APPENDIX 2

Detailed findings and action plan

7.1 Scope a: Training and awareness. The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities.

Risk: If staff do not receive appropriate data protection training, in accordance with their role, there is a risk that personal data will not be processed in accordance with the DPA resulting in regulatory action and/or reputational damage to the organisation.

a3. There is a Corporate Management Team (CMT) consisting of the Chief Executive, Directors and Corporate Heads of Service, which considers reports provided by the Democracy & Governance Manager (who is the Council's Data Protection lead) in regard to data protection training. These reports are general in nature (for example, raising awareness of data protection), rather than including training completion figures or KPIs. A report to CMT in December 2012 from the Democracy and Governance Manager detailed a request for training completion figures from Heads of Service but at the end of November only Legal and Democratic Services had supplied figures.

Recommendation: Reports to the Corporate Management Team should include training statistics from all Services regarding completion, or otherwise, of required data protection and related training, to provide a corporate overview.

Management response: Accepted

Implementation date: End of 2013

Responsibility: Each Head of Service

a9. The WDT is an exception at FCC in that the other Directorates do not each have their own dedicated training teams.

Recommendation: Ensure Directorates have a similar or equivalent mechanism to that in Community Services to ensure clear accountability for and delivery of required data protection training.

Management response: Partially accepted. Community Services Directorate have a greater need for Data Protection training than other Directorates and it would not be a sensible use of resources to have 9 additional staff giving training on Data

Protection. We will ensure each Directorate has appropriate mechanism for Data Protection training for that Directorate.

Implementation date: End of 2013
Responsibility: Democracy & Governance Manager

a11. There is no Corporate Training Manager, centralised function or post which has clear responsibility for the provision and monitoring of data protection training across FCC as a whole. This lack of overview increases the likelihood of inconsistency in the training provision across separate Directorates and departments.

Recommendation: FCC should take steps to centrally monitor and coordinate data protection training on an organisation wide basis.

Management response: Accepted.

Implementation date: End of 2013
Responsibility: Democracy & Governance Manager

a12. An internal audit in June 2012 identified that training records should be updated and centralised to better identify who should receive data protection training. A Strategic Risk Assessment undertaken in September 2012 prescribed that staff processing personal data should receive appropriate training. However, there is still no centralised corporate training programme for FCC and each Directorate is responsible for training their own respective staff, including training programmes, calendars, strategy and training needs analysis.

Recommendation: FCC should develop a corporate data protection training programme to identify and direct strategic and consistent DP training delivery.

Management response: Partially accepted. It is the responsibility of each Head of Service to identify and arrange for their staff to have appropriate Data Protection training. Only they can identify what training is appropriate for their staff. The Data Protection Team have provided a range of different Data Protection training options. The team will develop this further to give corporate advice which option is appropriate for the different circumstances that exist in the different services.

Implementation date: End of 2013
Responsibility: Democracy & Governance Manager

a21. The Information & Support Manager, within Corporate Services, maintains training logs in respect of data protection training (for example, in respect of 'Lunch and Learn' sessions from 2010–13 and 'Act Now' external training from 2008-13) which record details such as the name of the employee, details of which Service and Directorate the employee belongs to, the training attended and the

date of training.

Recommendation: FCC should produce monthly reports within the Directorates, regarding completion of required data protection and related training. FCC should also produce an aggregate overview of this for reporting of the training provision to the Corporate Management Team.

Management response: Partially accepted. It is the responsibility of each Head of Service to put in place appropriate arrangements for that service. In future this will be part of the existing quarterly reporting arrangements to Corporate Management Team.

Implementation date: By the end of 2013

Responsibility: Heads of Service

a23. The Paris administration team are currently considering the introduction of a new database to log training information such as what training has been received, competency levels, etc. It is unclear as to whether it would be possible to expand this prospective monitoring and reporting tool to encompass other data protection related training.

Recommendation: see a22

Management response: Not accepted. If the recommendation is to expand the database to log Data Protection training other than training for Paris, this would not be appropriate and would duplicate the database held by WDT.

Implementation date:
Responsibility:

a24. There are currently no KPIs regarding data protection or related training. This raises the risk of FCC having no clear Directorate level or corporate oversight regarding the provision and take-up of the data protection training provided.

Recommendation: FCC should introduce KPIs in regard to data protection training to proactively monitor and stimulate competency and completion levels.

Management response: Accepted.
Implementation date: End of 2013
Responsibility: Democracy & Governance Manager

a27. The WDT are able to generate electronic reports as to which individuals in the Community Services Directorate have applied for and then failed to attend data protection related training, but this is not undertaken on any formal or regular basis. It is unclear what process, if any, the other Directorates which do not have their own equivalent of the WDT utilise in respect of identifying and following up non-

attendance at data protection training.

Recommendation: FCC should introduce appropriate mechanisms in Directorates outside of Community Services for identifying and following up non-attendance of data protection training. Management information in relation to non-attendance by Directorate should also be provided to CMT to provide corporate oversight of this aspect.

Management response: Partially accepted. There may be good reasons for failing to attend Data Protection training such as sickness absence. The important issue is that they receive training, not the reason for non attendance. It is the responsibility of Heads of Service to ensure that where such training has been missed, the officer receives Data Protection training at a later date. Management information on who has received Data Protection training will however be included in the future reports to CMT.

Implementation date: By the end of 2013

Responsibility: Heads of Service and Democracy & Governance Manager

a31. The information security presentation explains the role of the Information Governance Manager, information security, the types of personal data processed by FCC, prohibited actions, the effect of data protection breaches, the powers of the ICO, the data protection principles and subject access requests. However, the presentation appears to indicate that the sixth principle of the DPA only relates to the right of subject access.

Recommendation: The Information Security Presentation '8 Data Protection Principles' slide should be clarified to indicate that all rights of the individual under the DPA have a central basis under the sixth data protection principle, although the right to subject access may be foremost amongst these.

Management response: Accepted

Implementation date: 1 September 2013
Responsibility: Information Governance Manager

a40. The Community Services Directorate Management Team (DMT) have identified that individuals should attend the recently developed course every three years. This is a relatively long interval for refresher training and may raise the risk of staff DP awareness not remaining current.

Recommendation: FCC should review the timeframe for refresher data protection training and give serious consideration to an annual cycle.

Management response: Partially accepted. The Council's Statement of Data Protection Policy clearly makes this the responsibility of Directors and Heads of Service. It also makes clear that the timeframe will differ from one department to another dependant

upon the degree of risk. In order to ensure consistency the Data Protection team will put forward recommended periods for different degrees of risk.

Implementation date: 1 November 2013
Responsibility: Heads of Service and Democracy & Governance

a42. Excluding the refresher requirement for the Community Services Directorate Data Protection course, we found no additional evidence to support provision within other directorates for periodic and mandatory data protection related refresher training, in line with the Statement of Data Protection Policy and Practice, Internal Audit recommendations and good practice requirements.

Recommendation: FCC should extend the provision of periodic and mandatory data protection related refresher training across their whole organisation.

Management response: Accepted. The Council's Statement of Data Protection Practice & Policy makes clear that it is already extended across the whole organisation. The audit visit concentrated on Community Services staff but nevertheless at least one example of other staff was given during the audit visit. Please also see a40 management response.

Implementation date: Already in place
Responsibility:

a43. The Records Manager has undertaken training in respect of the Information Systems Examination Board (ISEB) Certificate in Data Protection and intends to sit the examination. However, we found no evidence that other members of staff including members of the DPT, have or are expected to undertake the same training.

Recommendation: FCC should ensure that appropriate members of the Data Protection Team who have not undertaken ISEB training to date do so.

Management response: Partially accepted. This will be seriously considered but is dependant upon factors such as cost and the length of the training course as well as the benefits of it.

Implementation date: June 2014
Responsibility: Data Protection Team

a46. However, outside of the ISEB training for the Records Manager and the WASPI ISP Facilitator training for several members of staff, there is no evidence of specific data protection training for specialised roles or functions.

Recommendation: FCC should introduce the provision of specific data protection training for specialised roles or functions (such as SIRO, IAOs, SAR handlers) as appropriate.

Management response: Partially accepted. Whilst training will be provided for SIRO and IAO's it is believed the existing arrangements of guidance and access to a member of the Data Protection team is sufficient for SAR handlers.

Implementation date: By end of 2013 for SIRO and within 6 months of their appointments for IAOs.
Responsibility: Democracy & Governance Manager

a49. In more general terms, there is extensive data protection related material available on 'Infonet' in regard to formal policies, relevant internal contacts, related news articles and links to ICO guidance.

Recommendation: The 'Do's and don'ts' poster, the 'DP – what is it?' section of Infonet and the DP Adult Social Care policy should be amended to reflect that employees would only be liable to individual fines as a result of deliberate and / or reckless offences under s.55 of the DPA committed without the consent of FCC and not unintentional errors committed in the course of their employment.

Management response: Accepted
Implementation date: 1 September 2013
Responsibility: Democracy & Governance Manager

a50. The 'Individuals' rights' section of Infonet does cite the relevant sections in respect of some rights under the DPA (e.g. s.10), but not others (e.g. s. 11), although data subjects may cite these sections when seeking to exercise these rights. The guidance on Infonet does however explain the right given by Section 11.

Recommendation: The Individual Rights section of Infonet should include all data subjects' rights within the provisions of the DPA in order for staff to be better able to identify these in practice.

Management response: Accepted
Implementation date: 1 September 2013
Responsibility: Democracy & Governance Manager

a58. It appeared that staff whose roles involve records management have undertaken general data protection training such as the e-learning modules on 'Infonet' and the 'Act Now' courses. However, they have not undertaken any standalone records management training and it appears there is none currently available.

Recommendation: FCC should introduce appropriate records management training for members of staff who have specialised records management roles or functions.
Management response: Accepted
Implementation date: June 2014
Responsibility: Records Manager

7.2 Scope b: Records management. The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.

Risk: In the absence of appropriate records management processes, there is a risk that records may not be processed in compliance with the DPA resulting in regulatory action by the ICO, reputational damage to the data controller and/or damage and distress to individuals.

b2. There are no formal Terms of Reference for the DPT agreed at senior level. Paragraph 4.5 of the Statement of Data Protection Policy & Practice provides a broad overview of the purpose of DPT but does not contain specific details including member's roles and responsibilities, specific deliverables and measures to ensure these are met, frequency of meetings, quorate requirements or decision making authority.

Recommendation: Draft Terms of Reference for the DPT to ensure roles and responsibilities, decision making and quorums are clearly defined.

Management response: Accepted

Implementation date: 1 September 2013
Responsibility: Democracy & Governance Manager

b5. The Council have decided not to appoint a Senior Information Risk Owner (SIRO), instead spreading this responsibility amongst senior CMT staff with appropriate expertise.

Recommendation: Appoint and train a senior level SIRO.

Management response: Accepted. It has been decided that the Head of Legal & Democratic Services will be the Council's SIRO.

Implementation date: End of 2013
Responsibility: Corporate Management Team

b6. Although 'data set owners' have been identified they have not been trained to risk assess and report on the resources in place to maintain and protect the integrity of the systems they own and the personal data they contain.

Recommendation: Ensure data set owners are trained to perform the role of Information Asset

Owners in line with the 'Local Public Service Data Handling Guidelines v2 - August 2012'.

Management response: Accepted

Implementation date: Within 6 months of their appointment.
Responsibility: Democracy & Governance Manager

b13. The RM policy has been in place for a number of years and it was reported it had been approved by CMT. However, the Council did not appear to have robust procedures for creating and reviewing policy documents to ensure input from across the Council. This would include an appropriate cover sheet documenting version control, review date, policy owner, date approved and the approving body.

Recommendation: Ensure a standard procedure for creating and reviewing all policies, including the Records Management policy, as part of a regular policy review cycle to ensure they are kept up-to-date and reflect the current needs of the authority. This would include an appropriate cover sheet as described above.

Management response: Accepted in so far as this relates to Data Protection and Records Management Policies.

Implementation date: 1 September 2013
Responsibility: Democracy & Governance Manager

b14. The RM policy focuses on retention and destruction processes but does not identify and make connection to related policies, including email, information security, protective marking and data protection. Neither does it define RM roles and responsibilities or state how compliance with the policy will be monitored.

Recommendation: Review the RM policy to ensure it complies with the recommendations in Part 1, section 7 of the s46 Code of Practice on records management.

Management response: Accepted
Implementation date: End of 2013
Responsibility: Records Manager

b15. The Council's website does not currently have a 'Privacy Notice' or 'Information Charter' explaining why the Council collect personal data and what they do with it.

Recommendation: Ensure the Council's website includes a clear Privacy Notice statement, accessible from the home page.

Management response: Accepted.
Implementation date: 21 May 2013
Responsibility: Democracy & Governance Manager

b20. The Council do not have an Information Asset Register. This is a single list of all hard copy and electronic records, who is responsible for them, where they are stored and who has access to them. The register should be held in an accessible format and should also have a nominated owner responsible for ensuring it is reviewed and kept up to date.

Recommendation: Ensure a single Information Asset Register is produced of all the Council's electronic and paper records. The register should have an owner, be regularly reviewed and contain details of who is responsible for the assets, a risk assessment, where they are stored and who has access to them.

Management response: Accepted.

Implementation date: End of 2016
Responsibility: SIRO

b24. The introduction of an EDM system and a structured fileplan will reduce the current use of departmental file shares for group working. Work is on-going to integrate EDM with Paris and an imminent solution to this will enable EDM to be rolled out to Social Services.

Recommendation: Ensure the work to integrate EDM and Paris is continued to enable Social Services to store unstructured data on the corporate EDM.

Management response: Accepted

Implementation date: End of 2014
Responsibility: Information Governance Manager

b40. Hard drives are kept securely by IT before disposal by an approved 3rd party contractor. A 'Secure Disposal of Storage Media' procedure is in development.

Recommendation: Ensure the procedure on 'Secure Disposal of Storage Media' is completed and distributed to all relevant staff.

Management response: Accepted.

Implementation date: End of 2013
Responsibility: The Information Governance Manager

b41. Not all electronic systems holding personal data have archiving and disposal functionality. This includes Paris and Care.com. Work is on-going to address these issues with Paris but it was not clear what will happen to data held on Care.com. The Trent HR system does have deletion schedules for staff records including disciplinaries and grievances.

Recommendation: Ensure all electronic records, including those in Care.com, can be archived or deleted in line with the Councils retention schedules.

Management response: Partially accepted. This will be done for Paris and Care.com and investigated for other electronic record systems.

Implementation date: June 2016
Responsibility: Heads of Service and Information Governance Manager

b43. There is no time limit on retaining personal emails although there is limit on mailbox sizes. Emails containing personal data held indefinitely may breach principle five of the DPA.
Recommendation: Investigate if there is a function available with the Council's email application that will apply automatic disposal schedules.

Management response: Accepted

Implementation date: 1 October 2013
Responsibility: Operational Services Manager

b44. Records management performance measures are not identified in the RM policy. However, monthly KPIs, including box deposits and retrievals, and boxes destroyed, are reported by the Records Manager to the Director of Lifelong Learning. It was not known if these KPIs are subsequently reported to CMT.

Recommendation: Include performance measures or KPIs in the Records Management policy so the effectiveness of the RM function can be measured.

Management response: Not Accepted. It is not appropriate for performance measures or KPIs to be included in policies. The KPIs will however be included in the quarterly performance reports considered by Corporate Management Team.

Implementation date: December 2013
Responsibility: Records Manager

b45. Internal audit provided substantial assurance of the Records Management service in 2006. The frequency of this audit is stated as one in three years but it has not been repeated since, due to other more highly risk rated audit priorities.

Recommendation: Internal audit should review whether Records Management should be included in the audit plan as part of a three year review cycle.

Management response: Accepted. Already reviewed annually as part of the planning process. The findings of this report will inform the next annual review.

Implementation date: January 2014
Responsibility: Internal Audit Manager

b49. It is important that records and information management is included in the corporate risk management framework. However, no risks relating to records management were identified in either the QPRs or SARC reviewed onsite.

Recommendation: Ensure records and information management risk is incorporated into service level plans so potential threats can be identified at an early stage.

Management response: Accepted.

Implementation date: June 2014
Responsibility: SIRO and Heads of Service

b53. The Council have decided that Privacy Impact Assessments (PIAs) are not appropriate at this time as they are too resource intensive to undertake for small scale information systems development.

Recommendation: The Council should consider conducting PIA assessments when developing any projects that will process personal data on a case by case basis. These should be based on the recommendations in the ICOs PIA handbook which include conducting preliminary assessments on the level of PIA required in each case.

Management response: Partially accepted. PIA assessments will be considered for appropriate projects but not for all projects due to the resource implications.

Implementation date: End of 2013
Responsibility: SIRO and Data Protection Team

7.3 Scope c: Data sharing. The design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.

Risk: The failure to design and operate appropriate data sharing controls is likely to contravene the principles of the Data Protection Act 1998, which may result in regulatory action, reputational damage to the organisation and damage or distress for those individuals who are the subject of the data.

c5. Although the ISPs typically tend to indicate a requirement for partner organisations to ensure that members of their staff who are involved in systematic data sharing at a less senior operational level are appropriately trained, FCC does not provide specific training in regard to regular data sharing.

Recommendation: FCC should develop and introduce specific data sharing training for operational staff who have responsibility for systematic data sharing.

Management response: Partially accepted. Guidance will be produced, including who should be contacted with queries. Data sharing is best covered as part of the corporate training arrangements.

Implementation date: End of 2013
Responsibility: Democracy & Governance Manager

c8. In terms of one off disclosures, no senior authorisation or sign off is obtained, unless purely administrative members of staff have received the request for an ad hoc disclosure or the information requested engages considerations in respect of the Protection of Vulnerable Adults.

Recommendation: FCC should develop and introduce formal training and documented procedures specifically in regard to one off disclosures and these should ensure appropriate sign off.

Management response: Partially accepted. There is no need for routine senior authorisation or sign off if staff are appropriately trained. Further guidance will be produced on this, including who to contact with queries. It is best covered in the corporate training arrangements.

Implementation date: End of 2013
Responsibility: Democracy and Governance Manager

c13. There does appear to be some quality control in terms of an Information Officer considering the content of draft factsheets and forms to be distributed to prospective data subjects. However, the emphasis of this quality assessment does not include fair processing requirements.

Recommendation: FCC should ensure that there is a uniform mechanism for quality assessment of fair processing information across the organisation.

Management response: Accepted. There already exists a uniform mechanism whereby advice can be sought from the appropriate contact on the Data Protection team. The Data Protection team will issue further guidance on what needs to be covered in a fair processing notice.

Implementation date: September 2013
Responsibility: Democracy & Governance Manager

c14. It was reported that there are fair processing templates available on 'Infonet', but although the completed forms and leaflets which we have been able to view do provide fair processing information, the information provided is of varying detail.

Recommendation: FCC should ensure that the provision of fair processing information is uniformly consistent in terms of identifying FCC, the purposes for processing and any further appropriate information to ensure the processing is fair.

Management response: Partially accepted. Different parts of the Council will use personal information for different purposes and share it with different bodies therefore it is not possible to have uniform consistency. If however, this recommendation also relates to the quality of fair processing notices see management response to c13.

Implementation date: September 2013
Responsibility: Democracy & Governance Manager

c21. The ISPs themselves are currently stored within operational team files. However, FCC is considering putting all ISPs onto EDM to improve central oversight.

Recommendation: FCC should put all ISPs in a single place on EDM to enable central oversight.

Management response: Partially accepted. A central location for the storage of all ISPs will be created within the Data Protection team folder on the Council file share.

Implementation date: June 2013
Responsibility: Information Governance Manager

c26. In instances of regular data sharing and one off disclosures, the specific arrangements for retention and disposal are left to the discretion of each partner agencies' policies with the caveat that they should comply with the retention and security requirements of the DPA. It was reported that assurances are not obtained in regard to destroying personal data, but that partner organisations are able to audit each other's processes.

Recommendation: FCC to require partner agencies to provide assurances that shared personal data have been securely disposed of at the end of the ISP.

Management response: Partially accepted. This will be covered by version 4 of WASPI.

Implementation date: End of 2013
Responsibility: Democracy & Governance Manager and Heads of Service

c33. The practice in the Community Service Directorate - in posting or faxing ad hoc disclosures of personal data to third parties - is inconsistent with the 'Sending Personal Data to an External Party' policy. The reason for this may be that although this policy steers employees to sending personal data by GCSX, encryption and trackable courier and avoids fax altogether, the 'Policy on Security of Documents Containing Personal Information' does refer to the use of ordinary post, trackable courier and fax.

Recommendation: FCC should clarify which of the two aforementioned policies should be followed in practice.

Management response: Accepted

Implementation date: September 2013
Responsibility: Information Governance Manager and Democracy & Governance Manager