Appendix 2

Information Commissioner Audit Outstanding Recommendations
Action plan and progress

Recommendation	Agreed action, date and owner	Progress by November 2013
Training and Awareness		
A19 Ensure that annual mandatory Data Protection refresher training is developed and monitored. This could take the form of e-learning for most staff and additional face to face training for staff with specific information governance responsibilities.	Mandatory refresher training will be provided to relevant staff on an annual basis with attendance required every three years. New HR portal will monitor training. Implementation date: July 2013 Responsibility: Data Protection Officer	Organisational Development have confirmed that work is continuing in respect of the roll out programme that will alert staff in future on when they need to do a refresher (e.g. at the 3 yr point). **Estimated revised completion date: 31 March 2014**
A21 Require all managers to attend the additional data protection training.	HR portal will track the training of all staff including managers, and report on those that haven't attended. Training sessions will be developed and targeted at managers. All managers whose staff handle personal data will keep records and do regular spot checks to ensure training is completed Implementation date: July 2013 Responsibility: Data Protection Officer	Please refer to A19 above.
Records Management		
B5 Development work on an Information Asset Register (IAR) must be completed and should be linked to DMBC's retention and disposal schedules. Assets must be regularly risk assessed and the register reviewed by the SIRO.	This is a significant task given the size of the Council. A number of service areas are piloting the development and this will be compiled by the end of June 2013. The register will then be rolled out to the whole of DMBC but due to the size of the organisation, stringent checks will be put in	Information Asset Owners (IAOs) have been advised of their role in which the IAR is introduced. Training is being carried out and within the training the IAR is referred to and explained in more detail. The IAOs, once trained, will be required to complete their aspect of the IAR by the 31st January 2014, to enable a fully populated IAR to be in place by April

	place to ensure quality of the information entered. **Implementation date: April 2014** Responsibility: Information Management Officer	2014. **In progress**
B6 Identify and appoint business system owners, of an appropriate seniority, to assist IAOs. They will be accountable for identifying and risk assessing the information assets held within their departments and a forum of these Information Asset Administrators (IAAs) should be set up to share good practice and raise awareness.	Business System Owners (BSOs) will be identified by Heads of Service / Information Asset Owners who will support them along with key members of staff in their service areas. Implementation date: July 2013 Responsibility: SIRO	IAOs will be required to provide the names of BSOs and IAAs within 2 weeks of completing the training. They will be expected to ensure that their nominated BSOs and IAAs are aware of their responsibilities and to carry out the General User e-learning as mentioned in A10. **Estimated revised completion date: 31 March 2014**
B10. Develop and implement a comprehensive Records Management policy (as advised by the Code of Practice under s46 FOI Act 2000).	The Council accepts the need for a comprehensive Records Management Policy and this will be implemented. Implementation date: June 2013 Responsibility: Information Management Officer	Review and approval by senior management and communication to all staff to be completed.
B15. A review of all physical locations where personal data is held should be undertaken by DMBC and premises assessed for security and environmental factors. Manual records stored in unsuitable locations should be moved to secure storage as soon as is practical.	The Council recognises the need for a greater compliance function across all areas of Data Management; the Information Team will inspect areas. The use of Internal Audit is also being considered to carry out this function. Implementation date: September 2013 Responsibility: Information Team:- Data Protection Officer Information Management Officer Freedom of Information Officer	This will follow on from the appointment and training of the IAOs. **Estimated revised completion date: 31 March 2014**
B20 Ensure that leavers' files are weeded to the same standard as current files before they are sent to archive.	Files that have reached the end of their retention period will be destroyed – July 2013 The files of the leavers still within their retention period will be weeded.	The Head of Human Resources has confirmed that they are weeding out leavers when they are removed from current filing and prior to archiving. **Estimated revised completion date: 30 June**

	Implementation date: November 2013 Responsibility: Head of Human Resources	**2014**
B32 Ensure all staff are made aware of the current retention and disposal periods as recorded in the new schedule.	This will be cascaded through staff with information management responsibilities – IAOs, IAAs, Data Protection Lead Officers & FOI Lead Officers. Implementation date: July 2013 Responsibility: Information Management Officer	IAOs have been made aware of their responsibilities through an e-mail sent by the SIRO. Retention schedules are also included in the IAO training. Finalising of the remaining retention schedules is still underway and this will be aided now by the establishment of the IAO as a point of contact. Once these have been finalised they too will be available on the new web page for all staff and members of the public to be able to access. **Estimated revised completion date: 31 March 2014**
B37 Ensure that staff are aware that personal data stored on their S-drive must be disposed of in line with corporate retention and disposal schedules. Personal data should normally be held on corporate networks where retention and disposal schedules can be applied and monitored.	The Council recognises that this is an area of data storage that requires overhauling. Initial steps will be to review all data that hasn't been used for more than 6 years. Guidance to IAOs will be given regarding the rules around S drive. A demonstration will be given by Northgate to show the Records Management Function of the EDMS system by end of March 2013. **Implementation date: April 2014** Responsibility: Head of ICT Support Head of ICT Solutions	It is included in the Data Retention & Disposal Policy that retention periods relate to information in all formats, including electronic. The demonstration by Northgate has taken place and has revealed interesting information and figures in relation to what is stored on the Council's S Drives. The demonstration was undertaken using information held in the Children & Young People's area, the report is attached, however, we have redacted the information relation to costs. It is envisaged that this product will be purchased.
B43 To provide assurance to the SIRO on compliance with the Data Protection Act ensure Records	Risk management registers are to be re-written. To be added that when risk assessments are carried out Data Protection,	Information Governance is now included in the Risk Register Process, this is due for approval in February 2014. Attached is a copy of the e-mail

Management risks, including security, availability and disposal of records, are identified in Strategic, Operational and Work Plan risk registers, with controls identified and managed effectively.	Information Governance and Records Management must be included. Implementation date: September 2013 Responsibility: Policy and Performance Team	sent to Policy & Performance Team agreeing the wording to be included. A draft copy of the process is attached. **Estimated revised completion date: 28 February 2014**
Data Sharing		
C2 Assign responsibility for oversight of data sharing to a person or persons. This should include the periodic review of all data sharing agreements to ensure they are up to date and have been approved by a suitable senior person.	Information Asset Owners will have overall responsibility for data sharing agreements in their area and drawing up and updating the agreements. Requests for data sharing protocols will go to the SIGB board for Approval. A central log of all data sharing agreements will be kept by the Information Team. **Implementation date: April 2014** Responsibility: IAOs, SIRO Information Team:- Data Protection Officer Information Management Officer Freedom of Information Officer Head of Information and Transformation	The central log is currently being populated and all new agreements will be added to the log as they are approved by the SIGB. Also, all rejected data sharing requests will also be recorded and published for transparency purposed.
C5 Include the requirement for conducting Privacy Impact Assessments (PIAs) as part of a data sharing policy (see c1) as recommended in the ICO Data sharing Code of Practice.	The Council will develop and implement a data sharing policy in which it will be recommended that a PIA must be carried out if personal information is to be shared. Implementation date: July 2013 Responsibility: Data Protection Officer Information Management Officer IAOs to carry out PIAs	A PIA template has been developed and provided to the IAO in their IAO training. All new ICT projects will now require a PIA if personal/sensitive personal information is identified as part of the request for a new piece of work. Once the Project Officer receives the request if a PIA is required the request is referred to the Information Team for advice and guidance. The process is currently being finalised with ICT.

		IAOs are also advised that a PIA will also need to be carried out if there is an amendment to an ICT system which processes personal/sensitive personal information. Additional external training has also been arranged on privacy impact assessments for IAO's on the 10th and 31st January 2014. **Estimated revised completion date: 31 January 2014**
C10 Ensure shared data is accurate, retention and disposal arrangements have been agreed and assurance received that recipients will delete, destroy or return shared data once the purpose is served.	These recommendations will be incorporated into the new data sharing policy and the current master data sharing agreements. Implementation date: July 2013 Responsibility: Data Protection Officer Information Management Officer	Amendments are being made to the data sharing agreements to align them with the data sharing policy but to also ensure that the recommendations are contained within them. **Estimated revised completion date: 31 March 2014**
C13 Internal Audit to consider including data sharing agreements, together with procedures and protocols, as part of their system audits.	The SIRO will discuss and agree this with internal audit. Implementation date: July 2013 Responsibility: SIRO, Internal Audit	Internal Audit are carrying out a specific Data Sharing Audit. **Estimated revised completion date: 31 March 2014**