Agenda Item No. 7

Audit Committee – 20th November 2017

Information Commissioner Office (ICO) – Data Protection Audit (DPA)

1. Summary of report

1.1. This report provides a status update on the ICO Data Protection Audit recommendations as at the end of October 2017. It looks at progress towards completion of 49 recommendations and 1 overarching action made by the ICO following the recent audit and against the phased completion dates. The areas considered were Records Management, Data Sharing and Subject Access Requests (SARs).

1.2. The report also outlines the project team's plan to ensure any outstanding recommendations are met within the 12 month period agreed with the ICO.

2. Recommendations

That Audit Committee

2.1. Note the progress on the recommendations from the ICO Audit
2.2. That on Monday 6th November the ICO confirmed that that their engagement with the Council in relation to the Audit is now closed.
2.3. Note the ongoing risks related to performance in Subject Access Requests and associated plans to address.

3. Background

3.1. The Council is required to provide a detailed update to the ICO on progress following the Consensual Data Protection carried out in November 2016. The ICO issued 49 recommendations for completion with an additional action that requires the Information Governance Policy Framework to be updated following completion of all the tasks. The ICO now require an update on the progress that has been made over the last 8 months. A 3 month update was provided to Audit Committee on 24th June 2017.

3.2. The report to the ICO was submitted on 3rd November and they carried out a desk review on 6th November. As the update provided assurances that all recommendations met, were underpinned by robust evidence, they did not request any further information.

4. Report Detail

4.1. The Council planned that 46 of the 49 recommendations would be met by the end of October and Appendix 1 shows that 46 are now complete. It also contains details of the status and planned activity over the next 2 months to complete the remaining 3. All recommendations are due to be completed by December 2017, The additional action relating to the update of the overarching Policy Framework will be complete following re-submission to Cabinet in February 2018.

4.2. Completing the recommendations has provided the Council with the opportunity to further strengthen and embed it's Information Governance arrangements. This has been done through updating policies, procedures and processes, in the audit areas: Records Management, Handling of Subject Access Requests and Data Sharing, as well as reviewing the training and induction content.

4.3 In addition, particular progress has been made in the following areas:

- The Forum for Information Governance Assurance Group (FIGA) now meets more frequently, every two months, with additional monthly meetings for Information Champions currently focusing on preparing for the implementation of the General Data Protection Regulations.
- Records Management file audits are taking place across the Council, using a newly developed audit tool which works to identify areas of good and practice and areas of risk or which require improvement.
- The induction process had been reviewed to ensure that it promotes the Information Governance Policy Framework at all access points into the Council.
- The Information Governance Team has also developed an improved integrated information asset management system. This now enables us to better asses the risk to information assets with personal information, map data flows for assets that are shared, and maintain a central log of data sharing agreements. These tools are all connected to the information asset register.

4.4 Following the outcome of the audit, priority was given to completing the recommendations that relate to improving performance in the handling of Subject Access Requests and these have now been completed. However the level of compliance against the statutory timescale for responding to these requests has declined since the audit from 63% within timescale to 42% within timescale. This represents a risk to the Council as the ICO had previously assessed this area as achieving Limited Assurance. The response to the ICO will therefore include a details explanation of why there has been a drop in performance along with an indication of how the Council is seeking to address this.

4.5 On 6th November the ICO provided a considered response to the Council noting the significant progress and that in total there were 4 recommendations / actions still outstanding. The ICO advised that whilst they were happy to consider the Audit closed they considered that one of the actions relating to Quality Assurance of SARs was not yet complete as it required a more formal approach.

4.6 The ICO also noted that whilst these 5 recommendations/ actions remain outstanding this represents a continued residual risk to the Council of non-compliance with the Data Protection Act 1998'

5. Performance Management & Risk

5.1. Despite the appointment of 2 staff in December 2016, the Assurance Service continued to experience a fall in the compliance rate for SAR responses. However 1 of these appointees left the organisation after only 6 months in post.

5.2. In July 2017 a further 2 temporary resources were appointed for 6 months to focus solely on the processing of subject access requests. However, these individuals required an initial induction period and in line with ICO requirements their work needed to be fully quality assured. This quality assurance of cases detracted experienced handlers from progressing their own caseload which has also impacted on compliance rates.

5.3. The additional resource has had to focus on both historic cases and incoming cases. This has meant there has been an overall reduction in the number of open cases between end of May 2017 and end of October 2017 from 50 to 23, a 46% reduction. The need to work on all open cases was driven by customer demand and the need to respond to customers who had already been waiting for their information for some considerable time. As at the end of October 2017 of the 23 open cases 9 (39%) are within the statutory 40 days, 13 (57%) are outside of statutory timescales (overdue) and 1 (4%) is on hold. It is anticipated this position will continue to improve.

5.4. There are early indications that the volume of cases being closed each month has risen considerably over the last 3 months with 54 cases being closed between August and October 2017. The flow of new requests being received remains fairly steady (32 requests received between August and October 2017). The service has now reached a point where quality assurance of cases is being better managed.

5.5.The ongoing management of performance in the handling of SARs has led to detailed monitoring reports being presented to FIGA and, in line with ICO recommendations, reported through to CMT. Whilst rates of compliance are still lower than acceptable the challenges the service have faced in terms of loss of resource and varying levels of skills and experience within the team have enabled a more in-depth review of processes, procedures and performance data which will support permanent improvements in service delivery. Performance data for the last 2 quarters shows an improvement in compliance of 9 percentage points and the service manager is confident this will continue. Compliance with statutory timelines for requests due out in October 2017 was 70%. However the rate of compliance over a rolling 12 months of cases will remain low for some time to come and represents a significant risk as is lower than would be tolerated by the ICO. It also represents a service to customers that is below acceptable standards.

6. Resource Implications

6.1. Given the current performance CMT has supported funding for the recruitment of an additional 2 permanent assurance officer posts and 1 assistant assurance officer post has been approved. This will provide long-term, permanent stability for the Assurance team. This additional resource will focus on SARs and will bring the council's headcount in this area more in-line with neighboring authorities.

7. Citizen Impact

7.1. Subject access requests are submitted by the public who request this information for personal use. The impact on customers is likely to continue for a period of time. All customers have recourse to an internal appeal process and or to the ICO directly.

8. Equality Implications

8.1 There are no direct equality implications arising from this report

9. Consultation

9.1 None

10. Next Steps

10.1 The project team will now focus on completing the remaining 3 actions and work with directorates to embed learning form the Audit into business as usual.

10.2 The timely completion of the action plan will assist the Council to:

- reduce and or mitigate risks to personal data from Data breaches
- implement measures to support improved handling of subject access requests
- improve overall compliance with the Data Protection Act and
- assist with preparation for the General Data Protection Regulations (replacement for Data Protection Act)

10.3 The implementation of the training plan is expected to take a number of months but is expected to significantly improve efficiency and efficacy within the team towards improved performance. The ICO will be appraised of progress as appropriate.

11. Background Papers

ICO Data Protection Audit – Action Plan – 8 month update

James T. Walsh, Chief Finance Officer

Contacts

Nailah Ukaidi - Information Governance & Assurance Manager
☎ 650970 Nailah.ukaidi@walsall.gov.uk
Helen Dudson – Corporate Assurance Manager
☎ 653732 Helen.dudson@walsall.gov.uk

Appendix I - ICO Data Protection Audit Action Plan 8 Month Update

Purple	Completed
Blue	Not started- not yet scheduled to start
Green	Task Started (on track, no delays expected)
Amber	Task started (minor delays but expected to get back on track
Red	Task started (significant risk of missing target date)
Grey	Not started- Due to have started

Recommendation	Agreed action, owner and date	Status Month 8	Progress Month 8
Records Management			
a4. (a) Records management issues should be a standing agenda item on the FIGA agenda. **(b)** FIGA should consider meeting more regularly, in order to cover the wide ranging scope and objectives that are listed within the Information Governance Policy Framework.	**Accept-** Item added as of January 2017 and agreed to add additional dates added to schedule for 2017 and furthermore. **Implementation date:** 31/03/2017 **Responsibility:** Carol Williams.	🟪	(a) Records management is now a standing agenda item at FIGA. See Item 5 of Standard Agenda. Additionally a new Records Management Post has been created. (b) The Council has increased the frequency of FIGA meetings. There were 7 FIGA meetings scheduled for 2017 this is roughly 1 every 2 months. There have been no cancellations to date. This will be the frequency going forward. 2017 January 16th March 7th April 18th June 27th July 18th September 13th November 23rd
a6. Consider re-introducing a formal work plan to record risks identified and discussed at FIGA meetings which lists the date, action, description of action taken, updates, result, owner and completion date.	**Accept-** Action plan template re-introduced as of Jan 2017. **Implementation date:** 31 January 2017. **Responsibility:** Carol Williams.	🟪	The formal work plan for FIGA is now used at every FIGA and records the following: Ref No. Date of Meeting Owner Description of action Specific action required Purpose Target date Reminders to check it are sent out with FIGA minutes after each meeting. Access to the log has been given to FIGA members
a21. Conduct a review of records stored in team cabinets to check that operational teams are implementing adequate logging and tracking mechanisms to locate and retrieve physical records.	**Partially accept-** IAOs, IACs and ICs will be supported by IAT and IAGM to conduct periodic sample reviews using agreed measures. **Implementation date:** 31/08/2017 **Responsibility:** Nailah Ukaidi and Helen Dudson.	🟪	The Council has produced a Records Management Audit tool for use by IAOs and Information Champions to set out arrangements for a regular programme of records management audits to demonstrate and provide assurance of compliance with good practice and records management standards. Initial audits took place in October 2017 for manual records. The Audit tool encourages follow-up action for areas of non compliance, with ongoing reviews by IGAM and Information Champions.
a23. The Information Assurance Team should conduct audit checks on the access of Iron Mountain Connect every 3 months instead of annually. All leavers or staff who no longer require access should have their rights revoked.	**Partially accept-** IAOs will be supported by IAT to conduct audit checks on a more regular basis to ensure that leavers and staff who no longer have a need to access IM do have their rights revoked and good records management processes are in place. **Implementation date:** 30 September 2017. **Responsibility:** Nailah Ukaidi and Helen Dudson.	🟪	Access to Iron Mountain is predominately delivered via business support within Children Services. A process for a quarterly review of accounts has been developed and will be adopted as other users of IM are established. The quarterly directorate Quality Assurance of Iron Mountain accounts will be supported by the Corporate Assurance Team completing an annual review of all accounts and reported to the Records Manager Now working with HR to amend the corporate leavers form to include a prompt to ensure Iron Mountain accounts are closed.
a27. (a) Ensure that the documented Business Continuity Plan requires that the plan will be tested on an annual basis. **(b)** Ensure that the Corporate Business Continuity Plan is approved at senior management level. **(C)** The review log for the Corporate Business Continuity Plan needs to be kept up to date with the date it was last reviewed, its issue date and the date of its next review.	**Partially accept-(a)** The ICT Service will test its ICT Disaster Recovery Plan, as a minimum, on an annual basis with a prioritised methodology for annual reviews of specific scenarios. **(b)** This will be taken to the Chief Executive to seek formal approval at the Corporate Management Team on an annual basis for approval to the strategy. **(c)** The review log metadata table will be detailed on the cover page in line with the council's corporate document format. **Implementation date:** 31 October 2017. **Responsibility:** Steve Pretty.	🟪	The evidence attached shows the testing schedule for 2017 and confirms that testing will be carried out on an annual basis, prioritising areas appropriately Two examples of the 2017 test results are included; Website and Switchover to Tamworth The Head of Service for Planning, Engineering and Transportation has confirmed that the BCP will go to the November CMT for approval. Metadata table added to the document to include the following (Author, Version Date, Version number, Next review date and authorised by). The next review date reflects the annual review
a28. Ensure that the Information Security Policy covers all areas of information security, including network access and the use of WC's devices, as planned.	**Partially accept-** Work required: initial benchmarking exercise, followed by recommendation on what policies will be put in place which will need to be approved. Then policies drawn up and approved. **Implementation date:** 15/12/2017 **Responsibility:** Carol Williams.	🟩	A gap analysis is currently being created in regards to ISO 27001. Once the gap analysis has been completed required policies will be drafted, approved and published. Revised ISP with key elements cyber essentials and alignment 27002, GDPR , Privacy by Default
a29. Promote the protective marking scheme guidance in the Information Risk and Security Policy to all staff as appropriate.	**Accept-** Scheme and procedure will be rolled out to all staff, as appropriate, using Meta compliance tool. **Implementation date:** 30 June 2017. **Responsibility:** Nailah Ukaidi.	🟪	Despite the delays in implementing METACOMPLIANCE the council has still promoted the use of the Protective Marking Scheme. The Council is exploring the use of various solutions to increase the efficiency of how we work particularly around document management, this includes Office 365 and SharePoint. The ability to facilitate Protective Marking will be part of those discussions. To date the project team has promoted the scheme through: -The mandatory IG training - Responsible For Information -Promotion on the IG Intranet Page -Through FIGA - On Agenda for November 2017 Information Champions meeting See A59 for progress on Metacompliance

Recommendation	Agreed action, owner and date	Status Month 8	Progress Month 8
a40. Amend the Mosaic new access form to include changes to access and removal of access, for consistency of approach.	**Accept-** Review form and update. **Implementation date:** 31 March 2017. **Responsibility:** Lisa Harris.	🟪	There is a single multipurpose form for granting access to and removal from MOSAIC for Council staff.
a58. Recommendation: Any amendments from the review of the IG policy framework during December 2016 should be implemented, as appropriate.	**Accept-** Update the policy in line with the IG documentation review cycle taking into account any recommendations from the audit. **Implementation date:** 31 December 2017. **Responsibility:** Nailah Ukaidi.	🟩	The policy was updated as part of the annual review in December 2016. Further updates were made in February and July 2017 to account for the recommendations that were completed at that point. E.g. reference to the Data Quality Procedure. Whilst the document should be reviewed 12 months from its last review date i.e. August 2018. The document review date will be brought forward to March 2018 at which time all of the audit recommendations will have been completed and then the Framework Policy can be approved via Cabinet
a59. Continue with plans to utilise the policy compliance software so that WC has assurance that staff are accessing IG policies, procedures and guidance.	**Accept-** Currently conducting testing process. If successful, rollout will be extended to all machines. Agree administration structure and policy rollout priority. Communications in internal bulletins leading up to full implementation. **Implementation date:** 31/03/2018 **Responsibility:** Nailah Ukaidi.	🟧	The Metacompliance project is progressing and now at UAT and implementation phase. Testing is being carried out in stages to ensure issues are picked up before final roll out The implementation date has been revised to end of December 2017 due to some resource issues. To address this a mandate has been submitted to the ICT Governance Board to identify appropriate resource to assist with additional testing and the rollout of the client software. This mandate is scheduled to go to the Board on 22nd November.
a61. Recommendation: **(a)** Ensure all services are properly identify and document their departmental information risks. **(b)** Formal assurance of how risks are mitigated should be reported to the SIRO, for example sending them a copy of the risk register.	**Partially accept- (a)** Ensure that all directorates risk assess all their information assets, using an appropriate tool. **(b)** Document and embed the process and criteria for escalating risks and providing assurance to SIRO **Implementation date:** 30/09/2017 **Responsibility:** Nailah Ukaidi.	🟪	The risk assurance process now includes reporting to the SIRO where assets have a risk score of 15 or more. This was discussed at the June FIGA (Slide 11) and also documented in the risk assessment tool (see Guidance tab). Each directorate has completed a Risk Assessment Tool for assets with PID
a62. Promote awareness amongst staff of privacy impact assessments and the occasions when they need to be completed.	**Partially accept-** Use internal communication methods and ICT channels to continue to promote current PIA use alongside developments for introduction of GDPR. **Implementation date**: 31 October 2017. **Responsibility:** Nailah Ukaidi.	🟪	The IG homepage Intranet page is used to draw attention to new items. This is announced via the Intranet New pages. It also included a new PIA and privacy by design page. Information champions meeting-see slide 5 re: privacy impact assessments/ privacy by design. An independent IG Training Consltancy - Dylis Jones Associcates see slide 29 for details Advanced information security workshop screen shot of inside Walsall promoting Privacy impact assessments.
a66. Amend the clause in the contract referring to transfer of data under Safe Harbour to reflect the EU compliant model clauses now in use.	**Partially accept-** The Council will work with Iron Mountain to ensure that the contract is updated to reflect the measures that are in place. **Implementation date:** 28/08/2017 **Responsibility:** Carol Williams.	🟪	A contract variation has been issued and signed by both parties. It replaces clause 13.2.1 to include adoption of the model contractual clauses approved by the ICO and European Commission

Recommendation	Agreed action, owner and date	Status Month 8	Progress Month 8
Subject Access Requests			
b2. Review the Subject access request webpage to ensure it is appropriately tailored to the public and remove any duplication or incorrect information.	**Accept-** Review and update was completed shortly after audit. **Implementation Date:** 28 February 2017. **Responsibility:** Nailah Ukaidi.	🟪	The Subject Access Request webpage has been reviewed and updated to ensure it is appropriately tailored to the public. Incorrect/duplicate information has been removed - See the following *SARs page *Privacy Notices page
b3. Consider putting the subject access request form from the access to personal records leaflet into a separate link on WC's subject access request webpage.	**Accept-** Text has been added to website to indicate that leaflet contains form to be completed and copy of form will be placed on website separately if it can be extracted from leaflet. **Implementation date:** 28/02/2017 **Responsibility:** Carol Williams	🟪	The access to personal records leaflet has a link to subject access request form. See link to website to view updated page with link to form from leaflet as recommended
b4. Provide a link to the subject access request webpage from the privacy notices page located in the footer of the WC's website homepage.	**Accept-** key word search criteria will be updated via ICT service. Link has been added. **Implementation date:** 28 February 2017. **Responsibility:** Carol Williams.	🟪	A link to access SAR page is available on privacy notices page as recommended. Please see link to webpage "Access to my personal records"
b7. Recruit two Assurance Officers, to support the full resourcing of the Assurance Team, as planned.	**Accept-** 2 posts were filled Dec 2016. **Implementation date:** 31 January 2017. **Responsibility:** Carol Williams.	🟪	As part of the ongoing process to ensure that the Assurance Team is adequately resourced, two members of staff were appointed to the permanent role of Assurance Officer - SO and LA
b9. Review the subject access data processing arrangement with SCC as planned. If WC decides to continue their relationship with SCC, the data processing contract will need to be reviewed on an annual basis.	**Accept-** Review contract in line with GDPR requirements. Ensure this is on the IG document review cycle for annual review. **Implementation date:** 31/07/2017 **Responsibility:** Carol Williams.	🟪	As part of the review with SCC, they explained that they had reductions in their capacity and were no longer able to take additional work from other local authorities. This meant that the contract has naturally lapsed. Should circumstances change a new contract will be drafted to ensure it is compliant including factors relating to GDPR. As this additional capacity was no longer available, 2 temporary posts of Assurance Officer were funded since June 2017 to assist in the processing of subject access requests.
b10. Ensure staff are required to read the information governance policy framework through the induction process.	**Accept-** Induction process to be updated at all access points and policy rolled out through Policy Enforcement Tool. **Implementation date:** 30 June 2017. **Responsibility:** Carol Williams.	🟪	The Council is updating it's wider induction process. A new induction pack is being produced by HR . Managers across the Council will use this to introduce new employees to the workplace. The pack will include details of Council Policies and Procedures with general guidance including on Information Governance, with specific reference to the IGPF document and the link where to find it. HR will have the New Starter Pack ready for use in January 2018. 1. All line managers of new starters will continue to receive an email from the recruitment team confirming details e.g. name and start date 2. From 1st October 2017 the email will include the following paragraph: Information Governance All managers must ensure every new starter is aware of their responsibilities for Information Governance. Managers must either provide each new starter with a hard copy of the Information Governance Policy Framework document or provide them with the link to the document on the intranet pages at http://inside.walsall.gov.uk/walsall_ig_policy_framework_2017_v_2.3.pdf and seek assurances that it has been read and understood. The Policy Framework is also now Part of the mandatory RFI training which is undertaken by new starters and current staff. It is part of the resources. Staff who attend the face to face induction will also be made aware of the need to read the document (See page 6 of the slides)
b12. Consider adding more case scenarios for the subject access request handbook which relate to local government handling of subject access requests.	**Accept-** IGAM will consider as part of review process. **Implementation date:** 30 June 2017. **Responsibility:** Nailah Ukaidi.	🟪	More case scenarios for the subject access requests have been added to the Handbook. Examples have been modified so that they relate to council business and are more relevant. Note pages 16 and 17 are now Council examples as opposed to the previous version which related to online retail
b14. (a) Add subject access content to the e-learning module that all staff are required to complete **(b)** Staff should complete the e-learning module annually, as planned.	**Accept-** IGAM will update content as part of yearly review and relaunch. Annual refresh agreed at FIGA and CMT. **Implementation date:** 30 March 2017. **Responsibility:** Carol Williams.	🟪	Subject Access content has been added to the annual mandatory Responsible For Information e-learning module. See screen shot of new content on e-learning e-learning: level 1 section 2 page 10, level 2 section 1 page 21. paper version: level 1 paper version page 33 level 2 paper version page 28
b17. Design and document a subject access training plan for Lead Assurance Officers and Assurance Officers, including timescales by which different stages of training will be completed.	**Accept- (a)** Build a log of case scenarios that can be added to and adapted to ensure some consistency in learning. **(b)** Quarterly case review meetings to highlight and discuss recent cases that have been complex or challenging so learning shared across the team. **(c)** In addition to desk side support and training for new staff formal training will also be sought either as a training course or webinar similar in context to the one all staff have received. **Implementation date:** 31/08/2017 **Responsibility:** Carol Williams.	🟪	A clear training plan has been developed for SARs Handlers to ensure that they reach the required standard and their knowledge and skills are refreshed periodically. A SARs training template has been developed to enable each officer to self assess their knowledge and understanding of both the data protection act and the processing of subject access requests. This is based on the SAR handling handbook all officers use and also records other types of training received (e.g. webinars). Once individuals complete the self assessment a senior officer also completes an evaluation and the discussion that follows enables future activity to focus on specific areas that need further development. In addition once a quarter, the 'Respond' meetings include a discussion regarding learning from cases to assist the development of case scenarios. A SAR surgery is held once a week by the lead assurance officer (most experienced SARs handler) to enable focussed desk side support with live cases and additional resources have recently been allocated to provide more desk side support which will be key when new posts are recruited to

Recommendation	Agreed action, owner and date	Status Month 8	Progress Month 8
b18. Complete further SAR training for the Assurance Team in order to improve SAR compliance rates as soon as possible	**Accept** **Implementation date:** 18/08/2017 **Responsibility:** Carol Williams.	🟪	The training regime described in b17 has commenced in earnest with all handlers now having undergone some form of training, principally the development and use of the individual training log ,the provision of desk side support and ongoing development of case scenarios. Whilst compliance rates have now started to improve, having less experienced officers has meant more training and quality assurance of cases has been required and has impacted on our ability to improve this as quickly as anticipated.
b21. Recommendation: Amend the flow chart to explain when to include a third party who has made a request on behalf of the data subject.	**Accept-** Amend flowchart / SAR Handbook and disseminate to IAT. **Implementation date:** 31 May 2017. **Responsibility:** Carol Williams.	🟪	The flowchart has been amended (version 1.3) to explain when to include a third party who has made a request on behalf of a data subject (P45 of the handbook). The Handbook is owned by the the Information Assurance Team (Individuals Rights) and each SAR handles has access to a hardcopy which they use on a regular basis.
b22. Carry out a review of all template letters in Respond and remove any letters which are no longer relevant.	**Accept-** review and update as per recommendation. **Implementation date:** 31 May 2017. **Responsibility:** Carol Williams.	🟪	All templates have been reviewed and those no longer in use deleted.
b26. Subject access request documentation should be reviewed by the Assurance Team at the earliest opportunity to determine whether a letter needs to be sent to the data subject advising of a potential delay. If appropriate, offer to provide the information in batches and where possible a date for the final batch. This should be documented in the subject access flow chart for staff.	**Accept-** review and update documents and IAT staff as per recommendation. **Implementation date:** 31 May 2017. **Responsibility:** Carol Williams.	🟪	A template has been developed for an update to be provided to requesters at 20 days and a task has been set in the case management system (Respond) to remind officers of the need to update requesters earlier in the process. The flowchart has been amended to include "Consider if response is likely to be delayed. If so, contact requestor promptly. Consider providing in batches. Try to agree final date for completion" - P46 of the handbook
b29. Remind the Assurance Team that they should be specifying a deadline for SAR enquiries in the Memo to service areas.	**Accept-** Action as per recommendation. **Implementation date:** 28 February 2017. **Responsibility:** Carol Williams.	🟪	Memo to services has been updated to include the dates responses are required by. See text highlighted in yellow "I would be grateful if you would provide us with the information requested, by [GUIDANCE NOTE – this will be 10 calendar days and will be automated by Respond – please double check the date generated before sending this memo to services] ...."
b32. Children's Services should formally document the process for dealing with subject access requests from the Assurance Team. Consider adapting the Adults Services flow chart as a template.	**Accept-** Action as per recommendation. **Implementation date:** 28 February 2017. **Responsibility:** Lisa Harris.	🟪	Adults services have a SARs handling flow chart. This has been modified and is now used by relevant staff from other directorates
b40. Regular quality assurance should be undertaken on subject access responses. It may be more beneficial to complete this on live cases, as a preventative measure. Whether quality assurance is undertaken on live or closed subject access request cases, 'lessons learned' can be fed back to the member of staff responsible for the case and then to the Assurance Team for general guidance.	**Accept-** Links to the quarterly review meeting referenced previously. Agenda to be built to develop opportunity to spotlight specific cases. Monthly Respond meeting to include QA element of SAR process of all live cases and provide opportunity to review / discuss issues. **Implementation date:** 30 September 2017. **Responsibility:** Carol Williams.	🟪	Additional quality assurance is conducted as a way of supporting and training less experienced staff as they work through cases as well as when they have completed a case. The weekly SAR surgery is one way the additional 'live' case QA and discussion can happen as the time is sometimes used to feedback to officers on sections of files they have reviewed and marked for redaction.
b41. Document further examples of how exemptions can be applied to SAR's in the subject access request handbook.	**Accept-** IGAM will update content of SAR handbook. **Implementation date:** 31 March 2017. **Responsibility:** Carol Williams.	🟪	The Handbook has been updated to include further examples of how exemptions can be applied to SAR's in the subject access request handbook. See section on exemptions on P32
b42. (a) Review the supplying information template to ensure it includes the requirement to explain all exemptions used and redactions that have been applied (where possible). **(b)** The Assurance Team should be reminded to explain why information has been withheld rather than just highlighting which exemption or part of the DPA has been applied to the subject access request bundle.	**Accept- (a)** update document as per recommendation. **(b)** As per recommendation and compliance to be picked up in monthly and quarterly meeting. **Implementation date:** 31/08/2017. **Responsibility:** Carol Williams.	🟪	The supplying information (response) template has been updated to include the need to explain all exemptions. Extract includes [GUIDANCE NOTE – the categories below are those most frequently used but is not an exhaustive list. Delete those not appropriate and if necessary add the reason for some information being removed]
b43. Information about the searches which have been carried out to locate the information within WC should be included in the 'supply information' template and specified in the covering letter included in the subject access request bundle.	**Accept-** Action as per recommendation. **Implementation date:** 30/09/2017 **Responsibility:** Carol Williams.	🟪	Information about the searches which have been carried out to locate the information within WC are now included in the 'supply information' template and specified in the covering letter included in the subject access request bundle. Extract includes During the search for your information, Walsall Councils [enter service name/s] service/s were approached and a thorough interrogation of their systems and archived files was conducted.

Recommendation	Agreed action, owner and date	Status Month 8	Progress Month 8
b44. Provide specific guidance on the various procedures by which subject access request bundles can be supplied to data subjects.	**Accept-** IGAM will update content of SAR handbook. **Implementation date:** 31 May 2017. **Responsibility:** Carol Williams.	🟪	The updated SARs Handbook details specific guidance on the various ways by which data subjects can receive their bundles (See section 8 of Handbook Supplying Information to the Requester) "Form in which the information must be supplied Once you have located and retrieved the personal data that is relevant to the request, you must communicate it to the requester in intelligible form. In most cases, this information must be communicated to the requester by supplying him or her with a copy of it in permanent form. You may comply with this requirement by supplying a photocopy or print-out of the relevant information." How to provide the information Staff must ensure that information is provided to data subjects in a secure and customer friendly format. The Council's preferred format is electronic. The following steps must be followed when responding to a SAR. 1. Check with the Data Subject that they are willing to accept an electronic copy of their information via an encrypted (password protected) disk. 2. Copy the information to a disk using the Adobe Pro tool ensuring that the file has been properly redacted and 'secured' with a password. The file should also be marked as 'SAR COPY'. 3. Ensure that a copy of this file and the password are stored on the Council system for recording SARs 4. After confirming the correct postal address, provide the disk to the requestor by post or email. 5. Provide the password using a different delivery method, than that used for the disk. By telephone or email as appropriate. 6. Where the requestor asks for a paper copy, if the requestor is not able to collect, the file may be posted using the secure 'Special Delivery' post bags provided by Royal Mail. All fields on the post bag must be completed and the bag sealed properly. 7. When the file is sent using 'Special Delivery' checks should be made to ensure the file has been received by the requestor (usually within 48 hours) 8. Consideration should always be given to meeting specific needs of requestors including facilitating viewing of files on council premises.
b47. A terms of reference should be created for 'Camelot meetings' and minutes of the meeting should also be recorded.	**Accept** **Implementation date:** 28 February 2017. **Responsibility:** Carol Williams.	🟪	Camelot is the name of the Assurance Leads Meeting. The ToR have been updated and meetings are now more formal. They include monthly review of performance information on SAR. Minutes are also produced for these meetings
b48. Subject access compliance should be a standing agenda item for the FIGA group.	**Accept-** Agenda template updated. **Implementation date:** 28 February 2017. **Responsibility:** Carol Williams.	🟪	Subject Access performance is a standing item on the FIGA agenda. This is also reflected in the minutes. Reports are also passed through to CMT on a quaterly basis and Audit Committee as appropriate.
b49. (a) The Information Governance and Assurance Manager should finalise the proposal for children's services to process their subject access requests. **(b)** If approved, a date should be set for when Children's Services will take over for their areas subject access requests.	**Accept-** IGAM will action as recommended. **Implementation date:** 30 April 2017. **Responsibility:** Carol Williams.	🟪	A report went to CMT to address options around Children's Services processing their SARs. It was decided that the resource would be kept centrally to facilitate better sharing of knowledge and to gain experience in one place. Funding has therefore been approved for permanent posts going forward. Two temporary staff were appointed in June to increase the capacity in the interim.
b50. Finalise the reporting process for subject access requests to CMT, as planned.	**Accept-** Will be incorporated into the quarterly performance monitoring report produced by Assurance Team. **Implementation date:** 30 September 2017. **Responsibility:** Carol Williams.	🟪	Information on the level of SAR compliance is included in quarterly reports to CMT. In addition more detailed reports that breakdown the number of open cases and rolling compliance rates is provided to FIGA on a more regular basis. The development of the more detailed performance report has provided greater insight into the overall process and has highlighted areas for improvement to ensure a greater consistency in the handling of requests. This also supports the on job training of staff.
b51. (a) Add the timescale for WC to respond to a complaint about subject access requests to the subject access request webpage. **(b)** The timescale for responding to a subject access request complaint should also be added to an acknowledgement letter sent to the data subject.	**Accept-** Update template to reflect inclusion of guidance with letter. Estimated timescales will be included in acknowledgement letter and calculated on a case by case basis connected to complexity and volume of information to be reviewed. **Implementation date:** 31/05/2017 **Responsibility:** Carol Williams.	🟪	Template updated to reflect inclusion of procedural guidance with letter. Estimated timescales will be included in acknowledgement letter and calculated on a case by case basis connected to complexity and volume of information to be reviewed. Webpage has been updated, see heading "How the council uses your information" See Item 5 on the webpage for timescale for the Council to respond
b54. (a) Subject access complaints statistics and content should be reported to Camelot. **(b)** Subject access request complaints which have been reported to the ICO should be reported to FIGA and the CMT.	**Partially accept-** in addition to being information reviewed and discussed at Camelot this information will form part of report to CMT on a quarterly basis. **Implementation date:** 30 September 2017. **Responsibility:** Carol Williams.	🟪	Subject access request complaints statistics are reported to Camelot. This report also contains details of complaints reported to the ICO. The same document is shared as a regular standing agenda item at FIGA meeting and CMT See page 8

Recommendation	Agreed action, owner and date	Status Month 8	Progress Month 8
Data Sharing			
c3. Implement the procedure that is documented in the Information Sharing Procedural Guidelines, to log information sharing agreements in the information asset register.	**Accept-** IGAM will implement as part of procedural review. **Implementation date:** 31/08/2017 **Responsibility:** Carol Williams.	🟪	A corporate Information sharing log has been created and managed at directorate level by the respective Information Champions. These are linked from the Information Asset Managment Tools. The following details are collected: Ref No Asset No from IAR Name of the agreement Data being shared (e.g employee statistics) Date Key Parties Location of Document Directorate / Ownership Council Signatory Review Date
c12. Ensure that the privacy impact assessment (PIA) policy is publicised to all staff that may be involved in setting up a data sharing agreement.	**Accept-** Use existing corporate communication channels to advise anyone setting up a data sharing agreement that a PIA needs to be completed. Updates to DS Procedure. **Implementation date:** 31 May 2017. **Responsibility:** Carol Williams.	🟪	Data Sharing Procedure Guide, Intranet Page and PIA document have all been updated to advise staff that a PIA needs to be completed when data is shared. Article published on News Page of Intranet 31/08/2017 to advise that the document had been updated with direct link. In addition to Data Sharing. PIA's are routinely used for new IT solutions. These are all discussed at the ICT Governance Board
c13. No PIA examples were provided for data sharing agreements, therefore, it is unclear if data sharing agreements are subject to PIA assessment. Ensure PIAs are carried out on existing and future data sharing agreements.	**Accept-** IGAM will update and publish revised Data Sharing to be applied to future data sharing agreements. **Implementation date:** 30 June 2017. **Responsibility:** Carol Williams.	🟪	The Information Sharing Procedural Guidelines document contains a section on conducting a PIA to aid secure and appropriate sharing of personal data (see section 2 page 4) Step 2 of the step-by-step flowchart on pg 8 also confirms this requirement. Article published on News Page of Intranet 31/08/2017 to advise that document had been updated with direct link
C14. (a) Create a record of PIAs either within the information sharing log or the suggested central repository. **(b)** Ensure a copy of the PIA is kept and linked to the log or the suggested central repository.	**Accept-** Central repository has been set up, needs to be populated with back copies and future copies and supplementary documentation. **Implementation date:** 06/10/2017 **Responsibility:** Carol Williams.	🟪	The Council now has a log of all PIAs as well as a central repository for their storage . IAOs and ICs have also been informed of requirement to update.
c15. WC should ensure that the standard template, outlined in the Partners Overarching Sharing Protocol, is used for creating information sharing agreements. Unless it is the case that a leading partner organisation, outside of this protocol, stipulates that a different mandatory template is used.	**Partially accept-** This will be implemented to the extent that it is necessary. Alternative templates will contain all requisite clauses may also be used. **Implementation date:** 30 April 2017. **Responsibility:** Carol Williams.	🟪	Standard Information Sharing Templates are on the IG section of the Council intranet and all guidance has been updated.
c17. The IG Team should document a review process for information sharing agreements for the service areas. This could include the IG team using their log of agreements to set reminder deadlines to contact the service areas when an agreement is due for review.	**Accept-** Update the information sharing log to include the review date. Ensure the sharing agreement has a review date included. **Implementation date:** 31/08/2017 **Responsibility:** Nailah Ukaidi.	🟪	Data sharing log template includes process requirement for ICs to implement local process to ensure that IS agreements are reviewed in line with individual review dates
c19. WC should decide where information agreements are logged and stored, update the relevant policies and procedures to reflect this and ensure staff are aware.	**Accept-** Create the log and inform staff of it location and purpose. **Implementation date:** 30 September 2017. **Responsibility:** Nailah Ukaidi.	🟪	The Information Sharing Procedural Guidelines provides details on how to legally and securely share data. The last paragraph of the Introduction states "All Information Sharing Agreements/Protocols must be logged in the Council's Information Sharing Agreements register" As well as how to do it. Step 5 of the step-by-step flowchart (Section 9 page 8) states that the user should "Place an entry on the Information Sharing Log on the Council network". Information Champions and IAOs informed via email and Information Champion's monthly briefings
c20. (a) Update the data quality procedure to include quality and minimisation requirements for data sharing. **(b)** Update the WC IG policies and information sharing guides to refer to the data quality policy and data quality procedural requirements	**Accept- (a)** Add section on "data minimisation" to DQ procedure. **(b)** Ensure all relevant IG policies refer to the DQ procedure. **Implementation date:** 31 August 2017. **Responsibility:** Nailah Ukaidi.	🟪	The DQ procedure has been updated and now provides guidance on data minimisation. Section 8 page 6 of the procedure states ".....when sharing or using information they should identify the minimum amount of personal data needed to properly fulfil the purpose. In essence you should hold/share that much information, but no more. This is part of the practice known as data minimisation...." Additionally the Information Sharing procedural guidelines document has been updated to refer to the DQ Procedure see Section 6 page 7. The IG policy framework has also been updated to refer to the procedure (see section 3.3.7.2 page 28 and section 3.3.10 page 29)
c22. WC should update quality policy and procedures to include guidance on distinguishing between fact and opinion where appropriate in relation to the nature of shared data.	**Accept-** Update the DQ procedure to give guidance on distinguishing between fact and fiction. **Implementation date:** 31 August 2017. **Responsibility:** Nailah Ukaidi.	🟪	The DQ procedure has been updated and now provides guidance on distinguishing between fact and opinion. See section 7 of the data quality procedure - page 6 (...When recording or sharing information it is important to consider: What information you need to record or share, only record/share what is necessary and distinguish fact from opinion.....)
c24. Devise a process for seeking assurance, where necessary, that personal information has been securely deleted and disposed of at the end of the retention period.	**Accept-** develop template / communication that must be provided to partners as part of data sharing arrangements and returned to WC at end of sharing. This step will also be added to data sharing procedural guidelines. **Implementation date:** 30 September 2017. **Responsibility:** Carol Williams.	🟪	The Overarching Protocol Template has been updated and now requires parties "...to provide evidence of destruction.." (See Appendix F Q10). A sample destruction form is detailed in Appendix J of the protocol .
c29. Ensure that working practices for one off disclosures are supported by policy and procedural guidance for WC staff, as planned.	**Partially accept-** Review procedure if required to ensure process for one off disclosures is streamlined. **Implementation date:** 30/11/2017. **Responsibility:** Carol Williams.	🟩	Separate procedural process will be developed and linked to SARs Handbook will be disseminated to SARs handlers and councilwide. Expect to be completed 30/11/2017

I can confirm that this management response is a true representation of the current situation regarding progress made against our Action Plan outlined in the ICO Data Protection Audit Report dated 3 February 2017.

Signature: ………………...

Position: Head of Information, Communication and Technologies and Senior Information Risk Owner (SIRO)

Organisation: Walsall Council