pst format and create their own personal stores.
77. The Assessment Team were advised that when the FOI Team has concerns that all the information required for a request has not been found, relevant staff were then asked to check their personal emails. This demonstrates that DCSF recognises the risk that information with business value is being stored in private inboxes instead of the appropriate place on Meridio or other corporate system. However, it also demonstrates the corporate risk that DCSF are running, as when individuals leave, Critical information could be lost, and the risk of losing key information is a corporate and not a risk held by the individuals concerned.
78. A number of policy areas within DCSF manipulate sizeable documents and datasets, with email being the most convenient medium for transferring this information. It may be pertinent for DCSF to assess the risk of its current email policy with regard to the unlimited storage facility, to ensure that information that needs to be transferred is managed so that the risks of inappropriate storage and access to the information and datasets are limited and managed within strict policy parameters.

Recommendation 11: DCSF should review its email policy given the

potential long term risks to the organisation

Storage

79. DCSF has a contract with Iron Mountain to provide off-site storage for its documents. There are robust processes in place to ensure that items sent off-site can be tracked and retrieved when required. There is the expectation that teams and services should be proactive in selecting items to be sent off-site. However, there was evidence that some teams sent all closed files and documents for off-site storage without consideration of their business value. This is both unnecessary and an uneconomical use of resources, as information that does not need to be retained should not be retained beyond its need.

Recommendation 12: DCSF should review its guidance on use of off-site storage to ensure that only information that needs to be retained is retained

Access

“I will promote access to and re-use of our information, and protect personal and other sensitive information.”

Freedom of Information

80. The Information Rights Team in the department has responsibility for Freedom of Information (FOI) requests, data protection and copyright activity. Until recently, the team of eight also operated a shared service for FOI for the Department for Innovation, Universities and Skills, which has now become part of the Department for Business, Innovation and Skills under the recent machinery of government changes.
81. The department receives approximately 550 FOI requests and 100 Subject Access Requests annually. The department responded to 92% of all its FOI requests on target.
82. FOI requests are received via the Public Communications Unit, which are then devolved to the relevant business unit with a sample being checked by the Information Rights Team. All requests are tracked via the Electronic Correspondence Handling Organisation (ECHO) system.
83. The Information Rights Team has a site on the IWP system where extensive FOI and data protection guidance is available for staff. This guidance includes information on the process of responding to an FOI request, how to apply relevant exemptions and templates for responses.
84. As FOI is operated as a delegated system where each business unit has responsibility for responding to their relevant FOI requests, the Information Rights team provides training for those involved in the process. This is a reactive service delivered on request. A Chief Trainer has been identified to co-ordinate this work.
85. The Assessment Team were made aware that although FOI handling

and data protection procedures used to be part of the corporate induction process, they have since been removed and staff no longer receive a formal induction in this process. The department is at risk if staff respond incorrectly to FOI requests or mishandle personal data having not been provided with the necessary training at induction, particularly given that so much information is held locally.

Recommendation 13: FOI and DP training should be included in all corporate induction programmes, in the overall context of the importance of managing DCSF's information effectively and securely

Data Protection

86. The department has a substantial amount of personal, sensitive information. This includes the Contact Point database which contains millions of children's' details, and List 99 which contains details of those who have been barred from working with children. These databases contain highly confidential and sensitive personal information. The department has put stringent barriers in place to protect this information. This includes limiting who has access to these lists and what supervision is required.
87. The Information Rights Team has been proactive in providing data protection training for those in high risk areas. Most notably, the team has delivered a data protection training course for HR staff who handle sensitive personal information.
88. The team has also been involved in the development of an Information Asset Register for the organisation. Privacy Impact Assessments have been undertaken on key assets. However, because the team is limited in size, this has led to a compromise on how many can be conducted within a given period.

Re-Use

89. The department makes some of its material available for re-use on its website. All requests for licences to reproduce Crown copyright material should be directed to the Office for Public Sector Information

(OPSI, part of The National Archives), which processes the Click-Use Licence. The Assessment Team believes that there is further scope to maximise re-use of its material through identifying key information assets that may be of use to other organisations or individuals. There is a growing recognition within government and beyond that opening up departmental information to the public is essential to demonstrate transparency and accountability, engage citizens within the decision making process, raise standards and contribute to the development of new products and services. The Government's recent 'Making Public Data Public' initiative and data.gov website (the single point of access for public sector information), which are part of the Prime Minister's programme to stimulate the release of non-personal data for re-use, stress the need for public sector bodies to maximise the re-use of their information.

90. DCSF are committed to ensuring that information on the website remains available and are participating in The National Archives Web Archiving project. DCSF also follow government best practice guidance on the use of social media for business activities.

Recommendation 14: The department should review the material it makes available for re-use to determine if there are further information assets that could be surfaced and released proactively, in line with the Government's 'Making Public Data Public' initiative

Website

91. The department's corporate website is useful and user friendly. It has clear links and procedures for making FOI requests and Subject Access Requests. There are similarly clear procedures for the complaints process and for general contact with the department.
92. The website is easy to navigate with clear sections for each type of user, for example, parents, school governors or employers. This allows users to find information they are looking for quickly. The website also uses Twitter feeds and RSS feeds to keep users up to date with departmental news. This is an example of good practice.

Compliance

“I will make sure that our internal processes support effective information management.”

93. The Information and Records Team (IRMT), which is headed up by the DCSF Departmental Records Officer (DRO), provides advice and support on records and information management. The team consists of seven staff. The team’s responsibilities range from the production and overall responsibility for DCSF’s information and records management policies and procedures to the review, selection and transfer of records to The National Archives.
94. As a relatively small team, the profile of the IRMT is low across the organisation. The Team are based in Runcorn, Cheshire, away from corporate Headquarters in London. The location of the team may impact the profile of the team across DCSF, but this was not tested at the time of the assessment.
95. Staff interviewed were able to find the guidance and information they needed, in most cases on the Intranet. If they had a more complex query, staff were aware that they could contact the IRMT. The majority of queries related to the creation and allocation of folders on the corporate file plan.
96. The IRMT is pivotal to the development, implementation and monitoring of information management in DCSF, especially as there are a number of key projects in the organisation that have an impact on information and records management. Without a commitment to the development of some regular monitoring metrics to be reported at senior management level, there is risk that poor information management practices may continue.
97. Published metrics could be an effective management tool to ensure that the department is meeting its objective to raise organisational competence and awareness of what constitutes good knowledge and information management.

Recommendation 15: DCSF should assess the utility of key performance measures for information management, in line with the assessment of information risk, and with the goals of DCSF, to ensure that it is clear on the goals of the team in relation to the business

Policies and Guidance

98. The information and records management policies, procedures and guidance are held on the DCSF Intranet. The guidance is comprehensive and staff were confident that they could find the information they needed. However, staff were not always confident that they had sight of relevant policy changes or new ways of working.
99. The information and records management policy makes reference to all forms of record, irrespective of the media, including emails, wikis and blogs. Understanding of what constituted a record was inconsistent. DCSF needs to ensure that the relevant policies are supported with detailed guidance and that all staff are really clear on what they are required to do. Our assessment found that there was poor adherence to the policy.
100. Meridio does not automatically declare a record when an item is saved. Some staff were unsure when a record was to be declared. Other than raising awareness, DCSF are considering, under the IWP programme, a means by which staff are either prompted to declare a document a record, which the Assessment Team welcome.
101. The project to upgrade the Intranet may provide an opportunity to assess how staff should be alerted to new or changing internal policies to provide maximum coverage across DCSF.

Information Managers

102. The department recruited a number of Senior Information Managers and Information Managers to support the introduction of Meridio in DCSF. These individuals are local staff taking on additional responsibilities within their day job and come from all areas in DCSF. A number have IT or records management responsibilities. DCSF used

the skills, training and knowledge of the individuals to ensure that the corporate file plan and Meridio were utilised effectively. These staff were also able to use their technical knowledge to trouble shoot at a local level.

103. The Information Manager role was supported with a full training programme, seminars and a programme of forums. Gradually however, these roles have ceased as result of Information Managers leaving and not being replaced, Meridio not being used, and the lack of corporate commitment to the long-term role. A minority of Information Managers are still active in managing the file plan and Meridio within their teams.

104. It is critical that good information management is seen as a business activity that every team 'owns', just as every business team need to understand the importance of good people and financial management. DCSF need to have the mechanisms to support the local business owners or Information Managers so that they continue to contribute to the overall DCSF change programme and support the information management agenda. To this end, the Assessment Team believes that reinstating and supporting the Information Managers, and also integrating them with the IWP champions, will benefit the department and the individuals in the long term.

Recommendation 16: DCSF should develop an integrated IWP Champion and Information Manager support programme to run concurrently with the implementation project

Intranet

105. The department has recently undergone an upgrade programme for the department's Intranet. The piloting of the new Intranet began in April 2009. The intranet gives staff access to departmental procedures and guidance. The changes to the Intranet have been welcomed by interviewees, although many still raised concerns that they were not able to locate up to date contact information for colleagues.

106. Included in the IWP programme is the development of individual

“MySite” spaces for staff to upload contact details and biographies, to share contact information across the department. This was as a consequence of the various machinery of government changes and the difficulty for staff or members of the public to be able to contact the right person. Staff relied on the informal networks to find the right or latest contact information.

107. The Assessment Team were advised that all staff were to populate their “MySite” with their contact information by the end of August 2009. In the interim, staff stated that they accessed contact information via the pre-upgrade People Directory, which is managed by Human Resources.

Training

108. General induction training for new starters in DCSF is conducted via an e-learning package. Only in limited circumstances is a formal corporate induction programme run.
109. The Information and Records Management Policy covers the department’s expectations of staff as to how they contribute to effective information and records management in the organisation. Despite outlining information management responsibilities, training on records and information management is not included in any induction training for joiners to the department.

Recommendation 17: DCSF should introduce training on information and record keeping as part of all its induction programmes that emphasises how critical good information management is as a business activity that every team ‘owns’

110. The guidance states that the business embedded Information Managers are responsible for providing training on records management. A number of active Information Managers had taken this on as a responsibility, but the application was not consistent. The result is that most staff who joined DCSF in the last few years have not undergone any formal training and have been left to adopt their own work practices. If it was not for the diligence of a number of Information

Managers, no training would be provided. The outcome is that the inconsistency of approach has led to inconsistent levels of effective information and record management in DCSF, and an increase in risk to the Department as a whole.

111. Training on information and records management should not be seen as solely the responsibility of the central IRMT team. The commitment to training needs to be part of any upgrade or new ways of working in DCSF. Good records and information information management should be seen as a corporate requirement, just as good financial and people management is. Therefore, it would be appropriate for there to be corporate ownership of the training, with ongoing support provided by local Information Managers
112. The Assessment Team recommends that IRMT, in conjunction with HR, review how relevant training on knowledge, information and records is disseminated and integrated as part of the ongoing corporate change programme. This will enable a consistent approach to record and information management in DCSF

Recommendation 18: DCSF should ensure that IRMT, HR and others develop an appropriate training programme that includes knowledge and information management for all staff

113. DCSF should take responsibility for ensuring that staff have access to the guidance and protocols for effective information and records management. It should also ensure that there are other formal mechanisms for information sharing and training so that all new staff are actively aware of their responsibilities.
114. In 2009, the majority of training currently undertaken in DCSF, other than that for information security, is not mandatory. Therefore staff either did not attend or were not aware of any training opportunities.
115. Currently, the learning opportunities are provided via the Intranet-based e-learning or workshop presentations. Online training requires people to prioritise training in their busy schedules. Staff who had attended these workshops believed that they did not get the full benefit

in the workplace as support beyond the workshops was often not available. Additionally, people trained to do particular roles are not always replaced when they leave, creating gaps in legacy knowledge and training.

Recommendation 19: DCSF to review training methods and assess ongoing support to ensure that maximum benefit is derived from the training for individual staff and the department

116. As highlighted elsewhere in this report, there has been an absence of ongoing training aligned to previous system upgrades and roll outs. The implementation of the IWP project has made it imperative that DCSF ensures that the implementation programme includes consideration for the resourcing of future training and the support of specialist staff.
117. The Assessment Team were advised that there are plans to appoint a number of IWP “champions” or “super users” to support and provide training on setting up and monitoring the use of TeamSites and MySites. This is to be commended. DCSF must ensure that these “champions” or “super users” are supported by regular seminars and training, as they are the frontline operational users who will be able to give feedback on lessons learned to the department and provide consistency in application across the organisation.
118. DCSF need to ensure that the “IWP champions”, as part of their training, have a knowledge and understanding of what constitutes good knowledge and information management principles. Otherwise, there is the risk that the IWP Champions, and the already existing Information Managers, are seen as separate entities and not recognised as a resource able to set and influence how corporate records and information standards are proliferated into the department.

Web Continuity

119. It is imperative that departments actively manage their web content. Without this, there is the risk of broken URLs and that official publications made available only in electronic format are not captured.

The National Archives is currently working with most government departments to ensure that the government web estate is archived. The National Archives is also working with departments to develop a solution to the issues and developing best practice for webmasters. DCSF is not currently engaged in the web continuity programme.

120. We recommend that DCSF works with the Web Continuity Team within The National Archives to ensure that web content is captured and that the department has access to current best practice. There is no cost to DCSF for this work.

Recommendation 20: DCSF to work with The National Archives Web Continuity Team to ensure web content is captured

Culture

“Information is recognised as the key asset for running the business of the Department for Children, Schools and Families, and is used to support effective data and information sharing and knowledge creation.”

121. Widespread sharing of knowledge and information is not yet at a mature level in DCSF. There is no system to help staff share the information they hold. At present, it depends on previous contacts rather than a need to know. Staff have a tendency to hoard information, even in teams that produce and analyse data and information to assist policy making. For example, one team’s focus was to provide information externally without consideration of how that same information could benefit policy-making within DCSF. This example is repeated across the department. Without the will or the explicit direction to share information internally, there is a risk that the department is under-utilising its information and therefore potentially wasting resources.
122. DCSF is recognised internally as having a dominant culture that is averse to mandating or being overly prescriptive in how internal business is conducted. This policy does engender a more relaxed and informal work environment. This does much to encourage innovation and has a positive effect on morale. However, conversely, this “laissez faire” approach does have a negative impact on information management, and potentially significantly increases risk to DCSF as a whole. For example, use of Meridio was not mandated. Staff were allowed to “opt out” of using the system without sanction. The net result has been inconsistent usage and a significant risk that since its implementation, information with business value may have been lost completely.
123. Internal directorate changes and staff movements have led to the risk of a persistent loss of information with corporate value. Non-adherence to the corporate process and procedures is a risk that DCSF cannot afford to take. There is the potential that the level of loss may not be recognised and this may have a lasting impact on the reputation of

DCSF. The major change programme that DCSF is implementing should address the cultural impact of not mandating policies and ensure that DCSF provides clarity on what is expected at all levels, from senior management down.

124. With the raised expectation in adherence to guidance and protocols, all staff should understand how information and processes that generate information with business value are identified and how they contribute to the business. Where this is currently identified by individuals, the most common criteria for identifying what they deemed as business value was “common sense.” In a central government department such as DCSF, commonsense needs to be translated into something tangible that can be understood by a everyone. Reliance on the individual’s perception of what has business value, without clearly defined corporate criteria, is not sustainable in the long term.

Recommendation 21: DCSF should recognise that the Knowledge of the organisation must be managed, and that a formal and mandated set of processes, systems and principles be established and governed

125. The National Archives’ “What to Keep” project will assist DCSF in developing processes to identify business critical information. DCSF have already demonstrated commitment to the project in its pilot stage by agreeing to contribute case studies on how they are currently approaching the what to keep issue.

126. The impact of not mandating policies and procedures also has repercussions on how different teams conduct their business. The Assessment Team found that this fostered a culture of autonomous working practices. Sharing of knowledge and information outside of the immediate work area was not usually considered.

Recommendation 22: DCSF to consider implementing a formal repository of Knowledge and Information assets to maintain the corporate memory

127. IWP is key to addressing some of the issues identified throughout the

report. This programme, once implemented, can do much to set a new standard in DCSF and across government. It is a major piece of work which supports aspects of the internal change programme. IWP incorporates a new departmental Intranet, Team Sites, MySites and Records Centre. It is through this system that the department hopes to capture and manage its future electronic information.

128. The Assessment Team take the view that the full implementation of IWP will provide some of the physical means to share information across specific teams and if used effectively will contribute to sharing of knowledge, information and best practice.
129. Overall, information management and records management has a low departmental profile. The priority for the department is information assurance, which is perceived as more important. The security agenda has visibility, priority and profile in addition to senior support.
130. DCSF in the main was considered by those we interviewed to be an IT driven department. This has many benefits, as evidenced by the extensive progress made in securing information, and the commitment that has been made to upgrade the internal IT systems, and also the formulation of the IWP programme. There is a risk that the IT infrastructure changes are seen internally as enough to change behaviours and raise standards in the department. IT changes are only one part of the solution; the culture and governance structures within the department need to support good information management.
131. The priority for DCSF is to ensure that knowledge and information management are afforded the same priority level as information assurance. It should be emphasised that good knowledge, record and information management is at the heart of the business, supported by strategic direction and effective resource management. These should be underpinned by clear and consistent policies and guidance that support the business objectives.

APPENDIX ONE: SUMMARY OF RECOMMENDED ACTIONS

This is a summary of the recommended action to:

- remedy the weaknesses identified; and,
- strengthen the commitment to the Information Management Assessment Programme.

These recommendations, when agreed, will form an Action Plan that will be monitored.

Business Area	Ref	Recommendation
Governance and Leadership	1	In line with the Hannigan Review guidance, DCSF should ensure that they have board representation covering all aspects of information risk, and not just information security
	2	The Board should follow the guidance set out in the Information Matters report and consider information risk alongside, and as a contributory part of, other key risks, and give it priority accordingly
	3	DCSF should consider the formation of an Information Management Board to oversee all aspects of knowledge and information management
	4	DCSF, in line with the KIM reporting structure, should develop and communicate clear responsibilities for all staff
	5	DCSF to ensure that the IWP champion roles are clearly defined and fully supported
	6	DCSF to define, communicate and mitigate Information Management risk within its corporate and business reporting systems
Records Management	7	DCSF should define what information it needs to keep, with the support of The National Archives, and ensure that all staff are aware of this
	8	DCSF should revise the records and information management policies to ensure that they include fully the use of digital media

	9	DCSF should review the current resource levels to ensure that it will continue to meet future statutory requirements
	10	DCSF should develop a migration policy to manage legacy information
	11	DCSF should review its email policy given the potential long term risks to the organisation
	12	DCSF should review its guidance on use of off-site storage to ensure that only information that needs to be retained is retained
Access	13	FOI and DP training should be included in all corporate induction programmes, in the overall context of the importance of managing DCSF's information effectively and securely
	14	The department should review the material it makes available for re-use to determine if there are further information assets that could be surfaced and released proactively, in line with the Government's 'Making Public Data Public' initiative
Compliance	15	DCSF should assess the utility of key performance measures for information management, in line with the assessment of information risk, and with the goals of DCSF, to ensure that it is clear on the goals of the team in relation to the business
	16	DCSF should develop an integrated IWP Champion and Information Manager support programme to run concurrently with the implementation project
	17	DCSF should introduce training on information and record keeping as part of all its induction programmes that emphasises how critical good information management is as a business activity that every team 'owns'
	18	DCSF should ensure that IRMT, HR and others develop an appropriate training programme that includes knowledge and information management for all staff
	19	DCSF to review training methods and assess ongoing support to ensure that maximum benefit is derived from the training for individual staff and the department
	20	DCSF to work with The National Archives Web Continuity Team to ensure web content is captured

Culture	21	DCSF should recognise that the Knowledge of the organisation must be managed, and that a formal and mandated set of processes, systems and principles be established and governed
	22.	DCSF to consider implementing a formal repository of Knowledge and Information assets to maintain the corporate memory

APPENDIX TWO: GLOSSARY

IM	Information Management
IMA	Information Management Assessment
IMD	Information Management Directorate
KIM	Knowledge and Information Management
KPI	Key Performance Indicator
SLA	Service Level Agreement