APPENDIX 1

Internal Audit report – Final

Follow Up Audit

ICO Data Protection audit report

Democratic Services

January 2014

Report Ref: LD0220T2

CYNGOR
Sir y Fflint
Flintshire
COUNTY COUNCIL

CONTENTS

SECTION		Page
1	Executive Summary	1
2	Findings	5

Auditors	Flintshire Internal Audit Service
Client sponsor	Democracy and Governance Manager
Distribution	Head of Legal and Democratic Services Data Protection Team

1 EXECUTIVE SUMMARY

1.1 INTRODUCTION

A follow up audit of progress towards implementation of the Information Commissioner's Office's (ICO) Data Protection audit report was undertaken as part of the approved internal audit periodic plan for 2013/14. The ICO audit included three areas of data protection; namely:

A Training Awareness

B Records Management

C Data Sharing.

The ICO audit report was issued as a final version in June 2013. The audit opinion was one of reasonable assurance; the second highest level of assurance. Recommendations made were primarily concerned with enhancing existing processes to facilitate compliance with the Data Protection Act.

Part of the ICO audit process is to request a progress update from organisations where reasonable assurance was given. This is due in January 2014. Findings from this audit will be used in that update to give independent assurance of progress.

1.2 CONCLUSION

Adequate progress has been made towards implementing the recommendations made in the ICO report. The majority of the recommendations which were due for implementation by the end of the year, have either been implemented or are currently being addressed. Some recommendations with dates in the future have also been implemented or progress is being made towards implementation.

1.3 SCOPE OF THE REVIEW

The following areas were reviewed during the audit:

- The recommendations made in ICO data protection audit report.

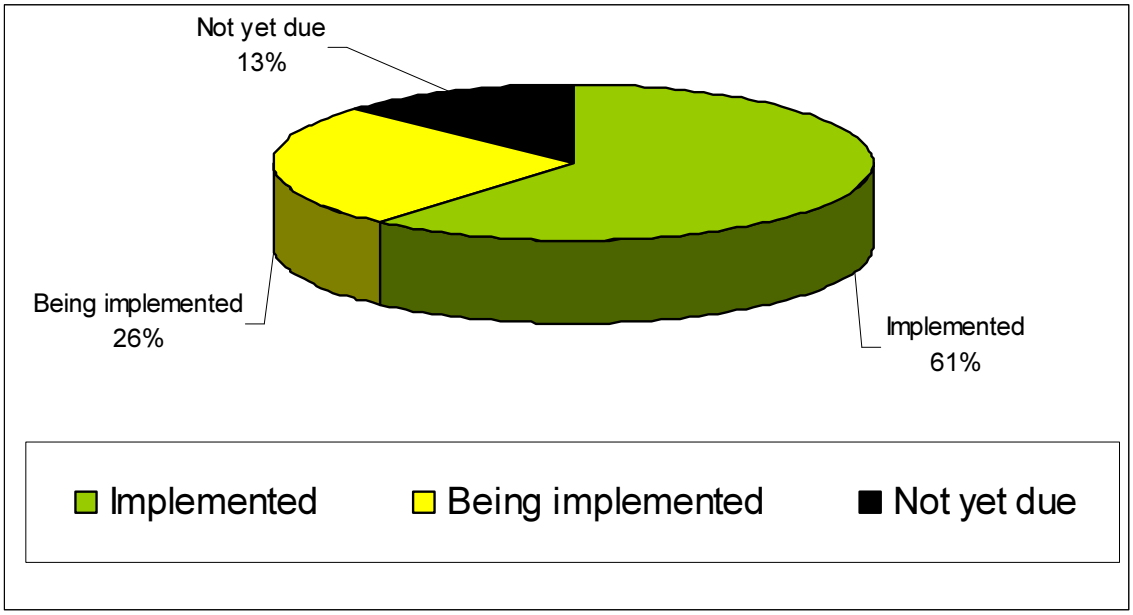
Limitations to the scope of the audit:

- The review is limited to the scope of the ICO recommendations.
- All testing will be undertaken on a sample basis and may therefore not be representative of the full population
- Our review does not provide an absolute guarantee that material error, loss or fraud does not exist.

The approach taken for this audit was a Follow Up Audit.

1.4 RECOMMENDATIONS SUMMARY

The pie chart below provides an overview of the status of recommendations that have been followed up as part of this review.



No further recommendations have been identified as a result of this review.

2 FINDINGS

Each recommendation followed up has been categorised in line with the following:

Status	Detail
1	The entire recommendation has been fully implemented.
2	The recommendation has been partly though not yet fully implemented.
3	The recommendation has not been implemented.
4	The recommendation has been superseded and is no longer applicable.
5	The agreed date for implementing the recommendation has not yet been reached.

	PROCUREMENT FOLLOW UP			FINDINGS	
Ref	Original Recommendation	Original Impl'n Date	Manager Responsible	Status	Comments / Implications / Recommendations
A3	Reports to the Corporate Management Team (CMT) should include training statistics from all Services regarding completion, or otherwise, of required data protection and related training, to provide a corporate overview.	End of 2013	Each Head of Service	2	Since summer 2013 the Heads of Service Performance Reports, which are presented half yearly to Cabinet and the relevant Scrutiny committees, have contained statistics relating to the provision of data protection training. The content of the information is currently varied as not all directorates had by then identified those posts which require data protection training so cannot present it in percentage form. Managers have been requested to identify the posts which require mandatory training and this information is currently being received and collated. During December informal CMT, a deadline to provide this information was set at December 20th 2013. The situation was reviewed during January 2014 and it was found that all this information had been received. Once all posts have been identified it is the intention to hold this information within the ITrent HR system which will include

	PROCUREMENT FOLLOW UP			FINDINGS	
Ref	Original Recommendation	Original Impl'n Date	Manager Responsible	Status	Comments / Implications / Recommendations
					dates of the latest training. This will allow the training reports to be produced corporately. December 2013 Informal CMT also approved a report which stated that "It is the intention that the performance reports would in future contain the percentage of those staff for whom data protection training is mandatory that have received such training". Performance reports are not routinely sent to CMT. The Democracy and Governance Manager has recently contacted the SIRO for his opinion regarding the reporting mechanism to CMT. It has been agreed that performance reports on data protection training are to be made six monthly to CMT.
A9	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.	End of 2013	Democracy and Governance Manager	1	This recommendation was partially accepted. The response stated that Community Services directorate have a greater need for data protection training than other Directorates and it would not be sensible use of resources to have nine additional staff giving training on data protection. The Democracy and Governance Manager wrote to all managers in October requesting the arrangements in place for ensuring their staff have data protection training as and when appropriate. To date not all responses have been received therefore during December the Democracy and Governance Manager wrote to managers explaining their responsibilities and accountabilities with reference to this area as detailed within the Statement of Data Protection Policy and Practice.
A11	FCC should take steps to centrally monitor and coordinate data protection training on an organisation	End of 2013	Democracy and Governance Manager	1	Data protection training is monitored via directorate performance reporting (as discussed in A3 above) issued to Cabinet and the relevant scrutiny committee. Central monitoring of training will be enhanced when all mandatory posts have been added to the ITrent system; this will allow for

	PROCUREMENT FOLLOW UP			FINDINGS	
Ref	Original Recommendation	Original Impl'n Date	Manager Responsible	Status	Comments / Implications / Recommendations
	wide basis.				training requirements to be flagged including refresher training. This information will also be used to obtain the performance data relating to training completed across the organisation. There is a performance indicator for all officers in mandatory posts to be trained by June 2014 as approved by CMT during December 2013. Central co-ordination of training has been achieved by corporately detailing the type of training available including refresher training and when each type of training is applicable.
A12	FCC should develop a corporate data protection training programme to identify and direct strategic and consistent DP training delivery.	End of 2013	Democracy and Governance Manager	1	The Data Protection Team has provided advice regarding the particular training routes available including refresher training. The type of training to be attended is dependant on the level of data processing undertaken by individuals (ie whether the data is sensitive and personal, personal or no processing). This advice will facilitate each directorate to identify the training route applicable for each officer. Training should therefore be consistent and the identification of the roles which require mandatory data protection training should ensure this is achieved.
A21	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.	End of 2013	Heads of Service	2	This recommendation was partially accepted stating that it is Heads of Service responsibility to put in place appropriate arrangements for their service. This has been achieved via the Performance Reports. These reports are submitted to Cabinet and the relevant Scrutiny Committee but are not routinely submitted to CMT. The response states that training statistics will be part of the existing quarterly reporting arrangements to CMT. Performance reports are now produced six monthly, the Democracy and Governance Manager will collate and report them to CMT.
A23	FCC should consider whether	Not accepted		N/A	Data protection training is to be logged via the ITrent system.

	PROCUREMENT FOLLOW UP			FINDINGS	
Ref	Original Recommendation	Original Impl'n Date	Manager Responsible	Status	Comments / Implications / Recommendations
	it is technically possible for the Paris administration team could expand the scope of their prospective new database to cover all data protection and data protection related training across the organisation.				
A24	FCC should introduce Key Performance Indicators (KPIs) in regard to data protection training to proactively monitor and stimulate competency and completion levels.	End of 2013	Democracy and Governance Manager	2	During informal CMT 16.12.13 the KPI that all staff who require mandatory training should have received it by the end of June 2014 was agreed. After that date it was agreed to change the KPI in the performance reports to include the percentage of such staff that have received refresher training and for all such staff to have had refresher training by the end of 2017 at the latest.
A27	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.	End of 2013	Heads of Service and Democracy and Governance Manager	2	This recommendation was partially accepted. It is acknowledged that it is the responsibility of the Heads of Service to ensure that where such training is missed that training is provided at a later date. Training which has been missed should be visible in future within the performance statistics regarding mandatory training as these would not then total 100% by June 2014.
A31	The Information Security Presentation '8 Data Protection Principles' slide should be clarified to indicate that all	1.9.13	Information Governance Manager	1	The slide has been amended and now covers further rights of data subjects i.e rights to: Have inaccurate data rectified, blocked, erased or destroyed

	PROCUREMENT FOLLOW UP			FINDINGS	
Ref	Original Recommendation	Original Impl'n Date	Manager Responsible	Status	Comments / Implications / Recommendations
	rights of the individual under the Data Protection Act (DPA) have a central basis under the sixth data protection principle, although the right to subject access may be foremost amongst these.				Claim compensation To object to processing if: Causes (or likely to) cause damage or distress, Direct marketing; or Automated decisions are made. The revised slide was going to be used in the Information Security session within the corporate induction sessions (which covers data protection) however, this action has not occurred as the corporate induction sessions have recently been amended and now no longer include a stand alone Information Security session. Aspects of information security have been included in the most recent corporate induction within the Corporate Governance session delivered by the Democracy Governance Manager. This session does not however contain the levels of detail previously provided and this slide was not used within this session.
A40	FCC should review the timeframe for refresher data protection training and give serious consideration to an annual cycle.	1.11.13	Heads of Service and Democracy and Governance Manager	1	This recommendation was partially accepted as it was stated that "Statement of Data Protection Policy clearly makes this (refresher training) 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". The timeframe for refresher training has been reviewed, discussed and agreed with the Data Protection Team. The Data Protection Training page on the Council's infonet site includes a "Refresher Training" section. This section details the recommended refresher training intervals as agreed by the Data Protection Team. These intervals depend

	PROCUREMENT FOLLOW UP			FINDINGS	
Ref	Original Recommendation	Original Impl'n Date	Manager Responsible	Status	Comments / Implications / Recommendations
					upon how often officers process sensitive personal information and / or personal information. This information has also been made known via an email to Senior Managers requesting a cascade to all relevant managers.
A42	FCC should extend the provision of periodic and mandatory data protection related refresher training across their whole organisation.	Already in place		1	This recommendation was accepted and it was stated that "The Council's Statement of Data Protection Practice and Policy makes clear that it is already extended across the organisation. The audit visit concentrated on Community Services staff but nevertheless at least one example of other staff was given during the audit visit". The statement states that "Directors and Heads of Service will identify those posts reporting to them for which Data Protection training is mandatory and ensure processes are in place to manage this. This should include maintaining records of all Data Protection training and ensuring regular refresher training, the frequency of which being dependent on the assessed level of risk" (4.2). This statement provides evidence of the extension of provision. Action is being taken to allow all posts requiring mandatory training to be noted in the ITrent system. This will allow the training requirement to be more easily monitored.
A43	FCC should ensure that appropriate members of the Data Protection Team who have not undertaken Information Systems Examination Board (ISEB) training to date do so.	June 2014	Data Protection Team	1	The Records Manager and Information Governance Manager are currently attending an ISEB training course which should be completed in February 2014.

	PROCUREMENT FOLLOW UP			FINDINGS	
Ref	Original Recommendation	Original Impl'n Date	Manager Responsible	Status	Comments / Implications / Recommendations
A46	FCC should introduce the provision of specific data protection training for specialised roles or functions (such as Senior Information Risk Owner (SIRO), Information Asset Owners (IAOs), Subject Access Request (SAR) handlers) as appropriate.	By the end of 2013 for SIRO and within 6 months of their appointments for IAOs	Democracy and Governance Manager	2	Half day SIRO role training has been arranged for February 2014, attempts were made to arrange an earlier date but the National Archives cancelled a December 2013 date arranged with it. This training will also be provided to the Information Governance Manager, Democracy and Governance Manager and Records Manager. A shorter training session relating to the role of the SIRO was provided to members of the Corporate Management Team during December 2013.
A49	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.	1.9.13	Democracy and Governance Manager	1	The Do's and Don'ts poster and the 'DP – what is it' section of the infonet have been amended. The Adult Social Care Policy does not contain this information so therefore does not require amendment. This information is however contained within a Powerpoint slide which was previously used as part of the training provided by adult social care prior to data protection training being delivered corporately. The presentation has been retained by Adult Social Care should it be required for local use and the slide has been updated. We have been advised that this information has not been required locally since at least May 2013.
A50	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.	1.9.13	Democracy and Governance Manager	1	The Individuals' Rights section has been amended to include all data subject rights as per those rights rights within the ICO website.

	PROCUREMENT FOLLOW UP			FINDINGS	
Ref	Original Recommendation	Original Impl'n Date	Manager Responsible	Status	Comments / Implications / Recommendations
A58	FCC should introduce appropriate records management training for members of staff who have specialised records management roles or functions.	June 2014	Records Manager	2	Staff who work in the records management function are currently working towards becoming accredited members of the Information and Records Management Society this includes evidence of experience and covers training. Training modules, which have already been provided to second and third tier managers as part of the asset rationalisation programme, are to be placed on the Infonet for access across the organisation. During 2013/14 it is envisaged that training will be targeted to those members of staff, who whilst not working directly within Records Management, do have records management responsibilities e.g. those specialised roles within Community Services.
B2	Draft Terms of Reference for the DPT to ensure roles and responsibilities, decision making and quorums are clearly defined.	1.9.13	Democracy and Governance Manager	1	The terms of reference have been drafted and approved by the Data Protection Team during their August 2013 meeting.
B5	Appoint and train a senior level Senior Information Risk Owner (SIRO).	End of 2013	Corporate Management Team	1	The Head of Legal and Democratic Services has been appointed as the SIRO. Training is to be provided during February 2014 by the National Archive (see A46 above).
B6	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'.	End of 2013	Records Manager	2	CMT endorsed that it be the responsibility of all Heads of Service to ensure that for their service area they have appointed sufficient information asset owners. Also, in the absence of IAO identification the SIRO will assume that the Head of Service is undertaking this role. This endorsement occurred on 16.12.13. A role specification is to be prepared and circulated. Training is to be provided following the SIRO training in February 2014. Information Asset Owners were only identified and approved

	PROCUREMENT FOLLOW UP			FINDINGS	
Ref	Original Recommendation	Original Impl'n Date	Manager Responsible	Status	Comments / Implications / Recommendations
					as such by the Corporate Management Team during December 2013. The Records Manager has briefly discussed the IAO training with the SIRO and has confirmed that it is due to be developed after the SIRO training in February 2014.
B13	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.	21.5.13	Democracy and Governance Manager	1	A standard procedure has been drafted which states that all policies are to be reviewed by the Data Protection Team with no longer than two years between reviews. A version control has also been agreed and is in use.
B14	Review the Records Management policy to ensure it complies with the recommendations in Part 1, section 7 of the s46 Code of Practice on records management.	End of 2013	Records Manager	1	The Records Manager has confirmed via email that the policy is compliant. It is currently being revised and definition of roles and responsibilities and how compliance is to be monitored is to be considered.
B15	Ensure the Council's website includes a clear Privacy Notice Statement, accessible from the home page.	21.5.13	Democracy and Governance Manager	1	Following the review we were advised the County Council website was updated to include a link to the Privacy Notice Statement from the home page. Subsequently the website underwent radical corporate change which resulted in the Privacy Notice Statement not being directly accessible by a link from the home page. This issue has since been addressed and resolved with IT and the Privacy Notice Statement is now accessible from a link on

	PROCUREMENT FOLLOW UP			FINDINGS	
Ref	Original Recommendation	Original Impl'n Date	Manager Responsible	Status	Comments / Implications / Recommendations
					the home page.
B20	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.	End of 2016	SIRO	5	
B24	Ensure the work to integrate EDM and Paris is continued to enable Social Services to store unstructured data on the corporate EDM.	End of 2014	Information and Governance Manager	5	The Information Governance Manager has confirmed that achievement of the deadline is still on schedule working with the Paris System Admin. Team.
B40	Ensure the procedure on 'Secure Disposal of Storage Media' is completed and distributed to all relevant staff.	End of 2013	Information Governance Manager	1	The procedure was completed during November 2013 and distributed to the relevant member of staff responsible for this area.
B41	Ensure all electronic records, including those in Care.com, can be archived or deleted in line with the Councils retention schedules.	June 2016	Heads of Service and Information Governance Manager	5	The Information Governance Manager has confirmed this work will be carried out in line with recommendation B24.
B43	Investigate if there is a function available with the Council's email application that will apply	1.10.13	Operational Services Manager	1	Investigations were undertaken, however the Operational Services Manager has confirmed that there are no tools or facilities to remove or archive personal information within

	PROCUREMENT FOLLOW UP			FINDINGS	
Ref	Original Recommendation	Original Impl'n Date	Manager Responsible	Status	Comments / Implications / Recommendations
	automatic disposal schedules.				emails. Applying automatic disposal schedules is not practical as there are many retention periods within the retention schedule which would make it difficult to apply automatic disposal schedules as users would have to create folders based on these retention periods. The email policy includes the statement "Avoid keeping personal data for longer than is necessary. Permanently storing personal data within Lotus Notes will breach Principle 5 of the Data Protection Act. Consider exporting the email into your main filing system where the corporate retention schedule can be applied".
B44	Include performance measures or KPIs in the Records Management policy so the effectiveness of the RM function can be measured.	Not accepted, however KPIs will be included in the quarterly performance reports considered by Corporate Management Team. December 2013	Records Manager	2	Following investigation, it was determined that CMT would not regularly receive routine reports of this nature, therefore the management response provided has been revisited. A decision has now been taken to quarterly report KPIs to the Head of Culture and Leisure with any exceptions being escalated to the Director where necessary to ensure the Records Management function is being effectively monitored. Discussions are ongoing regarding including the KPIs in the records management policy and also providing an infonet link to them.
B45	Internal audit should review whether Records Management should be included in the audit plan as part of a three year review cycle.	January 2014	Internal Audit Manager	5	The Internal Audit Manager has confirmed that Records Management will be part of the audit planning process which is due to commence January 2014.
B49	Ensure records and information management risk	June 2014	SIRO and Heads of Service	5	This recommendation will be taken forward following SIRO and Heads of Service training during early 2014.

	PROCUREMENT FOLLOW UP			FINDINGS	
Ref	Original Recommendation	Original Impl'n Date	Manager Responsible	Status	Comments / Implications / Recommendations
	is incorporated into service level plans so potential threats can be identified at an early stage.				
B53	The Council should consider conducting Privacy Impact Assessments (PIA) 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.	End of 2013	SIRO and Data Protection Team	2	This recommendation was partially accepted. The response stated that PIA assessments will be considered for appropriate projects but not all due to resource implications. PIA assessments have been previously completed by the Information Governance Manager and Records Manager. There is currently no mechanism in place for those responsible for this recommendation to initially identify projects and then assess them for appropriateness. This issue has been discussed with the Democracy and Governance Manager. It has been resolved that this recommendation will be addressed following SIRO training in February 2014, as this training may provide further guidance within the area of Privacy Impact Assessments.
C5	FCC should develop and introduce specific data sharing training for operational staff who have responsibility for systematic data sharing.	End of 2013	Democracy and Governance Manager	1	This recommendation was partially accepted. The response stated that "guidance will be produced, including who should be contacted with queries. Data sharing is best covered as part of the corporate training". A guidance note "Regular Sharing of Personal Information" has been produced and has been published on the infonet. The guidance includes managerial responsibility in this area, the fact that staff involved in routine data sharing need to have been provided with access to the relevant Information Sharing Protocol and the importance of compliance with this protocol. The guidance also states that if they require advice this should be sought from a member of the Data Protection Team. Training has been provided within the two hour "Data

	PROCUREMENT FOLLOW UP			FINDINGS	
Ref	Original Recommendation	Original Impl'n Date	Manager Responsible	Status	Comments / Implications / Recommendations
					Protection for Community Services" workshop delivered via the Workforce Development Team within Community Services. This training has been provided twenty times since March 2013 and is part of a rolling training programme. For other directorates training is provided via Act Now courses and the Democracy and Governance Manager's Lunch and Learn sessions.
C8	FCC should develop and introduce formal training and documented procedures specifically in regard to one off disclosures and these should ensure appropriate sign off.	End of 2013	Democracy and Governance Manager	1	This recommendation was partially accepted stating that further guidance will be produced and that it is best covered in corporate training arrangements. It was noted in the management response that "there is no need for routine senior authorisation or sign off if staff are appropriately trained". Documented procedures have been produced and have been uploaded to the infonet. Training has been provided within the two hour "Data Protection for Community Services" workshop delivered via the Workforce Development Team within Community Services. This training has been provided twenty times since March 2013 and is part of a rolling training programme. For other directorates training is provided via Act Now courses and the Democracy and Governance Manager.
C13	FCC should ensure that there is a uniform mechanism for quality assessment of fair processing information across the organisation.	September 2013	Democracy and Governance Manager	1	Guidance relating to fair processing notices has been placed on the infonet following agreement by the Data Protection Team. The guidance provides two options for fair processing notices dependant on whether the information includes sensitive personal data or personal data only. The guidance was emailed to senior managers with a request to cascade to all relevant managers during October 2013.

	PROCUREMENT FOLLOW UP			FINDINGS	
Ref	Original Recommendation	Original Impl'n Date	Manager Responsible	Status	Comments / Implications / Recommendations
C14	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.	September 2013	Democracy and Governance Manager	1	Guidance has been issued and placed on the infonet detailing the information fair processing notices should contain ie: That it is Flintshire County Council obtaining the personal information; Why there is a need to collect it What it is going to be used for Whether the information is going to be shared with other Council departments or external organisations. This information was emailed to senior managers with a request to cascade to all staff during October 2013.
C21	FCC should put all Information Sharing Protocols (ISPs) in a single place on Electronic Document Management (EDM) to enable central oversight.	June 2013	Information Governance Manager	2	A spreadsheet is maintained of all ISPs throughout the County Council and a shared folder has been placed on the Y Drive to store all ISPs. To date two ISPs have been placed within the folder. During the December Data Protection Team meeting a request was made for all members to place the remaining ISPs into the shared folder on the Y Drive.
C26	FCC to require partner agencies to provide assurances that shared personal data has been securely disposed of at the end of the ISP.	End of 2013	Democracy and Governance Manager and Heads of Service	1	This recommendation was partially accepted. The management response stated that it will be covered in the Wales Accord on the Sharing of Personal Information (WASPI) V4. WASPI V4 13.2 states that "All information, whether held on paper or in electronic format must be stored and disposed of in line with each partner organisation's retention and disposal schedule". FCC is a signatory to WASPI and is therefore bound to comply with all clauses. It was also noted that it would not always be applicable to dispose of the personal data at the end of ISP as there may be legal requirements to hold data for

	PROCUREMENT FOLLOW UP			FINDINGS	
Ref	Original Recommendation	Original Impl'n Date	Manager Responsible	Status	Comments / Implications / Recommendations
					longer (e.g. in the case of adoption data).
C33	FCC should clarify which of the two aforementioned policies should be followed in practice.	September 2013	Information Governance Manager and Democracy and Governance Manager	1	This recommendation refers to the use of fax / post and the fact that the "Sending Personal Data to an External Party" policy does not include the use of fax, whereas the "Policy on Security of Documents Containing Personal Information" does refer to the use of post and fax. Following the review the "Sending Personal Data to an External Party" policy has been amended to state that risk assessments should be completed when a form of communication method is used which is not Government Connect Secure Extranet (GCSX), secure connections or CD/DVD. The risk assessment procedure is detailed within the "Policy on Security of Documents Containing Personal Information". This information was disseminated to team managers within children's services and youth justice service. Eight managers were contacted to ascertain if they had cascaded the information throughout their team and were also asked if the use of fax had reduced since the memo had been provided. Three managers replied confirming that the information had been cascaded and the use of fax was, if used at all, only used on rare occasions.