

City of York Council

Data protection audit report

ico.

Information Commissioner's Office

Auditors: Christine Eckersley (Audit Team Manager)
Stephanie Blears (Engagement Lead Auditor)
Michael Stephenson (Lead Auditor)

Data controller contacts: Andrew Docherty (Assistant Director, Customer and Business Support Services)
Lorraine Lunt (Transparency and Feedback Team Manager)

Distribution: Andrew Docherty (Assistant Director, Customer and Business Support Services)
Lorraine Lunt (Transparency and Feedback Team Manager)

Date of first draft: 7 September 2015

Date of second draft: 13 October 2015

Date of final draft: 12 November 2015

Date issued: 12 November 2015

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rests with the management of the City of York Council.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

Contents

1. Background	page 04
2. Scope of the audit	page 05
3. Audit opinion	page 06
4. Summary of audit findings	page 07
5. Audit approach	page 08
6. Audit grading	page 09
7. Detailed findings and action plan	page 10
8. Appendix A	page 52

1. Background

- 1.1 The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit.
- 1.2 The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.
- 1.3 After two offers of a data protection audit by ICO Good Practice and following a data protection breach, a further offer by the ICO Enforcement Department, City of York Council (CYC) agreed to a consensual audit by the ICO of its processing of personal data.
- 1.4 An introductory telephone conference was held on 12th June 2015 with representatives of CYC to identify and discuss the scope of the audit and after that on 30th July 2015 to agree the schedule of interviews.

2. Scope of the audit

- 2.1 Following pre-audit discussions with CYC, it was agreed that the audit would focus on the following areas:
- a. Records management (manual and electronic) – The processes in place for managing both manual and electronic records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.
 - b. Subject access requests - The procedures in operation for recognising and responding to individuals' requests for access to their personal data.
 - 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.
- 2.2 The audit included visits to the adult and children's social care departments, plus other relevant teams or individuals identified by CYC, in line with the agreed scope areas.
- 2.3 The audit scope areas were chosen to reflect levels of risk agreed mutually between CYC and the ICO. CYC agreed for the ICO to audit areas where it was known that improvements could be made or where processes were in transition in order for the audit to be mutually beneficial.

3. Audit opinion

- 3.1 The purpose of the audit is to provide the Information Commissioner and the City of York Council with an independent assurance of the extent to which CYC, within the scope of this agreed audit, is complying with the DPA.
- 3.2 The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

Overall Conclusion	
Limited assurance	<p>There is a limited level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA.</p> <p>We have made limited assurance assessments across all three scope areas: records management; subject access requests; and data sharing where controls could be enhanced to address the issues summarised below and presented fully in the 'detailed findings' and 'action plan' (appendix A) of this report.</p>

4. Summary of audit findings

4.1 Areas of good practice

- Policy compliance software has been implemented and was reported to be working effectively to communicate key policies to staff and ensure that they have read them.
- Secure storage facilities and thorough archive procedures were in place at Yorkcraft.
- Quarterly information security checks are carried out at the council's two main offices and formal audit reports are produced and presented to the Corporate Information Governance Group (CIGG).
- The MAISP is a good model for Information Sharing Agreements (ISAs) because it is a high level agreement setting out common rules to be followed by all partners and is intended to be used as a basis for future ISAs.

4.2 Areas for improvement

- Many services did not have up-to-date retention schedules and many staff seemed unsure about who was responsible for monitoring retention periods.
- Records management does not currently feature regularly on the CIGG agenda to mandate and monitor records management improvements.
- CYC is in a transitional period in relation to its SARs processes and therefore many new procedures need to be formally documented and embedded.
- SARs compliance rates between 1st April 2014 and 31st March 2015 were very low, at 51.1%.
- There is no systematic data sharing training in place and no council wide information governance training needs analysis to identify the requirement for such training.
- CYC's PIA process is yet to be fully developed and implemented.

5. Audit approach

- 5.1 The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.
- 5.2 The audit field work was undertaken at West Offices and Yorkcraft from 18th August 2015 to 20th August 2015.

6. Audit grading

6.1 Audit reports are graded with an overall assurance opinion, and any issues and associated recommendations are classified individually to denote their relative importance, in accordance with the following definitions.

Colour code	Internal audit opinion	Recommendation priority	Definitions
	High assurance	Minor points only are likely to be raised	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with the DPA.
	Reasonable assurance	Low priority	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA.
	Limited assurance	Medium priority	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA.
	Very limited assurance	High priority	There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

7. Detailed findings and action plan

7.1 Scope a: 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 Data Protection Act 1998, resulting in regulatory action by the Information Commissioner's Office, reputational damage to the data controller and/or damage and distress to individuals.

a1. Information governance (IG), which includes the records management function, is now within the Customer and Business Support Services (CBSS). It is part of Legal, Civic and Democratic Services, following a restructure and the creation of a new operational post, 'Transparency & Feedback Team Manager' in April 2015. Therefore, this structure is still in its infancy.

a2. The Director of CBSS, who is also the Deputy Chief Executive Officer and the Senior Information Risk Owner (SIRO), has lead responsibility for the strategic direction and oversight of IG. For instance, the SIRO chairs the Corporate Information Governance Group (CIGG) is responsible for the Annual Governance Statement, and is the lead officer for Audit and Governance and has taken a number of reports to the Audit & Governance Committee.

a3. The Assistant Director of Governance and ICT reports to the SIRO, and it was confirmed during interviews that he now also has strategic responsibility for records management and some operational responsibilities. The Assistant Director of Governance and ICT, now line manages the Transparency and Feedback Team Manager.

a4. The new operational post, Transparency and Feedback Team Manager, sits within the Customer Complaints and Feedback Team (referred to as the 'council team' hereinafter). It was reported that this is an operational post within which the post holder also has operational responsibilities for records management. The Transparency and Feedback Team Manager is supported by the [REDACTED] [REDACTED] both post holders were interviewed and appeared to have detailed knowledge of how the information governance function is working day-to-day.

a5. A report issued to the Audit & Governance Committee in June 2015 from the SIRO, highlights the responsibilities of the Transparency and Feedback Team Manager. These include "providing strategic leadership in the development and delivery of the council's IG arrangements, including delivering priorities such as: the council's Information Governance Strategy; the council's data protection and information security arrangements; records management; and transparency of information". In addition to this, a job description for 'a new Information Governance Manager' was provided for review. As the new post has a different title, this seems to be an inherited job description although it appears to be consistent with the majority of responsibilities

reported onsite. This job description stated that the purpose and main objectives of the post are to “provide strategic leadership in the development and delivery of the Council’s information governance arrangements” including the records management function. However, the job description also details operational responsibilities such as providing expert advice, supporting related training and supporting the implementation of strategies and policies. Therefore, there is some inconsistency in the reports onsite and the documented report and job description provided, as to whether this post attracts operational or strategic responsibility for records management.

Recommendation: Ensure that the job description for the Transparency and Feedback Team Manager accurately reflects the newly assigned responsibilities for information governance, incorporating records management. There should be a clear distinction between post holders with strategic responsibility and post holders with operational responsibility for the records management function.

Management response: Accepted

CYC will review current job description to ensure clarity for strategic and operational responsibilities for records management.

Owner: Andy Docherty, Assistant Director

Date for implementation: 31st December 2015

a6. Prior to the creation of the Transparency and Feedback Team Manager post, CYC did not have a dedicated post holder with operational responsibility for the records management function since its last Records Manager left over a year ago. IG is currently outsourced to Veritau, which is a joint company set up between CYC and North Yorkshire County Council. Veritau essentially consists of both Councils’ audit and fraud teams. The Head of Veritau reports to the SIRO who chairs the company. Responsibility is currently being transferred back into CYC using a staggered approach,

to ensure operational control and overall accountability clearly sits within CYC.

a7. It was encouraging to hear reports that the SIRO has led on investing in resource for the restructure of the council team to support the operational aspects of the Council’s information governance arrangements incorporating the records management function.

a8. CYC also has a ‘Facilities Management Scanning and Mail Unit’. This unit’s services include: scanning documents onto the Council’s Electronic Document and Records Management System (‘Documentum’), either as part of day-to-day Council business or for projects i.e. move to offices with less storage space for paper records; storing scanned documents and arranging for their transfer to offsite storage; and delivering and collecting post. The services of this unit are corporate wide.

a9. CYC’s Records Management Policy sets out ‘directorate/service team manager’ responsibilities which include: “to ensure that appropriate staff are designated to assist and support the implementation of records management procedures within each service area”. However, there was no evidence to suggest that local responsibilities had been assigned.

Recommendation: Assign local records management responsibilities in line with the requirements of the Records Management Policy.

Management response: Accepted

CYC will identify and assign local records management responsibilities in line with the reviewed/updated Records Management Policy.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30th June 2016

a10. The Records Management Policy also sets out service management team and staff responsibilities. All staff are required to: adhere to the policy; ensure actions and decisions taken in the course of business are properly recorded; ensure the proper filing of records so that a colleague can easily find them; and ensure the proper disposal of records via the corporate confidential waste procedures and in accordance with the an agreed retention schedule. Service Management Team responsibilities include: ensuring implementation of the policy; ensuring local responsibilities are assigned; supporting staff in records management training; assigning owners to records; ensuring that records are stored with proper access arrangements and levels of security commensurate with their level of confidentiality; ensuring that electronic records are stored in a consistently ordered filing structure with an agreed retention schedule applied.

a11. The steering group in place for information governance is the Corporate Information Governance Group ('CIGG'). The group's Terms of Reference provide that it has overall responsibility "for the development and implementation of an effective corporate strategy to ensure CYC complies with its responsibilities for data protection, freedom of information and records management".

a12. However, it was reported that records management has not featured regularly on the CIGG agenda for at least twelve months. Interviewees explained that there was a big push on records management in line with office move two and a half years ago. This is in line with CYC's Information Governance Strategy produced in 2010 which states "*The move to the new council Headquarters (...) is actually a once-in-a-lifetime opportunity to put records management in good order and the principal tool to do so, the Documentum EDRMS, is already in place.*" It was also reported that more recently, the CIGG has focused on information governance issues attracting reputational risk

such as its compliance with Freedom of Information (FOI) requests. There were reports of intentions to ensure that records management is put back onto the CIGG agenda.

Recommendation: Ensure that records management features regularly on the CIGG agenda to mandate and monitor records management improvements.

Management response: Accepted
CYC has completed the review of the CIGG terms of reference which will now be the Information Management Board (IMB) and includes records management including monitoring and compliance, in its purpose, aim, remit and objectives. The first meeting is planned for mid-November at which the standard agenda items will be approved.
Owner: Lorraine Lunt, Transparency & Feedback Team Manager
Date for implementation: 31st December 2015

a13. The group is chaired by the SIRO and attended by the Assistant Director of Governance and ICT, the Transparency and Feedback Team Manager (who has been attending since the end of last year) and representatives from each directorate, some of whom are nominated Information Asset Owners. The group's Terms of Reference state that it meets eight times a year or approximately every 6 weeks.

a14. CYC does not currently have a targeted programme of work for records management as required by the current Records Management Policy. It was reported that the Transparency and Feedback Team Manager (who will be responsible for such a programme going forward) has some high level work on her agenda but this is not formally documented. It was also reported that the plan is to form the targeted work programme upon receipt of the ICO audit report.

Recommendation: Implement a records management programme of work and ensure that records management actions/ improvements and lessons learned are identified and implemented as necessary. This programme should be overseen by the CIGG.

Management response: Accepted

CYC will develop a records management forward work programme.

The IMB is to be responsible for records management monitoring and compliance as stated in the Terms of Reference

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st March 2016

a15. CYC's corporate Records Management Policy covers both manual and electronic records, sets out the records management principles, statement of policy, roles and responsibilities and the records management programme. However, it does not expressly state how policy compliance will be monitored.

Recommendation: Ensure that the Records Management Policy outlines methods for monitoring policy compliance and that this is communicated to staff.

Management response: Accepted

CYC will include monitoring compliance and guidance in the review of the current Records Management Policy. The launch of the revised policy will include a communications plan for raising awareness as well as guidance, training package(s). When completed, this will be published on the intranet and internet.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31 March 2016

a16. It was reported that CYC wants to review the policy in order to make it more user friendly by communicating the key information to all staff in an easily digestible format. Revision of the policy is to be led by the Transparency and Feedback Team Manager.

a17. The Records Management Policy was first approved by the CIGG in February 2013 and was due for review in February of this year. However, this review has not yet taken place. It was reported that this was because the CIGG has instead prioritised the council's FOI compliance rates and attainment of HSCIC IG toolkit assessment.

Recommendation: Ensure that the Records Management Policy is reviewed in line with time periods for review set out in the policy.

Management response: Accepted

CYC is currently underway with a review of the Records Management Policy (including a communications plan) and will put in place a monitoring process to ensure future reviews are undertaken within the set time periods.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st March 2016

a18. An extensive set of records management guidance was also provided for review. This is staff guidance that was produced by the previous Records Manager. However, most documents were marked as drafts and there was no evidence that this guidance had been widely communicated to staff across the Council.

Recommendation: Review the draft records management guidance alongside the Records Management Policy to ensure that it is complete, consistent and up-to-date. Ensure that communication of records management

guidance is included within a Communications Plan for the Records Management Policy.

Management response: Accepted

CYC is currently reviewing the guidance, training package(s) etc for records management alongside the review of the policy. Following the approval of the reviewed policy, CYC will undertake the actions from the communications plan including providing guidance, training package(s) and publication on the intranet.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st May 2016

a19. The Records Management Policy is available to staff on the intranet. However, CYC does not have a record of policy acceptance for the current Records Management Policy. It was reported that policies are usually communicated to staff via an all staff email and are then often discussed at directorate team meetings, but this is not recorded.

a20. It was widely reported that iComply, a policy management software product, is now in place and working effectively throughout the Council. It is anticipated that iComply will be used to communicate the revised version of the Records Management Policy.

a21. Job descriptions exist for those with key records management responsibilities. Namely, staff within the Facilities Management Scanning and Mail Unit and the role of the IG Manager which has now been taken on by the Transparency & Feedback Team Manager.

a22. It was confirmed that CYC's standard employment contract terms refer to council policies and procedures and therefore requirements, standards, instructions, guidance etc. set out in policies i.e. Code of Conduct, Electronic

Communications Policy, IT Security and Acceptable Use Policy etc. are all implied terms and conditions of CYC's employment contracts. Therefore, all staff legally agree to abide by CYC's information governance policies on appointment.

a23. Staff at CYC do not currently receive records management training within a formal training programme.

Recommendation: Ensure that records management is incorporated within a formal training programme that comprises mandatory induction and periodic refresher training for all staff with access to personal data.

Management response: Accepted

CYC will ensure that records management is included in its training/learning/development mandatory framework including induction, targeted dedicated sessions aligned to local records management responsibilities, and refresher.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30 April 2016

a24. Records management training material was developed in late 2012 and early 2013 by CYC's previous Records Manager. However, there is no record of staff receiving this training and receipt of such training was not reported during interviews.

a25. CYC introduced its latest mandatory IG induction training in September 2014 and was last delivered in June 2015. Staff are required to complete this training within three months of starting at CYC. This course covers general 'dos and 'don'ts', some of which touch on records management i.e. 'do practice a clear desk policy', 'do dispose of sensitive personal data securely' and 'don't email documents to your private address'. However, these are

headline points and not detailed enough to satisfy records management training requirements.

a26. Staff within social care services reported receipt of professional training which covered management of records and confidentiality of records in particular. There were also reports of discussions and reminders of data protection and confidentiality of records, during supervision and in team meetings. This supports the corporate view that 'pockets of training' are taking place but this is not formally recognised at records management training.

a27. It was reported that CYC is currently undertaking the development of a managed programme for records management with its Workforce Development Unit which will include records management learning needs, timely provision of training as well as reporting and monitoring.

a28. There is no current Training Needs Analysis (TNA) that has identified basic or additional records management training needs for individuals or staff groups.

Recommendation: Ensure that records management training needs are assessed and addressed for key roles and staff groups.

Management response: Accepted
CYC will link this with the identification of local records management responsibilities, inclusion in the mandatory framework and into the PDR process where appropriate. Progress of TNA as well as meeting the needs identified through the TNA, will be monitored via the IMB.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st May 2016

a29. It was reported that objectives and learning needs identified in Personal Development Reviews (PDRs) now feed

into the Council wide learning system, iTrent. Therefore, PDR information will be used to contribute to future TNAs. It was also reported that records management or IG more generally, has rarely featured in PDR learning objectives.

a30. CYC's Data Protection Policy, provides that Directors are responsible for providing a service privacy statement for each of their services. However, the policy does not appear to have been updated since 2008.

Recommendation: Review the Data Protection Policy to ensure that it is up to date and reflects best practice.

Management response: Accepted
CYC is currently underway with a review of the Data Protection Policy (including a communications plan, guidance, training packages) which is now taking account of the comments and recommendations in this ICO audit.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 29th February 2016

a31. Various privacy notices are available on CYC's website and links to some of these were provided for the purposes of the audit. There is a main council privacy notice, and service specific privacy notices were reviewed for schools services and some youth services. However, when searching the website without reference to links provided, some of the privacy notices reviewed were not easy to locate from the homepage.

Recommendation: Ensure all privacy notices are readily available and easily accessible from the council's homepage.

Management response: Accepted
At the launch of the new CYC website, we updated the Privacy Notice accessible via the main/home page. Further work will be undertaken following the collation of all existing

privacy notices, information sharing agreements etc as part of the new "information asset register monitoring and compliance" across the council, to identify how best to ensure all are easily accessible/searchable/linked where relevant from the main web page.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30 April 2016

a32. Privacy notices did not appear to be available for all services although the council's Data Protection Policy requires that such notices exist i.e. privacy notices were not located on CYC's website for adult social care services.

Recommendation: Ensure that privacy notices are made available for all services to inform individuals about the use of their personal data.

Management response: Accepted

As part of the new "information asset register monitoring and compliance" across the council, we will be able to identify where privacy notices are not held and therefore put in place a work plan to complete these.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30 April 2016

a33. It is not clear if there is a policy requirement to regularly review privacy notices.

Recommendation: Ensure that there is a policy requirement to regularly review the accuracy and content of privacy notices.

Management response: Accepted

CYC will include the requirement for regular review of the accuracy and content of privacy notices in the review of the Data Protection policy and develop guidance, training package(s) for staff responsible for privacy notices.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30 April 2016

a34. Examples of an initial assessment for a funding application, an application form for financial assistance, and a telephone data collection form used by the personal budget support team were provided for review. All examples provided contained fair processing information.

a35. Staff within social care teams reported that fair processing information was initially provided by the Customer Contact Team which is the first point of contact for a service user. Consent to share service users' personal data with relevant parties, is also requested at this stage and interviewees demonstrated completed consent forms on the relevant social care systems (the adult and children's social care systems).

a36. The adult social care system ('Frameworki') had a warning screen where refused consent could be recorded. This was demonstrated onsite. It is good practice to flag refused consent. However, the children's social care system did not have a similar facility and refused consent was recorded by way of case note.

a37. Interviewees also explained the process for adult social care service users who were deemed to lack capacity to understand fair processing information and consent to any sharing of their personal data. Checks are made with family members or other appropriate person(s) to establish if they have a power of attorney or deputyship. Staff demonstrated evidence of requesting and receiving copies of court documents and contact with the Court of Protection where official documentation could not be provided.

a38. CYC has a corporate Information Asset Register (IAR) in place that shows what information is held, in what

format and what value (recorded as high, medium or low risk) the information has. Additionally, the IAR records: who owns the information identified; whether the information is shared with another service/ organisation and if an Information Sharing Agreement is in place; and who has access to the information.

a39. However, it was reported that the IAR has not been reviewed for approximately 12 months and is therefore likely to contain out-of-date information, particularly where staff have left or moved roles and systems have changed. It was also reported that the required update for the IAR was discussed at the last CIGG meeting but there are no meeting minutes detailing this.

Recommendation: Review the IAR quarterly to ensure that it remains up-to-date and fit for purpose. Ensure that the IAR references relevant risks to the information assets.

Management response: Accepted

CYC is currently underway with updating the IAR which includes how it will be monitored and used to identify areas such as PIAs, PIA risks etc where relevant. The IMB will monitor compliance.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31 March 2016

a40. Quarterly information security checks are carried out at the council's two main offices (West Offices and Hazel Court), by its internal audit function (Veritau). Formal internal audit reports are produced and presented to the CIGG. A number of these reports were provided for review.

a41. The reports provided highlighted findings such as non-compliance with CYC's Clear Desk Policy; findings of several lockable cupboards and draws left unlocked containing personal data with varying levels of sensitivity; and unsecure storage of keys for storage units. However,

the reports provided showed that notable improvements were being made across the Council as reports issued in 2014 offered moderate assurance and reports issued in 2015 offered reasonable assurance.

a42. CYC also has its own archiving service, Yorkcraft. Yorkcraft is a supported business for people with disabilities. It is a council service and is therefore staffed with council employees. It was reported that arrangements at Yorkcraft had not yet featured in the Council's internal audit plan to date. Therefore, CYC does not currently have any formal assurance of how secure storage areas are at Yorkcraft.

Recommendation: Include storage arrangements at Yorkcraft within the internal audit plan of security checks.

Management response: Accepted

CYC will include Yorkcraft in the internal audit plan of security checks. Meeting arranged with internal auditors mid-November for this.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31 December 2015

a43. It was widely reported that the records held in adult and children's social care are now held electronically on their respective records management systems. CYC undertook a large project to reduce the number of physical records held when it moved its head office two and a half years ago, as the new premises has substantially less storage space for physical records.

a44. A demonstration was provided of the children's system ('Raise') to show where the locations of paper files relating to live service users are recorded. The system has a dedicated section to record this information so that staff can easily ascertain where a related paper file is, when it was put in this location and by whom.

a45. Children's and adult social care archived physical records are stored offsite at Yorkcraft. It was reported that details of archived files are recorded within services and that both adult and children's services maintain a spreadsheet of archived physical files. However, it was also reported that there are no files in archive that have not already been scanned onto the adult social care records management system ('Framework'). Due to this, there appears to be a duplication of adult social care data held by the service. This may increase the risk of the Council breaching Principle 4 or 5 of the DPA.

Recommendation: Review the requirement for the retention of both scanned and manual client records by adult social care.

Management response: Accepted

CYC will review retention requirements for both scanned and manual adult social care records. The Transparency and Feedback Team Manager and the IMB where appropriate, will advise and support the service area. The Transparency and Feedback Team manager is attending the case management system project board to incorporate the scanned and manual records retention requirements into the project.

Owner: Director of Adult Social Care

Date for implementation: 31st March 2016

a46. During the tour of Yorkcraft, boxes labelled 'mystery social services' were observed in the main archive. Yorkcraft staff did not know exactly which team these boxes belonged to but were aware which directorate they belonged to. In the absence of a named owner of these records, Yorkcraft does not know exactly who is responsible for them. In addition to this, there were also separate filing cabinets within Yorkcraft, containing adult social care records. It was reported that these filing cabinets were removed from CYC's previous offices and sent to Yorkcraft during the move.

Therefore, relevant teams within CYC may not know the whereabouts of these records. In addition, these records were not stored in barcoded storage boxes in the way that all other records were and were therefore not part of Yorkcraft's current logging and tracking system. This means that Yorkcraft is not managing the storage of these records in line with its documented archive procedure.

Recommendation:

- a) Assign owners to the boxes of 'mystery social care' records stored at Yorkcraft.
- b) Ensure that the adult social care records stored within the separate filing cabinets at Yorkcraft are logged and tracked in line with Yorkcraft's Archive Procedure.

Management response: Accepted

CYC will identify and/or assign owners within the service area.

The Transparency and Feedback Team Manager and Yorkcraft will work with the service area to ensure that arrangements are put in place for logging and tracking of the information held in the storage cabinets.

Owner: Director of Adult Social Care

Date for implementation: 31st May 2016

a47. Services requiring offsite storage of records at Yorkcraft, must first request the appropriate boxes and labels from Yorkcraft. This is done by completing a request form (copy provided for review) available on the staff intranet and emailing it to the Yorkcraft Archives Mailbox. The service must provide the department name, a contact for delivery and the delivery address. This allows Yorkcraft to produce the box labels and ensures that have a record of who the boxes have gone out to. Also, because tailored labels are produced for the boxes, they cannot be used by any other service. It was reported that Yorkcraft does chase services up if they do not return requested boxes. The full history, from box creation to record storage and eventual

destruction is recorded on Yorkcraft's database and services must sign an acknowledgement to confirm that they received the requested boxes.

a48. There is a further request form to complete to request that Yorkcraft collect boxes of archived records from the service. When a box arrives at Yorkcraft for storage, the label barcode is scanned and the location of storage is recorded on Yorkcraft's database.

a49. Equally, if a service requires a box of records from Yorkcraft, a request for retrieval of documents must be completed. Again, the transfer is recorded on Yorkcraft's database and the service must sign an acknowledgement to confirm receipt. Yorkcraft also retains a copy of all email requests for its own audit trail.

a50. Yorkcraft does not monitor the location of records once they have been retrieved from storage. Responsibility for the whereabouts of retrieved records lies with the service. However, services reported that monitoring of records retrieved from storage was not actively taking place. Services record requests of archived records from storage on their case management system, but nobody checks whether records have been returned to storage.

Recommendation: Introduce a tracing system to ensure that services actively manage the whereabouts of records retrieved from storage.

Management response: Accepted
CYC will complete the development and introduce a tracing system for records retrieved from storage.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st March 2016

a51. CYC's legal services also hold all of their current records on their case management system ('Norwel'). Legal services also have a physical archive at the Guildhall, an old council building. Records held there include social services correspondence files from 1996 – 2012 and some court bundles. Although, it was reported that a project is underway with the Facilities Management Scanning and Mail Unit, to scan the bundles on to Norwel. All social services new cases (since 2012), only have electronic correspondence files and electronic court bundles. Other legal services files are also kept at the Guildhall and it was reported that they will eventually be scanned onto Norwel.

a52. It was reported that if a record is retrieved from the Guildhall, there is no logging system there. Instead, the retrieval is recorded on Norwel as soon as the record is brought back into the office. Legal services records retrieved from archive are not actively monitored to ensure that they are returned to storage in a timely manner. Although, it was reported that records are returned to the Guildhall when the work is finished, and the return date is recorded on Norwel.

a53. It was reported that CYC has two data centres. The main data centre is within West Offices and a smaller data centre at Hazel Court, which is just less than two miles away from West Offices. The data centre at Hazel Court mirrors data held at West Offices for back-up.

a54. It was reported that testing of the back-up system is done at server level. Periodic testing was reported to have taken place along with controlled testing prior to any new projects that could affect data held going live, to check that systems can be recovered.

a55. A number of Business Continuity Plans and Business Impact Assessments were provided for services across the council. These documents identify risks to critical software, systems and applications, along with documentation and

vital records. However, most were either draft versions or over a year past their review date.

Recommendation: Ensure that all Business Continuity Plans are finalised and reviewed and tested in line with the review dates specified on the plans/ assessments.

Management response: Accepted

CYC will ensure all BCPs are finalised and reviewed in line with the dates they specify.

Owner: Steve Waddington, Assistant Director Housing and Public Protection

Date for implementation: 30 June 2016

a56. CYC has an Information Systems Security & Acceptable Use Policy which addresses storage, handling and transmission of records. This policy sets out responsibilities of employees, managers and chairs of relevant committees. ICT staff reported that staff awareness of this policy was last raised in January 2015 using iComply.

a57. It was also confirmed that the policy is based on the information provided by the Cabinet Office for PSN accreditation and ISO27001. However, it has not been officially benchmarked against ISO27001.

a58. There is also an Electronic Communications Policy in place. This communicates staff responsibility for the security of data held by CYC and forms part of CYC's corporate induction. The induction checklist must be signed off by a new starter's line manager to confirm that they have read this policy.

a59. At the end of a working day live physical records held in the office are stored in lockable team cabinets or personal lockers viewed onsite. There did not appear to be any consistency across services as to whether live physical records were stored in team cabinets or personal lockers.

Staff reported that they keep keys to personal lockers in their possession and take them home at the end of a working day. This raises the risk of live records being difficult to track or access, if other team members are unaware that their colleagues have stored live records in their personal lockers.

Recommendation: Ensure that a consistent approach is taken across all services for the storage of physical files in the office.

Management response: Accepted

CYC has 2 main sites at West Offices and Hazel Court, as well as other facilities/locations across the city. CYC will respond to this recommendation at the 2 main sites by putting in place a consistent approach to storage of physical files. CYC will then roll this out across the other facilities/locations and monitor compliance with this through the information security sweeps conducted by internal auditors.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st March 2016

a60. The arrangements for secure storage of team cabinet keys appeared to differ between services, with some services storing keys to locked cabinets in other unlocked cabinets and other services returning keys to be stored in a key safe in the Security Team's office.

Recommendation: Ensure that all services, and teams within them, have a procedure for the secure central storage of cabinet keys.

Management response: Accepted

CYC is underway with investigating the options and impacts for the development of a process for secure central storage of cabinet keys. This will include a roll out/ implementation

plan, communications plan and compliance/ monitoring plan.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st May 2016

a61. Fee earning staff within legal services have team storage cabinets to store physical records at the end of a working day [redacted]

a62. Yorkcraft [redacted]

a63. Visitors to Yorkcraft must sign the visitors' book and if they wish to view records onsite, they must be listed as an authorised person prior to arriving. CYC ID cards are checked on arrival. Approved persons are determined by Heads of Service and Yorkcraft issues their approved persons list to Heads of Service monthly to ensure that they remain correct. Approved persons viewing records onsite are taken to a separate room for this purpose and the relevant records are retrieved for them by Yorkcraft staff. Approved persons are not allowed into the archive to retrieve records.

a64. [redacted]

[redacted] An authorised Business Support Officer from children's services was present at Yorkcraft during the tour

to demonstrate this. [redacted]

a65. The Facilities Management Scanning and Mail Unit prepares original copies of scanned documents for storage after they have been scanned into the EDRMS ('Documentum'). Original copies are stored in cardboard boxes by this unit for up to two weeks before they are collected [redacted]

Recommendation: Ensure that appropriate restrictions are in place to prevent [redacted]

Management response: Accepted
CYC is currently investigating options to ensure that appropriate restrictions are in place to meet this recommendation.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st March 2016

a66. In legal services, the Practice Manager manages access controls for Norwel. It was reported that different teams within the service cannot view each other's cases on Norwel. The Practice Manager sets access permissions for new starters and also removes these as required.

a67. CYC's ICT service reported that it was responsible for administering access to a number of council systems including the adult social care system and the housing and benefits system. However, ICT does not administer access

controls for the children's social care system – Raise. This is strictly controlled by Raise Support and only given when requested by a Service Manager. Access to the new Mosaic system will be administered by ICT going forward.

a68. There is a new user request form available via the ICT self-service portal. Guidance on the intranet directs line managers to complete a new user request for their new starters, to allow them to gain a log-in and access to central ICT facilities. It was reported that upon receipt of a request, a member of ICT contacts the relevant line manager to determine the level of access needed for service specific systems and the team that the user should be associated with.

a69. If staff move teams or services within the council, the receiving line manager completes a transfer user form. The internal transfers induction checklist provided for review, instructs the line manager to contact ICT and arrange access to team folders. It was reported that home drives are mapped to areas so a mover's access would be really affected if their access permissions were not changed. ICT reported good compliance with this process.

a70. The managers' checklist in the exit procedure provided for review requires a delete user account request to be made via the ICT self-service portal. It was reported that ICT receives a list of leavers from HR each month and runs a script through the active directory to ensure that leavers' access permissions have been removed. This process acts as a backstop in the event that a line manager does not complete a delete user account request.

a71. ICT has an escalation process for the immediate removal of access permissions if required and this is usually led by the Head of ICT. Immediate removal of access permissions is required by the Electronic Communications

Policy in the event that employment is terminated as a result of disciplinary action.

a72. The systems administrator for Raise grants and revokes user access. Requests to set up a new user come via ICT as they receive the new user request forms from line managers. The process is similar for movers and leavers. However, there is a support mailbox for the Raise support team and therefore user access requests can be made directly to the team rather than via the ICT self-service portal.

a73. It was reported that staff are required to complete systems training prior to obtaining access permissions. Staff reported that there was a dedicated trainer for Frameworki who delivers several training modules and access links to completion of these modules. Therefore, full access is not granted until all modules have been completed. Staff using Raise reported that system training has been delivered by admin staff within the service or by buddying up with experienced colleagues. There did not appear to be a formal approach to system training in children's services.

a74. However, it was reported that a new children's social care system is being implemented ('Carelogic' provided by Mosaic) and systems training has already been sourced. The training will be provided by MeLearning, a company that provides ELearning courses to teach users how to use the new Carelogic system.

a75. It was reported that legal services has a record of access permissions granted to Norwel but it is not routinely reviewed to ensure that privileges granted continue to be based on business need and have been correctly authorised. Access permissions are granted only by the Practice Manager, and this is done when a person starts working in legal team and then again on the rare occasions when staff

move within the team for example trainee solicitors rotating through work areas, or staff secondments to other teams.

Recommendation: Introduce periodic reviews of access permissions granted in Norwel.

Management response: Accepted

CYC is underway with investigating the tasks required and the impacts of introducing periodic access permission reviews in Norwel.

Owner: Practice Manager

Date for implementation: 31st March 2016

a76. ICT staff reported that there is a schedule of systems access reviews which take place bi-annually or annually. The review process reported is that a list of all system users is sent to the relevant manager and system owner and they must confirm that the access permissions listed are correct. It was reported that this process occasionally highlights a leaver, or a user with a slightly different role to the role that their access permissions are aligned to, but instances of inappropriate access permissions are not usually found.

a77. It was reported that inactivity reports are ran periodically to monitor access permissions for Raise, and business support complete audit checks of teams and manage phone lists as a lot of staff work away from the office.

a78. There is no routine auditing of access to records but it was reported that Frameworki, Raise and the housing and benefits system were all capable of producing audit logs of user activity to support monitoring, incident response and investigation. Therefore, audit of this nature is exception-based.

a79. Social workers take physical copies of assessments offsite, usually for home visits. It was reported that social workers are made aware of security risks and told how records should be managed when taken offsite. However, communication of expectations varied with some staff believing these messages to have been communicated within their professional training and others reporting that occasional reminders are sent round from Veritau. Staff were generally unclear as to whether there was any documented guidance on the matter.

Recommendation: Clear and consistent guidance on taking records containing personal data offsite, should be produced and made available to staff.

Management response: Accepted

CYC will include this in the current review of the DP policy and guidance and training package(s).

Owner: Director of Adults Social Care and Director of Children's Services

Date for implementation: 29 February 2016

a80. Staff are not provided with means of secure storage to transport records offsite i.e. a lockable briefcase, trolley bag etc. However, it was reported that adult social care is looking at introducing tablets so that staff do not have to take physical records offsite.

Recommendation: Staff should be provided with or advised on appropriate methods and/or media for transporting client records offsite.

Management response: Accepted

CYC will include this in the current review of the DP policy and guidance and training package(s).

Owner: Director of Adults Social Care and Director of Children's Services

Date for implementation: 29 February 2016

a81. Staff consistently report two methods for sending electronic copies of personal data securely. These were: using their GCSx account for which they had to complete mandatory ELearning training; or by secure email if the recipient is not part of the GCSx. CYC uses MacAfee IronMail and [REDACTED]

[REDACTED] This means that the information does not leave CYC's network.

a82. Some staff also reported on the implementation of a secure document exchange system ('Doqex') which was being trialled in certain services at the time of the audit.

a83. We were advised that CYC use a protective marking scheme for personal data. This outlines what security measures should be taken when sending different classifications of personal data. We were provided with a screenshot of the staff intranet page referring to data security. The page includes a link to guidance on security classification. The link states "Read all Ten Golden Rules - the Do's and Don'ts". It is not clear if this corresponds to the "Simple security classification document" we were provided outlining the above.

Recommendation: Ensure guidance on the protective marking scheme within the staff intranet is up-to-date. Any updated scheme arrangements should be communicated to staff.

Management response: Accepted

CYC will undertake a review of the current guidance and update this where required. This will include a review of the layout and look and feel of the information on the intranet. All changes will be communicated to staff.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st March 2016

a84. Procedures for sending personal data by post appeared to vary across services with some services marking this post as 'private and confidential' and informing recipients that post had been sent and others only sending letters to say that personal data such as an assessment is complete and requests that the recipient contacts CYC if they wish to receive a copy. Addresses on post did not appear to be double-checked despite often being hand written.

Recommendation: Appropriate and consistent security measures should be in place when sending personal data (especially sensitive personal data) by post. Considerations should be given as to whether personal data can be minimised or sent by other means; and addresses should be checked.

Management response: Accepted

CYC will include this in the current review of the DP policy and guidance and training package(s).

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st March 2016

a85. Incoming and outgoing post is managed by the Facilities Management Scanning and Mail Unit. There are pigeon holes for incoming and outgoing post viewed onsite, in central hubs on each floor. The pigeon holes are not secure and accessible by any staff with access to that floor. Each floor is open plan with several departments across different services located on it. It was reported that the Scanning and Mail Unit is hoping to move to digital mail to speed up delivery and address such security risks for incoming post.

Recommendation: Consider an appropriate method to reduce the risk of unauthorised access to incoming and outgoing post.

Management response: Accepted

CYC will consider options to provide appropriate methods (both in the short and long term) to reduce the risk of unauthorised access to incoming and outgoing post.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st March 2016

a86. The last post collection is at 2pm each day, and there are no formal procedures in place for storage of outgoing post after this time. It was reported that outgoing post could be left unsecured in the outgoing post pigeon holes until the following day.

Recommendation: Introduce procedures to ensure that outgoing post is stored securely after the last collection each day.

Management response: Accepted

CYC will investigate options to provide appropriate procedures for ensuring outgoing post is stored securely

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st March 2016

a87. There is a formal process to report all personal data related incidents. CYC has a security incident report form available on the intranet which must be completed and sent to Veritau. Staff consistently reported that they would report any data breaches to their line manager who would then escalate the report.

a88. CYC has a Security Incident Log in place which was provided for review and showed incidents logged for 2014/15 and 2015/16.

a89. CYC's Records Management Policy requires all employees to ensure that records are disposed of in line with an agreed retention schedule. Guidance has also been produced to explain what a retention schedule is, and why it is needed. However, the majority of staff interviewed were unsure if retention schedules existed. Retention schedules were not provided for review.

Recommendation: CYC should have up-to-date retention schedules in place which are based on business needs and have reference to statutory requirements and other relevant principles. Retention schedules should provide sufficient information for all records to be identified and disposal decisions put into effect. There should also be a link between the assets in the IAR and their associated retention schedules.

Management response: Accepted

CYC is currently underway with a review of the Records Management Policy as well as updating the IAR which will include identifying retention schedule(s) that need updating. This identification will then inform a work plan to ensure they are based on business needs and reference statutory requirements and provide information on identification and disposal.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30th June 2016

a90. A retention schedule monitoring spreadsheet was provided for review. This logged service codes, whether a retention schedule exists, any email follow ups, and retention schedule status. However, no monitoring appears to have taken place since 2013.

Recommendation: Retention schedules should be regularly reviewed to ensure that they meet business needs and statutory requirements.

Management response: Accepted

CYC has updated the terms of reference for the IMB (replacing CIGG) and it includes records management monitoring and compliance. Alongside this, CYC is underway with updating the IAR and identifying a work plan for updating retentions schedules, all of which will support the regular review of retention schedules to ensure they meet business needs and statutory requirements.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30th June 2016

a91. CYC's Records Management Policy provides that Directorate/ Service Management Team responsibilities include ensuring that records have an identified owner charged with their proper maintenance which includes setting appropriate retention periods. However, the majority of staff interviewed did not know who was responsible for monitoring retention periods with many reporting that they did not think retention periods were being properly monitored in their service.

Recommendation: Assign responsibility to appropriate individuals/asset owners to ensure retention periods are adhered to.

Management response: Accepted

CYC has updated the terms of reference for the IMB (replacing CIGG) and it includes records management monitoring and compliance. Alongside this, CYC is underway with updating the IAR and identifying a work plan for updating retentions schedules, all of which will support

the assigning of responsibility for adherence to retention schedules.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30th June 2016

a92. Yorkcraft's archive procedure provides that it will contact services in advance of the destruction date marked on each archive box, to seek authorisation for destruction. It was consistently reported by staff that this was the usual process for destruction of archived physical records.

a93. Yorkcraft has a contract [REDACTED]

a94. ICT reported that CYC has a contract [REDACTED] accredited to ISO9001 and ISO14001. [REDACTED] granted approval as an Authorised Treatment Facility (AATF) [REDACTED]

a95. There are locked confidential waste bins on each floor of West Offices. These were observed onsite and staff reported using the bins to dispose of confidential waste. Biodegradable bags with secure ties are provided for Hazel Court, as this office does not yet have lockable bins.

a96. The confidential waste bins are managed by Yorkcraft, [REDACTED]

[REDACTED]

a97. [REDACTED]

a98. [REDACTED]

[REDACTED] When there are a number of items awaiting disposal, CYC contacts [REDACTED]

a99. CYC's service contract [REDACTED] was provided for review. Prior to placing the contract, [REDACTED] site was inspected by senior staff from CYC. The subsequent contract was agreed following a trial of the service. This contract was the [REDACTED] standard contract and CYC reported that this met its requirements.

a100. Yorkcraft is a council service, although there is a SLA in place. However, this is dated 2010 and there is no evidence of any subsequent reviews despite the Agreement providing that it will be reviewed at quarterly intervals.

Recommendation: Ensure that the Yorkcraft SLA is periodically reviewed in line with review periods set out in the Agreement.

Management response: Accepted
CYC will review the Yorkcraft SLA and ensure ongoing reviews are conducted in the time periods subsequently set out.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st March 2016

a101. Yorkcraft provided copies of documentation confirming that [REDACTED] held an Environmental Waste Permit and a Certificate of Registration under the Environmental Regulations 2011.

a102. Yorkcraft demonstrated the Certificate of Destruction it receives from [REDACTED]. Yorkcraft also recently requested confirmation of [REDACTED] procedures to ensure that they were still in line with the original agreement and a copy of this response was provided for review.

a103. [REDACTED] provides CYC with access to its bespoke secure browser reporting system, [REDACTED]. [REDACTED]

[REDACTED] Certificates of destruction are also provided.

a104. Records management performance measures do not appear to have been formally identified. There was no

record of who had read the Records Management Policy and the policy did not detail how policy compliance is monitored.

Recommendation: Identify records management performance measures that reflect organisational needs and risks identified in the corporate risk management framework.

Management response: Accepted

CYC has updated the terms of reference for the IMB (replacing CIGG) and it includes records management monitoring and compliance. Work will now be done to determine what the key performance indicators are to reflect our needs and risks. These will be aligned to the risks identified for the corporate risk management framework.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st March 2016

a105. Yorkcraft's SLA does set timescales for delivery of its services and provides that reporting details will be produced. However, reporting details are not being produced.

Recommendation: Ensure that reporting details are being produced as required in the Yorkcraft SLA.

Management response: Accepted

CYC will review the Yorkcraft SLA and ensure reports are produced.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st March 2016

a106. It was reported that there have not been any recent records management audits. One audit report from 2014 was provided covering document management. This was

conducted because the Council had recently undertaken a major project to reduce the amount of business storage and documentation held within departments. It aimed to provide assurance to management that the controls put in place to manage key risks relating to the arrangements for the scanning and storage of documents at West offices and Hazel Court are effective. However, records management does not appear to routinely feature as part of the annual internal audit plan.

Recommendation: There should be periodic internal audits of the security and use of records, and formal reports issued to senior management.

Management response: Accepted

CYC will include this in the internal audit plan. Meeting arranged with internal auditors mid-November for this.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31 December 2015

a107. CYC provided the newest version of its Risk Management Policy and Strategy for review. It explains how risk is assessed, recorded and managed and sets out the risk reporting structure. The accompanying risk guide recognises information as a potential area of risk and data quality as a risk category. It was reported that the new policy was agreed at the Audit & Governance Committee on 29th July 2015. At the time of the audit, the new policy was due to go live within a couple of weeks.

a108. There is also an Information Security Incident Procedure in place although it is past its review date of May 2014. CYC's information security incident procedure is currently managed by Veritau. However, the Transparency and Feedback Team Manager is overseeing the process with Veritau as part of the staggered approach to transfer this to the council team.

Recommendation: Review the Information Security Incident Procedure and ensure that it is fit for purpose and in line with best practice.

Management response: Accepted

CYC have provided breach management training for 2 key staff and they are now underway with a review of the breach management process, procedures and training materials. This will take account of ICO codes of practices, exemplar organisations processes, etc and will also identify links to the Caldicott Guardian issues reporting process. The review will also include the development and delivery plan for training, guidance/toolkits, and key performance indicators and how to ensure lessons are learned from breach management reporting. Monitoring has been included in the new terms of reference for the IMB.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st January 2016

a109. CYC has identified its key corporate risks and information risk features within its governance risk. This risk is owned by the SIRO and mitigating controls have been identified.

a110. There is also a dedicated Information Governance Risk Register in place which was originally produced by Veritau but responsibility is being transferred to the Transparency and Feedback Team Manager. It is notable that 'recognition of and responding to requests for information' is highlighted as a risk but rated 'very low'. This is surprising considering CYC's subject access request compliance rates.

Recommendation: Review the IG Risk Register in line with the new Risk Management Policy and Strategy to ensure that risk ratings are correct.

Management response: Accepted

CYC will start the review of the IG risk register in mid-November to ensure it is in line with the new Risk Management Policy and Strategy.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st December 2015

a111. Departmental risk registers are also in place. The adult social care risk register does not identify information management as a risk and the security incident log does not highlight a large number of security incidents for this service. The Children's Social Care register includes 'breach of data protection leading to a fine or investigation' as a risk. The risk has a risk owner and mitigating controls are identified.

a112. It was reported that some IAOs (Information Asset Owners) may not realise that they have this responsibility as the roles have not been widely communicated across the Council and there has not been any specific training on the IAO role. Instead, nominated owners may assume that they have such responsibilities because they are a head of service, for example.

Recommendation:

- a) Assigned responsibility for IAO roles across CYC should be clearly communicated.
- b) IAOs should receive appropriate training to fulfil their roles.

Management response: Accepted

CYC is underway with reviewing the IAR and this will include identifying assigned IAOs and IAAs. This will then enable us to develop and deliver awareness, guidance and dedicated training for the IAOs and IAAs and a communications plan.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: (a) 31st March 2016 (b) 30 June 2016

a113. It was reported that CYC is also looking to nominate Information Asset Administrators (IAAs) to support IAOs. A draft template for the revised IAR was provided which showed a column to identify IAAs.

Recommendation: IAAs should be identified and nominated, as planned to support the IAO function, and should receive training as appropriate.

Management response: Accepted

CYC is underway with reviewing the IAR and this will include identifying assigned IAOs and IAAs. This will then enable us to develop and deliver awareness, guidance and dedicated training for the IAOs and IAAs and a communications plan.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30 June 2016

a114. Example data protection clauses for a Data Processor Contract were provided for review. The example clauses require providers to comply with Principle 7 of the DPA and provide CYC with the right to request a written description of the technical and organisational methods employed by the Provider and/or relevant Sub-Contractors at reasonable intervals. The example clauses do not however, provide CYC with a right of physical audit.

Recommendation: CYC should ensure that its Data Processor Contracts provide it with a right to physically audit its data processors' premises.

Management response: Partially Accepted

CYC will write a clause to be included in new tender documents to provide us with this right and for existing contracts. We will include this at the point of renewal.

Owner: Andy Docherty, Assistant Director

Date for implementation: 29th February 2016

7.2 Scope b: Subject Access Requests – There are appropriate procedures in operation for recognising and responding to individual's requests for access to their personal data.

Risk: Without appropriate procedures, there is a risk that personal data is not processed in accordance with the rights of the individual and in breach of the sixth principle of the DPA. This may result in damage and/ or distress for the individual, and reputational damage for the organisation as a consequence of this and any regulatory action.

b1. CYC is implementing a new council wide SAR process. This process is being led by the Transparency and Feedback Team Manager, and falls within the IG Action Plan 2015. Many SAR functions administered by Veritau are in the process of being handed over to the council team. The full set of functions are intended to be passed to the council team by the end of this calendar year. The new SAR process is still being developed. Further changes will be made to the process as the council team both develops and expands its role.

Recommendation: Finalise and implement the new SAR process.

Management response: Accepted

CYC is currently underway with a review of the SAR process, Access to Records policy, training material etc and will use this ICO report recommendations to further update where required. This review will include the writing of what will be required in the training packages, checklists/toolkits, templates and a communications plan.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st January 2016

b2. The Access to Records Policy and SAR checklist are in draft form. There is currently interim guidance for children's services and adult social care ('Interim Practice Guidance to Social Workers: Subject Access Requests'). We were also provided with the 'Business Support SAR Process for Children's Services' and a 'Business Support SAR flowchart'. These procedures will need updating to reflect the new SAR process.

Recommendation: Finalise the draft Access to Records Policy and SAR checklist. Update the 'Interim Practice Guidance to Social Workers: Subject Access Requests', 'Business Support SAR Process Children's Services' and 'Business Support SAR flowchart' to reflect the final SAR process.

Management response: Accepted

CYC is currently underway with a review of the SAR process, Access to Records policy, training material etc and will use this ICO report recommendations to further update where required. This review will include the writing of what will be required in the training packages, checklists/toolkits, templates and a communications plan.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st January 2016

b3. CYC's website provides guidance to individuals on making a SAR. This can be located by entering 'request for your personal data' or 'subject access request' in the search bar. This information could be made easier to locate. The information provided is a brief overview of how to make a SAR. A link to a SAR form is provided to assist individuals making a SAR. There is also a link to the 'Confidentiality and Access to Records Leaflet' advising individuals on housing and social care records. CYC is aware the website guidance needs updating to reflect the new SAR process, which should be in place by November.

Recommendation:

- a) Update website guidance to reflect the new SAR process, as planned.
- b) Make the SAR guidance on the website easier to locate.

Management response: Accepted

Following completion of the review of the SAR process and Access to Records policy, and as part of the communications plan being actioned, (a) the website pages will be updated and (b) easier access and search options will be investigated and put in place where possible.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st March 2016

b4. CYC provided an example of the contract clauses included in data processor contracts. The example contract clauses state that the data processor will notify CYC within 5 business days if it receives a SAR. The data processor is required to comply with a subject access request within the relevant timescales set out in the Data Protection Act and in accordance with the CYC's instructions. However, it is not clear if these clauses are included in all data processing contracts. Moreover, CYC believes it could further integrate data processors into the council wide SAR process. For example, data processors could be required to log receipt of the SAR with the council team.

Recommendation:

- a) CYC should review current data processing contracts to ensure they include the appropriate obligations regarding SARs. This should be included in all future contracts with data processors.
- b) Integrate third party SARs into the new SAR process to ensure adequate oversight.

Management response: Partially accepted

(a) CYC will undertake reviews of current data processing contracts at the time of renewal and (b) include the provision for 3rd party SARs within the review of the SAR process.

Owner: (a) Andy Docherty, Assistant Director

(b) Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: (a) to be determined by renewal timescales (b) 31st March 2016

b5. All SAR requests should be logged with the council team. The council team will check the validity of the SAR, establishing whether CYC is able to satisfactorily identify the requestor as the data subject. The council team previously passed the SAR to the relevant service area and recently this has been direct to the appropriate Head of Service.

b6. Business Support staff in children's services and adult social care have been locating personal data that has been requested since approximately autumn 2014. The unredacted material will then be considered for disclosure by social workers, who will withhold material where appropriate and a response is provided to the requestor.

b7. Advice on redaction and exemptions is currently provided by Veritau where requested, although this function will be passed to the council team by end of this calendar year. The council team intends to validate all requests upon receipt. It was reported that it will then quality check a random sample of responses as part of a compliance monitoring system that it is introducing across information governance.

Recommendation: Implement quality assurance procedures through the council team for all SAR responses as proposed.

Management response: Accepted

CYC is currently underway with a review of the SAR process, Access to Records policy, training material etc and will include how the CYC team will quality assure/check SAR responses and how this will be reported. The new IMB will be responsible for monitoring and compliance.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st March 2016

b8. The 'Interim Practice Guidance to Social Workers: Subject Access Requests' was issued a week before our onsite visit. Therefore, staff will not yet be fully aware of the new procedures. This guidance appears to relate to children's services and not adult social care.

Recommendation: Raise awareness of the 'Interim Practice Guidance to Social Workers: Subject Access Requests' amongst all relevant staff/teams.

Management response: Accepted

CYC team will continue to raise awareness and provide guidance to relevant teams and staff.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30th November 2015

b9. CYC does not currently have council wide training in place for SARs. Without training some staff may not be able to recognise a SAR. Moreover, social workers in children's and adult social care typically respond to SARs. Whilst the staff interviewed had experience in responding to SARs, they did not appear to have received any specific training for their role. CYC has recognised the need to develop SAR training across the council. The Customer Feedback & Complaints Manager has a data protection qualification and has completed a 'train the trainer' course. This expertise will be used to assist in the development of council wide and role specific SAR training.

Recommendation: As proposed, develop council wide training for staff so staff can recognise a SAR. Conduct training needs analysis of staff involved in the SAR process and provide role specific training where appropriate.

Management response: Accepted

CYC will include this training needs analysis in with that being done for records management, IAOs, IAAs etc. Training packages are being developed which will include induction and refresher awareness, and more role and responsibility specific training packages. Delivery will be using the most appropriate method e.g. Icomply, elearning or classroom.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30 April 2016

b10. A brief overview of SARs is available on the staff intranet. This guidance will need updating to reflect the new SAR process.

Recommendation: Update guidance available on staff intranet to reflect new SAR process.

Management response: Accepted

CYC will update intranet guidance when SAR process and Access to Records policy reviews are completed.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30 April 2016

b11. We were advised that CYC has made use of ICO posters to raise awareness of SAR requests throughout West Offices.

b12. The council team checks the validity of the requestor's SAR, ascertaining whether the requestor is able to satisfactorily identify themselves as the subject of the data requested. The council team also ensures that there is

enough information to locate the personal data. Services double check the requestor's identity.

b13. When a request is made by a third party on the data subject's behalf, CYC checks its validity. In the case of parent applicants, the Council team checks whether the parent is entitled to the information or whether the child is competent enough to understand their rights to their own information.

b14. Staff interviewed had a good awareness of issues such as consent and capacity. However, the Business Support SAR flowchart and 'Interim Practice Guidance to Social Workers: SARs' states that where a child is under 12 years old the request is required to be made by a parent or person with legal authority to act on their behalf. Whilst it is reasonable to assume most children will not have capacity if under 12 years, there may be exceptions.

Recommendation: Where appropriate, staff should consider whether children have capacity to independently request a SAR.

Management response: Accepted

CYC will include this in SAR process and Access to Records policy guidance, training and published on the intranet. However if advice sought verbally whilst this work is underway, the CYC team will give this.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30 April 2016

b15. CYC does not charge a fee to process SAR requests. This gives the public free access to their personal data.

b16. We were advised that the council team send a letter/email to the SAR requestor acknowledging receipt.

This acknowledgment informs the requestor when the response must be provided.

b17. The council team has a system called Respond which logs SARs received by CYC. This system records pertinent information such as date received; date due; reminders sent to services; and date completed.

b18. We were shown a further spreadsheet held by the Business Support staff in children's services which recorded broadly similar information to the council team's Respond, with a greater service level focus. With respect to adult social care, we were advised that they maintain a similar spreadsheet on the adult social care network drive and a notation is made within Frameworki (their case management system) of all actions relating to any SAR request.

b19. The council team does not routinely record information about what personal data has been withheld in response to a SAR on Respond. However, the council team holds some scanned correspondence and recorded interactions between themselves, the services, and the requestor, which sometimes contains such information. The routine recording of this information would facilitate the planned quality checking function of the council team and help the council team process any complaints.

Recommendation: The council team should routinely record what information (if any) is withheld under exemption or relating to third parties and the basis for withholding the personal data.

Management response: Accepted

CYC is currently underway with a review of the SAR process, Access to Records policy, training material etc and will use this ICO report recommendations to further update where required. This review will include the writing of what will be

required in the training packages, checklists/toolkits, templates and a communications plan.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st January 2016

b20. The 'Interim Practice Guidance to Social Workers: Subject Access Requests' does not state that Social Workers should contact the requestor in the event of delay. However, it may be the case that this is done in practice.

Recommendation: Formalise the requirement for staff to promptly contact the SAR requestor in the event of delay. In such cases, CYC should explain to the requestor the reason for the delay and the expected date for response.

Management response: Accepted

CYC is currently underway with a review of the SAR process, Access to Records policy, training material etc and will use this ICO report recommendation to further update where required. This review will include the writing of what will be required in the training packages, checklists/toolkits, templates and a communications plan.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st January 2016

b21. The council team will send a reminder to the service(s) when a SAR is 30 days old. They will send subsequent chasers just before the SAR is due, on the day it is due, and if it is late. The council team has recently started to routinely include the Heads of Service/ Assistant Directors/ Directors in chaser emails for overdue SARs. We were advised that the Head of Service SAR chaser email is not formalised in procedural guidance. The council team is also considering implementing a form that can be sent to the service(s) to establish why the SAR is overdue, get an

update on progress, and know when the SAR is likely to be finished.

Recommendation: Record the formal process for chasing departments for SAR responses and escalating to Heads of Services when overdue. This process should look to identify why the SAR is overdue, current progress, and when it is likely to be finished.

Management response: Accepted

CYC will include this in the SAR process and monitoring reports will go to the IMB to monitor compliance.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st January 2016

b22. Staff interviewed did not report any specific problems in locating manual records. However, they did report that the maintenance of the records (e.g. reliable indexes, file contents pages, descriptions of documents) were inconsistent within and across services. This can hinder locating the personal data relevant to a SAR.

Recommendation: Ensure any new manual records are maintained to a good standard. Where practicable, take steps to improve any older files that have been poorly maintained.

Management response: Accepted

CYC will undertake to develop good standards for manual records in line with the work being done in Adults and Children's Social Care case management system improvements and linked to recommendations made for records management in this audit report.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30 June 2016

b23. It was also reported that Business Support staff are able to effectively interrogate and retrieve the personal data from Raise and Frameworki. We note that CYC is currently in the process of upgrading these case management systems to the Mosaic system.

b24. Business Support does not keep a record of the searches made to locate personal data. Having a record would assist CYC in reviewing instances where the requestor does not believe they have received all their personal data.

Recommendation: Keep a record of the searches made to locate personal data in response to a SAR.

Management response: Accepted

CYC is currently underway with a review of the SAR process, Access to Records policy, training material etc. and will use this ICO report recommendations to further update where required. This review will include the writing of what will be required in the training packages, checklists/toolkits, templates and a communications plan.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st January 2016

b25. We were informed that children's services retain both a redacted and unredacted copy of their SAR responses. Adult social care retains a copy of redacted SAR responses. It is unclear whether adult social care retains an unredacted copy of the response. Retaining these copies will allow CYC to respond to queries from the requestor or the ICO about withheld personal data.

Recommendation: Ensure that adult social care retains an unredacted copy of the SAR response.

Management response: Accepted

CYC is currently underway with a review of the SAR process, Access to Records policy, training material etc. and will use this ICO report recommendations to further update where required. This review will include the writing of what will be required in the training packages, checklists/toolkits, templates and a communications plan.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st January 2016

b26. Adult social care retains SAR responses for up to one year. It is not clear if this is a stated retention period, or if it is customary. Children's services will retain the unredacted and redacted documents for the SAR, subject to the normal file retention criteria for the child's case file.

Recommendation: Ensure there are appropriate retention periods for unredacted and redacted SAR responses.

Management response: Accepted

CYC will include this in the Access to Records policy, guidance, training and also publish on the intranet. However if advice sought verbally whilst this work is underway, the CYC team will give this.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st January 2016

b27. Redaction has previously been carried out manually by children's and adult social care. We were informed that these services are in the early stages of rolling out electronic redaction, using Adobe Professional. It was reported that the council team also uses this software.

b28. Previously, redacted adult social care SAR documents were stored at Yorkcraft with no retention dates assigned. It is unclear if any of these SAR documents, which

are now beyond the current 12 month destruction date, are still being held at Yorkcraft.

Recommendation: Ensure Yorkcraft securely destroy SAR responses in line with retention periods.

Management response: Accepted

CYC will include the requirement for a checking process at Yorkcraft for destruction of SAR responses in line with the current checking process they have for destruction of other stored records.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st January 2016

b29. Veritau is currently contracted to provide advice on exemptions and redactions to CYC staff. It was reported that the most common query from staff was about redaction of third party information. This function will be passed to the council team by the end of this calendar year. We were advised that the council team currently provide initial advice to staff about exemptions and redactions when passing the SAR to the service(s), with the advice tailored to the request and service area as appropriate.

b30. There does not appear to be any formal written guidance to help staff exempt and redact information. This would improve staff understanding and reduce the number of straightforward queries regarding exemptions and redactions made to Veritau, and in future the council team.

Recommendation: Support the advice function provided by Veritau, and in future the council team, with written guidance on exemptions and redactions.

Management response: Accepted

CYC is currently underway with a review of the SAR process, Access to Records policy as well as training and guidance

material required which includes exemptions and redacting information. Delivery of awareness and role –specific training will be delivered using a variety of methods such as induction and refresher sessions, Icomply, elearning and classroom based. However if advice sought verbally whilst this work is underway, the CYC team will give this.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30th June 2016

b31. The 'Interim Practice Guidance to Social Workers: Subject Access Requests' states that the "allocated Social Worker for the Subject Access Request must review the unredacted personal data and use professional judgement to apply the statutory legislation and guidance relating to what should and should not be disclosed to the Applicant". Whilst the document does refer to ICO guidance, it does not mention contacting either Veritau, or in future, the council team for advice where required.

Recommendation: Amend practice guidance to advise staff to contact either Veritau or the council team for SAR advice when required.

Management response: Accepted

CYC is currently underway with a review of the SAR process, Access to Records policy as well as training and guidance material, which will include contact information for advice and support. However if advice sought verbally whilst this work is underway, the CYC team will give this.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30th April 2016

b32. We were advised that social workers will informally check each other's SAR responses and also check with managers. Whilst this is beneficial, having a formal quality

assurance process in place at service level, by the council team as proposed, will promote consistency.

b33. There are no template covering letters for SAR responses. The covering letters reviewed did not include information specified in section s7 (1) (b) of the DPA, which is a description of how their personal data is being used and to whom it may be disclosed, nor the searches undertaken to locate the personal data. Some covering letters clearly explained the reason(s) for redacting information, others did not. We were advised that there may be some standard material used in adult social care for SAR responses, and a number of interviewees believed that developing this material would be beneficial.

Recommendation: Issue guidance and template letters/paragraphs to assist staff in their response to the data subject. This should include a description of how data subjects' personal data is being used and to whom it may be disclosed, an explanation of the searches undertaken to locate their personal data, and where appropriate, an explanation as to why information has been redacted or exempted.

Management response: Accepted

CYC is currently underway with a review of the SAR process, Access to Records policy as well as training and guidance material. This will include a suite of template responses for SARs. However if advice sought verbally whilst this work is underway, the CYC team will give this.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30th April 2016

b34. SAR responses are not marked 'data subject copy' before release. Such marking may help identify the source of any further disclosure of the information, should the need arise.

Recommendation: Consider marking SAR responses 'data subject copy' before release.

Management response: Accepted

CYC will include the requirement for a marking process in the review of the SAR process and Access to Records policy as well as include in the review of the data protection policy where relevant.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st January 2016

b35. We also asked whether individuals can view their SAR response onsite if they requested. CYC advised that they can arrange onsite viewing.

b36. There is currently no systematic reporting of SAR performance and complaints to the CIGG and other relevant groups. The Transparency and Feedback Team Manager is aware of this matter and plans to introduce regular reporting to the CIGG, Management Team and Councillor Corporate Management Team. The proposed reports will highlight key themes to help identify systemic issues and any lessons that can be learned from complaints. The Transparency and Feedback Team Manager would also like SAR performance information to be reported through the Strategic Business Intelligence Hub and be added to the CYC dashboard and/ or made available publicly via website or York Open Data Platform. We note the Respond system is currently capable of producing a range of reports on SAR performance.

Recommendation: Introduce regular reporting of SAR performance and complaints to the CIGG or other relevant groups as proposed. Ensure that issues are acted upon accordingly.

Management response: Accepted

CYC has completed the review of the CIGG terms of reference which will now be the Information Management Board (IMB) and includes monitoring and compliance, in its purpose, aim, remit and objectives. The first meeting is planned for mid-November at which the standard agenda items, such as KPI reporting, will be approved.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st December 2015

b37. Between 1st April 2014 and 31st March 2015, CYC recorded receipt of 131 SARs. 67 of these requests were complied with in the statutory timescale, which is compliance rate of 51.1%. This is extremely low. We understand that CYC intend to introduce a target compliance rate of 100%, once responsibility for this function passes fully to the council team.

Recommendation: Introduce and regularly monitor an appropriate target rate for SAR compliance, as planned. See also b36.

Management response: Accepted

The SAR report for 1st April 2015 to 31st August 2015 shows 30 SARs received, 25 responded to in time and 5 out of time, which is a compliance rate of 83.3%.

Reporting of KPIs will be through the new IMB and will include SAR compliance. The first meeting is planned for mid-November.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st December 2015

b38. The Transparency and Feedback Team Manager intends to produce management information on SAR performance that will show the performance of specific services, to help identify any specific issues affecting overall compliance.

Recommendation: Produce management information on SAR compliance which can demarcate performance at the service level, as planned.

Management response: Accepted

Reporting of KPIs will be through the new IMB and will include SAR compliance rates both for the whole council and by service. The first meeting is planned for mid-November. Also the review of the SAR process will include points during the 40 day timescale to provide opportunities for early identification of issues.

Owner: Lorraine Lunt Transparency & Feedback Team Manager

Date for implementation: 31st December 2015

b39. It was reported that whilst a large amount of SAR requests go through the council team there may be some SARs that are not being passed to the council team from the services.

Recommendation: Raise awareness amongst staff that the new process requires all SAR requests go to the council team in the first instance.

Management response: Accepted

CYC has conducted an awareness campaign for SARs using a variety of methods e.g. staff email, staff newsletter, display screens in staff hub areas and posters on all staff noticeboards.

The current review of the SAR process and Access to Records policy will include opportunities for further ongoing awareness.

Owner: Lorraine Lunt Transparency & Feedback Team Manager

Date for implementation: 31st January 2016

b40. Complaints regarding the handling of SARs are logged by the council team on the Respond system. They

are then passed to Veritau. The Veritau Information Governance Team will review the complaint and advise CYC accordingly. The complaints handling role of Veritau will be passed to the council team by the end of this calendar year.

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.

c1. CYC recently entered the Multi-Agency Information Sharing Protocol (MAISP). This agreement is currently between North Yorkshire County Council, City of York Council, North Yorkshire Fire and Rescue Service, and North Yorkshire Police (the ‘protocol partners’).

c2. The MAISP is the principal high-level agreement used by CYC, setting out common data sharing rules to be followed by protocol partner agencies. This includes the aims & objectives of MAISP, general principles, information covered by MAISP, organisational & individual responsibilities, restrictions on the use of information shared, obtaining consent, security arrangements, information management, data sharing training, and protocol review arrangements. Going forward, the MAISP will also inform other ISAs used by CYC.

c3. The Draft MAISP Implementation Strategy outlines CYC’s new approach to ISAs. Existing ISAs will remain unchanged until they become ready for review. After review, agreements with all protocol partners must comply with the MAISP. New arrangements with other partner agencies and existing ones at review must be informed by the MAISP.

Recommendation: Finalise and action the MAISP Implementation Strategy, and align existing ISAs to MAISP requirements, as planned.

Management response: Accepted

The MAISP has been published on the CYC intranet and further progress of the final MAISP implementation strategy is underway. The MAISP information sharing template is also published on the intranet and has been used for new arrangements. Using the IAR monitoring process, CYC will be able to identify a schedule for review of ISAs which will include alignment with MAISP for relevant ISAs.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30 June 2016

c4. The MAISP Data Sharing Template provides the structure for an ISA between partner agencies. The template requires a signature from each party. Having reviewed the MAISP, Draft MAISP Implementation Strategy, and MAISP Data Sharing Template, there does not appear to be an explicit written requirement for an ISA to be signed off by a senior member of staff.

Recommendation: Ensure all ISAs are signed off by an appropriately senior member of staff.

Management response: Accepted

CYC has highlighted this at the MAISP group and there has been an agreement to consider making any relevant amendments to the MAISP from the recommendations. CYC is also underway with the review of data protection policy and processes which include the development of a toolkit for completing ISA e.g. request and decision templates, ISA templates, checklists etc and training and guidance will be provided to those with ISA responsibilities.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st March 2016

c5. The MAISP states that decisions about whether to share information or not and the reasoning behind them should be recorded. If personal data is shared, the partner agency should record exactly what data was shared, with whom and for what purpose. A draft communication for staff about MAISP instructs staff to record data sharing decisions. However, this requirement has not been embedded across CYC. Moreover, the routine recording of data sharing decisions should be recorded in all cases, irrespective of whether they fall under the MAISP.

Recommendation: Embed requirement to record the reason for all data sharing decisions at CYC.

Management response: Accepted

CYC is underway with the review of data protection policy and processes which include the development of a toolkit for completing ISA e.g. request and decision templates, ISA templates, checklists etc. and training and guidance will be provided to those with ISA responsibilities.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st March 2016

c6. We were advised that in instances where personal data is shared/ received by the council, it is routinely recorded in the Housing Benefits and Local Council Tax departments. Typically, this will be recorded on the services' case management systems. An example of this would be information shared with DWP, where CYC have direct access to the DWP system to process benefits information.

c7. CYC has not carried out any corporate level training needs analysis for staff making decisions about data sharing. Generic and role-based training needs analysis is important to ensure personal data is shared correctly.

Recommendation: Conduct generic and role-based training needs analysis for all staff sharing personal data at CYC. Deliver appropriate training, including refresher training, thereafter.

Management response: Accepted

CYC will link this with the identification of other local records management and data protection role specific responsibilities, and include it in the training/ learning/development mandatory framework including induction, targeted dedicated sessions aligned to local or role specific responsibilities, and refreshers as well as the PDR process. This means that progress of TNA will be aligned to the timescales for training development and delivery.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30th June 2016

c8. The MAISP states that appropriate employees are provided with the training that accompanies MAISP. We understand this e-training is not yet available. The protocol does allow CYC to develop equivalent training. We were advised that CYC has made use of the ICO data sharing checklists and data sharing flowcharts in the MAISP. The Draft MAISP Implementation Strategy states that specific additional training will be required for data sharing. A Communications/ Training & Support Schedule is included in the Draft MAISP Implementation Strategy. This includes a requirement for e-learning training for all CYC staff.

c9. We were advised that Housing Benefits and Local Council Tax departments have data sharing training, including training for the Public Service Network for individual assessors. We understand they have their own dedicated training officer. Staff are also required to undertake systems training when accessing the DWP system for benefits.

c10. The MAISP sets out individual responsibilities for those who share data. This includes validating authorisation before disclosing information and upholding the general principles of confidentiality. These responsibilities should be communicated to staff.

Recommendation: Communicate individual responsibilities set out in MAISP to relevant staff.

Management response: Accepted

CYC has published the MAISP on the intranet. CYC team has already advised on responsibilities to those services/ areas/ staff who have requested advice on information sharing. Further roll out is planned as set out in the MAISP implementation strategy which will be amended and finalised from the draft version provided during the audit.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st December 2015

c11. A draft communication for staff about MAISP provides guidance to staff on decisions to share information. The guidance appears to focus on when children or adults are at serious risk of harm. But the guidance can be applied generally.

c12. The Data Protection Policy outlines both routine and one-off data sharing. However, the policy was published in 2008, and needs updating. For example, it does not mention MAISP.

Recommendation: Update the data sharing elements of the Data Protection Policy.

Management response: Accepted

CYC will include this in the review underway of the data protection policy.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 29th February 2016

c13. CYC does not have a comprehensive up-to-date suite of policies, procedures and guidance that clearly set out who has the authority to make decisions about systematic sharing or one-off disclosures, and when it is appropriate to do so.

Recommendation: Develop a comprehensive up-to-date suite of policies, procedures and guidance for data sharing.

Management response: Accepted

CYC is underway with a review of full suite of policies and processes, training packages, guidance, checklists, toolkits, templates, monitoring and compliance reporting (with KPIs and targets) which includes data sharing.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30th June 2016

c14. The YorOK website is maintained by York Family Information Service, which is part of CYC. It provides processes and common tools for data sharing to be used amongst various practitioners working to help children and young people.

c15. We were provided with many examples of where fair processing information is provided to data subjects regarding data sharing (unless an exemption applies). Interview feedback suggested that there were some examples of good practice across CYC. For example, the Family Focus Leaflet explains why, how, and with whom an individual's personal data will be shared. We also understand that a lot of fair processing information is given out over the phone.

c16. The MAISP explains the importance of privacy notices and the need to regularly update them. The protocol also provides a link to the ICO Privacy Notices Code of Practice.

c17. Where necessary, fair processing information is actively communicated to individuals and consent is sought. Examples of this can be seen in the Funding Application Form, the Troubled Families initiative, and Housing Benefit and Local Council Tax Support Form.

c18. CYC is in the early stages of introducing Privacy Impact Assessments (PIAs) council wide. This forms part of the IG Action Plan 2015. The Project Manager for Transformation has produced a draft Project Management Approach. This requires PIAs to be done in the project planning phase. It also refers to the ICO PIA Code of Practice. We were also provided with a PIA process map, draft PIA Briefing (version 2), and PIA screening questions & template (version 2). The Transparency & Feedback Team Manager intends to link the PIA issues and risks to the project risk register and/or the corporate risk registers which means they will be aligned to the Risk Management Policy. However, CYC do not have a specific PIA Policy which would further support the PIA process.

Recommendation: Finalise the draft Project Management Approach, and associated documents. Develop a specific policy for PIAs. See also c13.

Management response: Accepted

CYC will finalise the draft PM approach and associated documents. CYC will finish development of a PIA policy which will include the current PIA toolkit and guidance material and updating the information available on the intranet.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st December 2015

c19. The MAISP discusses the legal basis for sharing personal data and has a detailed appendix listing the legal basis for sharing personal data.

c20. We were advised that requests for advice on disclosing information are currently managed by the council team. The matter may then be passed to Veritau to provide further advice if necessary. Otherwise, advice requests are dealt with by the council team. We understand this full function is being transferred in house to the council team by the end of this calendar year on a staggered basis.

c21. Awareness of PIAs exists within CIGG, ICT, and the Project Transformation Team. This has been supported by communications to ICT and the main project team and the production of draft guidance on incorporating PIAs into the project management process. But as the guidance is in draft form it has not yet been cascaded throughout CYC. We note ICT will advise services about the need for PIAs through their involvement in projects and/ or service requests for significant changes to systems.

Recommendation: Cascade PIA requirements and guidance throughout CYC, once finalised.

Management response: Accepted

CYC is underway with the cascading of PIA requirements and guidance, by publishing on the intranet and provision of advice and support in conducting PIAs. PIAs will be monitored via the IAR and the IMB.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st December 2015

c22. We were provided with an initial PIA that ICT carried out for the Doqex file sharing application currently in development. It was reported that it will be up to individual service areas to assess if they need to carry out a further PIA

to identify any potential risks specific to their proposed use of Doqex, which are not covered by those identified by ICT in the PIA for Doqex. When registering to use the Doqex service, services will be prompted to assess whether they need to carry out a PIA and if necessary to seek advice from the Transparency & Feedback Team Manager.

Recommendation: Ensure PIAs are carried out for individual applications of Doqex, as planned.

Management response: Accepted
CYC is underway with the further PIA requirements for Doqex.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager
Transparency & Feedback Team Manager.

Date for implementation: 31st December 2015

c23. The ISAs provided that predate the MAISP were of a reasonable standard and did not present any significant concerns.

c24. We could not evidence any current governance arrangements at CYC to systematically review ISAs to ensure partner organisations are removed from or added to agreements when required, and to regularly examine the working of and ongoing necessity for, the agreements.

Recommendation: Establish governance arrangements at CYC to systematically review ISAs.

Management response: Accepted
CYC will include this in the IAR monitoring process and has included the monitoring/compliance in the new terms of reference for the IMB.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st December 2015

c25. The MAISP has an established cross-county Information Governance Monitoring Group which will meet at least annually. This would be a good forum to review the membership and workings of MAISP. The terms of reference for this group have not yet been formalised. We were also advised there is a MAISP "Information Sharing Quarterly Review" and all partners are invited to attend. The next meeting is 22 September 2015.

Recommendation: Formalise the terms of reference for the MAISP cross-county Information Governance Monitoring Group. Ensure the MAISP cross-county Information Governance Monitoring Group and/or MAISP "Information Sharing quarterly review" group periodically review the membership and workings of MAISP.

Management response: Accepted
The terms of reference for the MAISP being formalised and the comment regarding incorporating periodic review of the membership and workings of MAISP by the relevant group, was raised at the September meeting. This will be formalised at the next relevant meeting.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st January 2016

c26. The ISA between York Youth Offending Team and CYC states when the agreement will be reviewed and by whom. It was also evidenced that there will be an annual review throughout the life of the Troubled Families Programme within CYC and a review whenever amended guidance is received from the DCLG.

c27. There is no central list of ISAs, and it was reported that there is no complete schedule of ISAs in adult social care, or other service areas. This raises the risk of a lack of corporate or departmental awareness of the number and nature of data sharing activities in place. We understand the

Transparency & Feedback Manager plans to develop the Information Asset Register to include this information.

Recommendation: Develop service level and a central, register of all ISAs, which detail the nature of the sharing, authorisation, and the partners. This should include information about the legal basis for data sharing.

Management response: Accepted

CYC is underway with implementing a register of all ISAs using the IAR process and the development of data sharing request and decision templates.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st January 2016

c28. From the evidence provided and interviews held there is limited evidence of corporate quality controls in place to ensure the data shared is of appropriate quality and is not retained for longer than necessary by all parties. We were also advised that it is difficult to find information about data quality in existing policies.

Recommendation: Ensure there are corporate controls in place to ensure the data shared is of appropriate quality and is not retained for longer than necessary by all parties. This requirement should also be reflected in relevant policies and guidance.

Management response: Accepted

CYC will include the requirement for controls for quality within both the review of the data protection policy and processes and records management policy and processes.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 29th February 2016

c29. Data minimisation is not mentioned explicitly in MAISP. But it is included within the relevant legislation appendix of the MAISP under the Data Protection Act.

Recommendation:

- a) Update MAISP to explicitly discuss the requirement that shared data is minimised to agreed data sets or redacted.
- b) Ensure ISAs, relevant policies and guidance include the requirement that shared data is minimised to agreed data sets or redacted.

Management response: Accepted

(a) This recommendation will be shared at the next relevant MAISP group meeting

(b) CYC will include this requirement within the review of the relevant policies and processes.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 29th February 2016

c30. In line with data protection requirements, shared data should clearly distinguish between fact and opinion. We were advised that Housing Benefits and Council Tax staff are trained to focus on the facts when recording personal data. Furthermore, the Strategic Business Intelligence Hub - Data access, recording and security policy requires information recorded to be factually accurate. However, there does not appear to be any common guidance on this across CYC.

Recommendation: Issue common guidance to CYC about clearly distinguishing between fact and opinion when recording personal data.

Management response: Accepted

CYC will update existing guidance where required and include in the relevant policy and processes reviews e.g. as part of the development of training materials and packages.

Owner: Lorraine Lunt Transparency & Feedback Team Manager

Date for implementation: 29th February 2016

c31. The sender of personal data should inform recipients when shared personal data has been amended or updated. There was limited evidence that this was being done consistently in CYC.

Recommendation: Ensure that where appropriate, the sender informs recipients when shared data has been amended or updated.

Management response: Accepted

CYC will update existing guidance where required and include in the relevant policy and processes reviews e.g. as part of the development of training materials and packages.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 29th February 2016

c32. We were advised that Housing Benefits has a quality assurance role which checks 4% of Assessors work each day. This will include information shared with DWP and other organisations. This will identify any accuracy issues (e.g. financial and procedural).

c33. We understand that adult social care has spent a large amount of time assessing the accuracy of its electronic records held on Frameworki. This is part of the data migration process for the upcoming switch to their new system Mosaic.

c34. The MAISP requires that in ISAs, partner agencies establish specific arrangements for retention and disposal of information for all parties involved, including details of the exact arrangements for the transfer, storage and destruction of data where required. The ISA between York Youth

Offending Team and CYC includes retention and destruction procedures for shared data. However, retention and destruction details do not appear to be routinely included in other ISAs.

Recommendation: Ensure common retention and disposal arrangements are included in all ISAs and that these are adhered to by all parties to any given ISA.

Management response: Accepted

CYC will include the requirement for retention and disposal arrangements to be included in all new ISAs and be part of the review for existing ISAs. The IAR process will enable monitoring of this.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 30th June 2016

c35. CYC use secure systems such as GCSx and PSN to transfer personal data to other organisations (e.g. benefit information to the DWP). CYC were also accredited with the NHS Information Governance Toolkit for the previous year.

c36. The MAISP states that specific security arrangements for ISAs should be detailed in the Partner Agency Information Sharing Arrangements, which should be periodically reviewed to ensure that security arrangements are appropriate and effective. However, it is not clear to what extent ISAs and supporting procedures set out how personal data will be shared, e.g. recorded post; encrypted email; secure file transfer protocol (SFTP) etc.

Recommendation: Ensure that all ISA and supporting procedures set out specifically how personal data will be shared securely.

Management response: Accepted

The partner information sharing agreement template in the MAISP has a section to detail how information will be shared at section 7. CYC has included this in the development of the data sharing request and decision templates. It will also be reflected in the review of the data protection policy and processes, training material etc.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 29th February 2016

c37. CYC is planning to implement a secure file sharing service called Doqex, which staff can use to securely share files with internal and external parties. This would be another option to those mentioned in finding c36 especially when the files are very large. We were advised that the system is fully auditable, files are automatically encrypted when loaded into Doqex and there is an option to set a share password (for non CYC Doqex account holders) which is sent via text (separate to the emailed download link) to the recipient. This project is still in the early trial stages and has not been rolled out council wide.

c38. The MAISP states that access to the shared personal data will be detailed in the Partner Agency ISAs. However, there was limited evidence that access to data was detailed in all ISAs (both MAISP and non-MAISP).

Recommendation: ISAs should ensure that access to shared personal data is restricted to authorised personnel within each organisation where possible, on the basis of business need, e.g. a nominated point-of-contact.

Management response: Accepted

CYC will include this requirement in the review of the data protection policy and processes, training material etc. and in the data sharing request and decision templates.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 29th February 2016

c39. It was apparent from the interviews that staff were mindful of ensuring personal data was only disclosed on a need to know basis.

c40. CYC has a system for reporting potential security incidents. This includes incidents involving data sharing.

c41. We were provided with an example of data processor contract clauses used by CYC. Whilst they clearly set out the various security requirements required from a data processor, they do not explicitly require the data processor to notify CYC in the event of a potential data security breach.

Recommendation: Include a clause in data processor contracts requiring them to notify CYC of any data security breaches.

Management response: Accepted

CYC will write a clause to be included in new tender documents to provide us with this notification and for existing contracts. We will include this at the point of renewal.

Owner: Andy Docherty, Assistant Director

Date for implementation: 29th February 2016

c42. CYC does not have a corporate policy on disclosing personal data to third parties. This would help ensure a consistent standard was applied to disclosure decisions council wide.

Recommendation: Develop a policy for disclosing personal data to third parties. This should be communicated to staff and updated regularly.

Management response: Accepted

CYC is underway with a review of the data protection policy and processes (and Access to Records policy) which will include provision for disclosing to 3rd parties. This will be reflected in training packages and guidance.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 29th February 2016

c43. CYC has some guidance for staff considering requests from North Yorkshire Police (NYP). We were provided a RIPA Protocol between CYC and NYP. We were also provided a Section 29 template form to be used by NYP when requesting information from CYC.

c44. We were provided with some evidence that decisions to disclose information to third parties is logged by some teams and services. This includes the RIPA Protocol between CYC and North Yorkshire Police. But given the amount of teams and services it is difficult to establish a full picture. We do note the Draft MAISP Communication tells staff to record data sharing decisions.

c45. However, there is no council wide log or register of third party disclosures (in most cases disclosures relate to section 29). The Transparency & Feedback Team Manager and the Customer Complaint and Feedback Manager have advised that the council team is able to log third party requests and disclosures on their Response system.

Recommendation: Establish a central register for information requests from third parties. This should record the steps taken to identify the nature of the disclosure, the requester and the reason for any disclosure.

Management response: Accepted

CYC will create a central register for third party information requests as part of the review of the data protection policy and processes. This will be created and managed using the

case management system currently used for FOI, EIR, SAR etc. enquiries.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 31st December 2015

c46. There was limited evidence that third party disclosure decisions were quality assured or approved by appropriate staff.

Recommendation: Ensure third party disclosure decisions are quality assured and/or approved by appropriate staff.

Management response: Accepted

CYC is underway with a review of the data protection policy and processes which will include provision for quality assurance monitoring. Quality assurance monitoring will include the checking of appropriate approvals for disclosure decisions to third parties.

Owner: Lorraine Lunt, Transparency & Feedback Team Manager

Date for implementation: 29th February 2016

c47. CYC provides the York Open Data website. The website provides hundreds of up-to-date, searchable, open source datasets for organisations, with the aim of benefitting the local area.

c48. CYC was one of five local authorities that received top marks from an independent innovation charity NESTA, for the York Open Data platform.

c49. It was reported that CYC ensure any data published on the York Open Data Platform is completely anonymised. Prior to publication, all personal data is analysed and anonymised by CYC. The personal data is kept on a secure server and is then sent in its anonymised form to Castlegate IT, for publication. The exception to this would be

anonymised data taken from external websites. It was confirmed that if there were concerns about releasing information that could be personally identifiable, it would not be published.

- 7.4 The agreed actions will be subject to follow up to establish whether they have been implemented.
- 7.5 Any queries regarding this report should be directed to Stephanie Blears, Engagement Lead Auditor, ICO Good Practice.
- 7.6 During our audit, all the employees that we interviewed were helpful and co-operative. This assisted the audit team in developing an understanding of working practices, policies and procedures. The following staff members were particularly helpful in organising the audit:

Lorraine Lunt, Transparency & Feedback Team Manager.

Appendix A

Detailed findings and action plan

Action plan and progress

Recommendation	Agreed action, date and owner	Progress at 3 months Describe the status (complete/ partially complete/ not started) and action taken.	Progress at 6 months Describe the status (complete/ partially complete/ not started) and action taken.
<p>a5. Ensure that the job description for the Transparency and Feedback Team Manager accurately reflects the newly assigned responsibilities for information governance, incorporating records management. There should be a clear distinction between post holders with strategic responsibility and post holders with operational responsibility for the records management function.</p>	<p>Management response: Accepted CYC will review current job description to ensure clarity for strategic and operational responsibilities for records management.</p> <p>Owner: Andy Docherty, Assistant Director</p> <p>Date for implementation: 31st December 2015</p>		
<p>a9. Assign local records management responsibilities in line with the requirements of the Records Management Policy.</p>	<p>Management response: Accepted CYC will identify and assign local records management responsibilities in line with the reviewed/updated Records Management Policy.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation:</p>		

<p>a12. Ensure that records management features regularly on the CIGG agenda to mandate and monitor records management improvements.</p>	<p>30th June 2016</p> <p>Management response: Accepted CYC has completed the review of the CIGG terms of reference which will now be the Information Management Board (IMB) and includes records management including monitoring and compliance, in its purpose, aim, remit and objectives. The first meeting is planned for mid-November at which the standard agenda items will be approved.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st December 2015</p>		
<p>a14. Implement a records management programme of work and ensure that records management actions/ improvements and lessons learned are identified and implemented as necessary. This programme should be overseen by the CIGG.</p>	<p>Management response: Accepted CYC will develop a records management forward work programme. The IMB is to be responsible for records management monitoring and compliance as stated in the Terms of Reference</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st</p>		

<p>a15. Ensure that the Records Management Policy outlines methods for monitoring policy compliance and that this is communicated to staff.</p>	<p>March 2016</p> <p>Management response: Accepted CYC will include monitoring compliance and guidance in the review of the current Records Management Policy. The launch of the revised policy will include a communications plan for raising awareness as well as guidance, training package(s). When completed, this will be published on the intranet and internet.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31 March 2016</p>		
<p>a17. Ensure that the Records Management Policy is reviewed in line with time periods for review set out in the policy.</p>	<p>Management response: Accepted CYC is currently underway with a review of the Records Management Policy (including a communications plan) and will put in place a monitoring process to ensure future reviews are undertaken within the set time periods.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st March 2016</p>		

<p>a18. Review the draft records management guidance alongside the Records Management Policy to ensure that it is complete, consistent and up-to-date. Ensure that communication of records management guidance is included within a Communications Plan for the Records Management Policy.</p>	<p>Management response: Accepted CYC is currently reviewing the guidance, training package(s) etc. for records management alongside the review of the policy. Following the approval of the reviewed policy, CYC will undertake the actions from the communications plan including providing guidance, training package(s) and publication on the intranet.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st May 2016</p>		
<p>a23. Ensure that records management is incorporated within a formal training programme that comprises mandatory induction and periodic refresher training for all staff with access to personal data.</p>	<p>Management response: Accepted CYC will ensure that records management is included in its training/learning/development mandatory framework including induction, targeted dedicated sessions aligned to local records management responsibilities, and refresher.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30 April 2016</p>		
<p>a28. Ensure that records</p>	<p>Management response:</p>		

<p>management training needs are assessed and addressed for key roles and staff groups.</p>	<p>Accepted CYC will link this with the identification of local records management responsibilities, inclusion in the mandatory framework and into the PDR process where appropriate. Progress of TNA as well as meeting the needs identified through the TNA, will be monitored via the IMB.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st May 2016</p>		
<p>a30. Review the Data Protection Policy to ensure that it is up to date and reflects best practice.</p>	<p>Management response: Accepted CYC is currently underway with a review of the Data Protection Policy (including a communications plan, guidance, training packages) which is now taking account of the comments and recommendations in this ICO audit.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 29th February 2016</p>		
<p>a31. Ensure all privacy notices are readily available and easily accessible from the council's</p>	<p>Management response: Accepted At the launch of the new CYC</p>		

homepage.	<p>website, we updated the Privacy Notice accessible via the main/home page. Further work will be undertaken following the collation of all existing privacy notices, information sharing agreements etc. as part of the new "information asset register monitoring and compliance" across the council, to identify how best to ensure all are easily accessible/searchable/linked where relevant from the main web page.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30 April 2016</p>		
<p>a32. Ensure that privacy notices are made available for all services to inform individuals about the use of their personal data.</p>	<p>Management response: Accepted As part of the new "information asset register monitoring and compliance" across the council, we will be able to identify where privacy notices are not held and therefore put in place a work plan to complete these.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30 April 2016</p>		
<p>a33. Ensure that there is a policy</p>	<p>Management response:</p>		

<p>requirement to regularly review the accuracy and content of privacy notices.</p>	<p>Accepted CYC will include the requirement for regular review of the accuracy and content of privacy notices in the review of the Data Protection policy and develop guidance, training package(s) for staff responsible for privacy notices.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30 April 2016</p>		
<p>a39. Review the IAR quarterly to ensure that it remains up-to-date and fit for purpose. Ensure that the IAR references relevant risks to the information assets.</p>	<p>Management response: Accepted CYC is currently underway with updating the IAR which includes how it will be monitored and used to identify areas such as PIAs, PIA risks etc. where relevant. The IMB will monitor compliance.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31 March 2016</p>		
<p>a42. Include storage arrangements at Yorkcraft within the internal audit plan of security checks.</p>	<p>Management response: Accepted CYC will include Yorkcraft in the internal audit plan of security checks. Meeting arranged with internal auditors mid-November</p>		

	<p>for this.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31 December 2015</p>		
<p>a45. Review the requirement for the retention of both scanned and manual client records by adult social care.</p>	<p>Management response: Accepted CYC will review retention requirements for both scanned and manual adult social care records. The Transparency and Feedback Team Manager and the IMB where appropriate, will advise and support the service area. The Transparency and Feedback Team manager is attending the case management system project board to incorporate the scanned and manual records retention requirements into the project.</p> <p>Owner: Director of Adult Social Care</p> <p>Date for implementation: 31st March 2016</p>		
<p>a46.</p> <p>a) Assign owners to the boxes of 'mystery social care' records stored at Yorkcraft.</p> <p>b) Ensure that the adult social care records stored within the separate filing cabinets at Yorkcraft are logged and</p>	<p>Management response: Accepted CYC will identify and/or assign owners within the service area. The Transparency and Feedback Team Manager and Yorkcraft will work with the service area to ensure that arrangements</p>		

<p>tracked in line with Yorkcraft's Archive Procedure.</p>	<p>are put in place for logging and tracking of the information held in the storage cabinets.</p> <p>Owner: Director of Adult Social Care</p> <p>Date for implementation: 31st May 2016</p>		
<p>a50. Introduce a tracing system to ensure that services actively manage the whereabouts of records retrieved from storage.</p>	<p>Management response: Accepted CYC will complete the development and introduce a tracing system for records retrieved from storage.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st March 2016</p>		
<p>a55. Ensure that all Business Continuity Plans are finalised and reviewed and tested in line with the review dates specified on the plans/ assessments.</p>	<p>Management response: Accepted CYC will ensure all BCPs are finalised and reviewed in line with the dates they specify.</p> <p>Owner: Steve Waddington, Assistant Director Housing and Public Protection</p> <p>Date for implementation: 30 June 2016</p>		
<p>a59. Ensure that a consistent approach is taken across all services for the storage of physical files in the office.</p>	<p>Management response: Accepted CYC has 2 main sites at West Offices and Hazel Court, as well</p>		

	<p>as other facilities/locations across the city. CYC will respond to this recommendation at the 2 main sites by putting in place a consistent approach to storage of physical files. CYC will then roll this out across the other facilities/locations and monitor compliance with this through the information security sweeps conducted by internal auditors.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st March 2016</p>		
<p>a60. Ensure that all services, and teams within them, have a procedure for the secure central storage of cabinet keys.</p>	<p>Management response: Accepted CYC is underway with investigating the options and impacts for the development of a process for secure central storage of cabinet keys. This will include a roll out/ implementation plan, communications plan and compliance/ monitoring plan.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st May 2016</p>		
<p>a65. Ensure that appropriate</p>	<p>Management response:</p>		

<p>restrictions are in place to prevent ████████████████████ ████████████████████ ██████████████████ ████████████████████ ██████</p>	<p>Accepted CYC is currently investigating options to ensure that appropriate restrictions are in place to meet this recommendation.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st March 2016</p>		
<p>a75. Introduce periodic reviews of access permissions granted in Norwel.</p>	<p>Management response: Accepted CYC is underway with investigating the tasks required and the impacts of introducing periodic access permission reviews in Norwel.</p> <p>Owner: Practice Manager</p> <p>Date for implementation: 31st March 2016</p>		
<p>a79. Clear and consistent guidance on taking records containing personal data offsite, should be produced and made available to staff.</p>	<p>Management response: Accepted CYC will include this in the current review of the DP policy and guidance and training package(s).</p> <p>Owner: Director of Adults Social Care and Director of Children’s Services</p> <p>Date for implementation: 29 February 2016</p>		

<p>a80. Staff should be provided with or advised on appropriate methods and/or media for transporting client records offsite.</p>	<p>Management response: Accepted CYC will include this in the current review of the DP policy and guidance and training package(s).</p> <p>Owner: Director of Adults Social Care and Director of Children’s Services</p> <p>Date for implementation: 29 February 2016</p>		
<p>a83. Ensure guidance on the protective marking scheme within the staff intranet is up-to-date. Any updated scheme arrangements should be communicated to staff.</p>	<p>Management response: Accepted CYC will undertake a review of the current guidance and update this where required. This will include a review of the layout and look and feel of the information on the intranet. All changes will be communicated to staff.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st March 2016</p>		
<p>a84. Appropriate and consistent security measures should be in place when sending personal data (especially sensitive personal data) by post. Considerations should be given as to whether personal data can be minimised or sent by other means; and</p>	<p>Management response: Accepted CYC will include this in the current review of the DP policy and guidance and training package(s).</p> <p>Owner: Lorraine Lunt,</p>		

addresses should be checked.	Transparency & Feedback Team Manager Date for implementation: 31 st March 2016		
a85. Consider an appropriate method to reduce the risk of unauthorised access to incoming and outgoing post.	Management response: Accepted CYC will consider options to provide appropriate methods (both in the short and long term) to reduce the risk of unauthorised access to incoming and outgoing post. Owner: Lorraine Lunt, Transparency & Feedback Team Manager Date for implementation: 31 st March 2016		
a86. Introduce procedures to ensure that outgoing post is stored securely after the last collection each day.	Management response: Accepted CYC will investigate options to provide appropriate procedures for ensuring outgoing post is stored securely Owner: Lorraine Lunt, Transparency & Feedback Team Manager Date for implementation: 31 st March 2016		
a89. CYC should have up-to-date retention schedules in place which are based on business needs and have reference to statutory requirements and other relevant	Management response: Accepted CYC is currently underway with a review of the Records Management Policy as well as		

<p>principles. Retention schedules should provide sufficient information for all records to be identified and disposal decisions put into effect. There should also be a link between the assets in the IAR and their associated retention schedules.</p>	<p>updating the IAR which will include identifying retention schedule(s) that need updating. This identification will then inform a work plan to ensure they are based on business needs and reference statutory requirements and provide information on identification and disposal.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30th June 2016</p>		
<p>a90. Retention schedules should be regularly reviewed to ensure that they meet business needs and statutory requirements.</p>	<p>Management response: Accepted CYC has updated the terms of reference for the IMB (replacing CIGG) and it includes records management monitoring and compliance. Alongside this, CYC is underway with updating the IAR and identifying a work plan for updating retentions schedules, all of which will support the regular review of retention schedules to ensure they meet business needs and statutory requirements.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation:</p>		

	30 th June 2016		
a91. Assign responsibility to appropriate individuals/asset owners to ensure retention periods are adhered to.	<p>Management response: Accepted CYC has updated the terms of reference for the IMB (replacing CIGG) and it includes records management monitoring and compliance. Alongside this, CYC is underway with updating the IAR and identifying a work plan for updating retentions schedules, all of which will support the assigning of responsibility for adherence to retention schedules.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30th June 2016</p>		
a100. Ensure that the Yorkcraft SLA is periodically reviewed in line with review periods set out in the Agreement.	<p>Management response: Accepted CYC will review the Yorkcraft SLA and ensure ongoing reviews are conducted in the time periods subsequently set out.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st March 2016</p>		
a104. Identify records management performance	<p>Management response: Accepted</p>		

<p>measures that reflect organisational needs and risks identified in the corporate risk management framework.</p>	<p>CYC has updated the terms of reference for the IMB (replacing CIGG) and it includes records management monitoring and compliance. Work will now be done to determine what the key performance indicators are to reflect our needs and risks. These will be aligned to the risks identified for the corporate risk management framework.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st March 2016</p>		
<p>a105. Ensure that reporting details are being produced as required in the Yorkcraft SLA.</p>	<p>Management response: Accepted CYC will review the Yorkcraft SLA and ensure reports are produced.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st March 2016</p>		
<p>a106. There should be periodic internal audit of the security and use of records, and a formal report issued to senior management.</p>	<p>Management response: Accepted CYC will include this in the internal audit plan. Meeting arranged with internal auditors mid-November for this.</p> <p>Owner: Lorraine Lunt,</p>		

	<p>Transparency & Feedback Team Manager</p> <p>Date for implementation: 31 December 2015</p>		
<p>a108. Review the Information Security Incident Procedure and ensure that it is fit for purpose and in line with best practice.</p>	<p>Management response: Accepted CYC have provided breach management training for 2 key staff and they are now underway with a review of the breach management process, procedures and training materials. This will take account of ICO codes of practices, exemplar organisations processes, etc. and will also identify links to the Caldicott Guardian issues reporting process. The review will also include the development and delivery plan for training, guidance/toolkits, and key performance indicators and how to ensure lessons are learned from breach management reporting. Monitoring has been included in the new terms of reference for the IMB.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st January 2016</p>		
<p>a110. Review the IG Risk</p>	<p>Management response:</p>		

<p>Register in line with the new Risk Management Policy and Strategy to ensure that risk ratings are correct.</p>	<p>Accepted CYC will start the review of the IG risk register in mid-November to ensure it is in line with the new Risk Management Policy and Strategy.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st December 2015</p>		
<p>a112. a) Assigned responsibility for IAO roles across CYC should be clearly communicated. b) IAOs should receive appropriate training to fulfil their roles.</p>	<p>Management response: Accepted CYC is underway with reviewing the IAR and this will include identifying assigned IAOs and IAAs. This will then enable us to develop and deliver awareness, guidance and dedicated training for the IAOs and IAAs and a communications plan.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: (a) 31st March 2016 (b) 30 June 2016</p>		
<p>a113. Information Asset Administrators should be identified and nominated, as planned to support the IAO function, and should receive training as appropriate.</p>	<p>Management response: Accepted CYC is underway with reviewing the IAR and this will include identifying assigned IAOs and IAAs. This will then enable us to develop and deliver awareness,</p>		

	<p>guidance and dedicated training for the IAOs and IAAs and a communications plan.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30 June 2016</p>		
<p>a114. CYC should ensure that its Data Processor Contracts provide it with a right to physically audit its data processors' premises.</p>	<p>Management response: Partially Accepted CYC will write a clause to be included in new tender documents to provide us with this right and for existing contracts. We will include this at the point of renewal.</p> <p>Owner: Andy Docherty, Assistant Director</p> <p>Date for implementation: 29th February 2016</p>		
<p>b1. Finalise and implement the new SAR process.</p>	<p>Management response: Accepted CYC is currently underway with a review of the SAR process, Access to Records policy, training material etc. and will use this ICO report recommendations to further update where required. This review will include the writing of what will be required in the training packages, checklists/toolkits, templates and a communications plan.</p>		

	<p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st January 2016</p>		
<p>b2. Finalise the draft Access to Records Policy and SAR checklist. Update the 'Interim Practice Guidance to Social Workers: Subject Access Requests', 'Business Support SAR Process Children's Services' and 'Business Support SAR flowchart' to reflect the final SAR process.</p>	<p>Management response: Accepted CYC is currently underway with a review of the SAR process, Access to Records policy, training material etc. and will use this ICO report recommendations to further update where required. This review will include the writing of what will be required in the training packages, checklists/toolkits, templates and a communications plan.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st January 2016</p>		
<p>b3. a) Update website guidance to reflect the new SAR process, as planned. b) Make the SAR guidance on the website easier to locate.</p>	<p>Management response: Accepted Following completion of the review of the SAR process and Access to Records policy, and as part of the communications plan being actioned, (a) the website pages will be updated and (b) easier access and search options will be investigated and put in place where possible.</p>		

	<p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st March 2016</p>		
<p>b4.</p> <p>a) CYC should review current data processing contracts to ensure they include the appropriate obligations regarding SARs. This should be included in all future contracts with data processors.</p> <p>b) Integrate third party SARs into the new SAR process to ensure adequate oversight.</p>	<p>Management response: Partially accepted (a) CYC will undertake reviews of current data processing contracts at the time of renewal and (b) include the provision for 3rd party SARs within the review of the SAR process.</p> <p>Owner: (a) Andy Docherty, Assistant Director (b) Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: (a) to be determined by renewal timescales (b) 31st March 2016</p>		
<p>b7. Implement quality assurance procedures through the council team for all SAR responses as proposed.</p>	<p>Management response: Accepted CYC is currently underway with a review of the SAR process, Access to Records policy, training material etc. and will include how the CYC team will quality assure/check SAR responses and how this will be reported. The new IMB will be responsible for monitoring and compliance.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team</p>		

	<p>Manager</p> <p>Date for implementation: 31st March 2016</p>		
<p>b8. Raise awareness of the 'Interim Practice Guidance to Social Workers: Subject Access Requests' amongst all relevant staff/teams.</p>	<p>Management response: Accepted CYC team will continue to raise awareness and provide guidance to relevant teams and staff.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30th November 2015</p>		
<p>b9. As proposed, develop council wide training for staff so staff can recognise a SAR. Conduct training needs analysis of staff involved in the SAR process and provide role specific training where appropriate.</p>	<p>Management response: Accepted CYC will include this training needs analysis in with that being done for records management, IAOs, IAAs etc. Training packages are being developed which will include induction and refresher awareness, and more role and responsibility specific training packages. Delivery will be using the most appropriate method e.g. Icomply, elearning or classroom.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30</p>		

	April 2016		
b10. Update guidance available on staff intranet to reflect new SAR process.	<p>Management response: Accepted CYC will update intranet guidance when SAR process and Access to Records policy reviews are completed.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30 April 2016</p>		
b14. Where appropriate, staff should consider whether children have capacity to independently request a SAR.	<p>Management response: Accepted CYC will include this in SAR process and Access to Records policy guidance, training and published on the intranet. However if advice sought verbally whilst this work is underway, the CYC team will give this.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30 April 2016</p>		
b19. The council team should routinely record what information (if any) is withheld under exemption or relating to third parties and the basis for withholding the personal data.	<p>Management response: Accepted CYC is currently underway with a review of the SAR process, Access to Records policy, training material etc. and will use this ICO report</p>		

	<p>recommendations to further update where required. This review will include the writing of what will be required in the training packages, checklists/toolkits, templates and a communications plan.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st January 2016</p>		
<p>b20. Formalise the requirement for staff to promptly contact the SAR requestor in the event of delay. In such cases, CYC should explain to the requestor the reason for the delay and the expected date for response.</p>	<p>Management response: Accepted CYC is currently underway with a review of the SAR process, Access to Records policy, training material etc. and will use this ICO report recommendation to further update where required. This review will include the writing of what will be required in the training packages, checklists/toolkits, templates and a communications plan.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st January 2016</p>		
<p>b21. Record the formal process for chasing departments for SAR responses and escalating to Heads</p>	<p>Management response: Accepted CYC will include this is the SAR</p>		

<p>of Services when overdue. This process should look to identify why the SAR is overdue, current progress, and when it is likely to be finished.</p>	<p>process and monitoring reports will go the IMB to monitor compliance.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st January 2016</p>		
<p>b22. Ensure any new manual records are maintained to a good standard. Where practicable, take steps to improve any older files that have been poorly maintained.</p>	<p>Management response: Accepted CYC will undertake to develop good standards for manual records in line with the work being done in Adults and Children’s Social Care case management system improvements and linked to recommendations made for records management in this audit report.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30 June 2016</p>		
<p>b24. Keep a record of the searches made to locate personal data in response to a SAR.</p>	<p>Management response: Accepted CYC is currently underway with a review of the SAR process, Access to Records policy, training material etc. and will use this ICO report recommendations to further update where required. This</p>		

	<p>review will include the writing of what will be required in the training packages, checklists/toolkits, templates and a communications plan.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st January 2016</p>		
<p>b25. Ensure that adult social care retains an unredacted copy of the SAR response.</p>	<p>Management response: Accepted CYC is currently underway with a review of the SAR process, Access to Records policy, training material etc. and will use this ICO report recommendations to further update where required. This review will include the writing of what will be required in the training packages, checklists/ toolkits, templates and a communications plan.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st January 2016</p>		
<p>b26. Ensure there are appropriate retention periods for unredacted and redacted SAR responses.</p>	<p>Management response: Accepted CYC will include this is in the Access to Records policy, guidance, training and also</p>		

	<p>publish on the intranet. However if advice sought verbally whilst this work is underway, the CYC team will give this.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st January 2016</p>		
<p>b28. Ensure Yorkcraft securely destroy SAR responses in line with retention periods.</p>	<p>Management response: Accepted CYC will include the requirement for a checking process at Yorkcraft for destruction of SAR responses in line with the current checking process they have for destruction of other stored records.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st January 2016</p>		
<p>b30. Support the advice function provided by Veritau, and in future the council team, with written guidance on exemptions and redactions.</p>	<p>Management response: Accepted CYC is currently underway with a review of the SAR process, Access to Records policy as well as training and guidance material required which includes exemptions and redacting information. Delivery of awareness and role –specific</p>		

	<p>training will be delivered using a variety of methods such as induction and refresher sessions, Icomply, elearning and classroom based. However if advice sought verbally whilst this work is underway, the CYC team will give this.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30th June 2016</p>		
<p>b31. Amend practice guidance to advise staff to contact either Veritau or the council team for SAR advice when required.</p>	<p>Management response: Accepted CYC is currently underway with a review of the SAR process, Access to Records policy as well as training and guidance material, which will include contact information for advice and support. However if advice sought verbally whilst this work is underway, the CYC team will give this.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30th April 2016</p>		
<p>b33. Issue guidance and template letters/paragraphs to assist staff in their response to the data subject. This should include a</p>	<p>Management response: Accepted CYC is currently underway with a review of the SAR process,</p>		

<p>description of how data subjects' personal data is being used and to whom it may be disclosed, an explanation of the searches undertaken to locate their personal data, and where appropriate, an explanation as to why information has been redacted or exempted.</p>	<p>Access to Records policy as well as training and guidance material. This will include a suite of template responses for SARs. However if advice sought verbally whilst this work is underway, the CYC team will give this.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30th April 2016</p>		
<p>b34. Consider marking SAR responses 'data subject copy' before release.</p>	<p>Management response: Accepted CYC will include the requirement for a marking process in the review of the SAR process and Access to Records policy as well as include in the review of the data protection policy where relevant.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st January 2016</p>		
<p>b36. Introduce regular reporting of SAR performance and complaints to the CIGG or other relevant groups as proposed. Ensure that issues are acted upon accordingly.</p>	<p>Management response: Accepted CYC has completed the review of the CIGG terms of reference which will now be the Information Management Board (IMB) and includes monitoring</p>		

	<p>and compliance, in its purpose, aim, remit and objectives. The first meeting is planned for mid-November at which the standard agenda items, such as KPI reporting, will be approved.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st December 2015</p>		
<p>b37. Introduce and regularly monitor an appropriate target rate for SAR compliance, as planned. See also b36.</p>	<p>Management response: Accepted The SAR report for 1st April 2015 to 31st August 2015 shows 30 SARs received, 25 responded to in time and 5 out of time, which is a compliance rate of 83.3%. Reporting of KPIs will be through the new IMB and will include SAR compliance. The first meeting is planned for mid-November.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st December 2015</p>		
<p>b38. Produce management information on SAR compliance which can demarcate performance at the service level, as planned.</p>	<p>Management response: Accepted Reporting of KPIs will be through the new IMB and will include SAR compliance rates</p>		

	<p>both for the whole council and by service. The first meeting is planned for mid-November. Also the review of the SAR process will include points during the 40 day timescale to provide opportunities for early identification of issues.</p> <p>Owner: Lorraine Lunt Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st December 2015</p>		
<p>b39. Raise awareness amongst staff that the new process requires all SAR requests go to the council team in the first instance.</p>	<p>Management response: Accepted CYC has conducted an awareness campaign for SARs using a variety of methods e.g. staff email, staff newsletter, display screens in staff hub areas and posters on all staff noticeboards. The current review of the SAR process and Access to Records policy will include opportunities for further ongoing awareness.</p> <p>Owner: Lorraine Lunt Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st January 2016</p>		
<p>c3. Finalise and action the MAISP Implementation Strategy, and align existing ISAs to MAISP</p>	<p>Management response: Accepted The MAISP has been published</p>		

<p>requirements, as planned.</p>	<p>on the CYC intranet and further progress of the final MAISP implementation strategy is underway. The MAISP information sharing template is also published on the intranet and has been used for new arrangements. Using the IAR monitoring process, CYC will be able to identify a schedule for review of ISAs which will include alignment with MAISP for relevant ISAs.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30 June 2016</p>		
<p>c4. Ensure all ISAs are signed off by an appropriately senior member of staff.</p>	<p>Management response: Accepted CYC has highlighted this at the MAISP group and there has been an agreement to consider making any relevant amendments to the MAISP from the recommendations. CYC is also underway with the review of data protection policy and processes which include the development of a toolkit for completing ISA e.g. request and decision templates, ISA templates, checklists etc. and training and guidance will be provided to those with ISA responsibilities.</p>		

	<p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st March 2016</p>		
<p>c5. Embed requirement to record the reason for all data sharing decisions at CYC.</p>	<p>Management response: Accepted CYC is underway with the review of data protection policy and processes which include the development of a toolkit for completing ISA e.g. request and decision templates, ISA templates, checklists etc. and training and guidance will be provided to those with ISA responsibilities.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st March 2016</p>		
<p>c7. Conduct generic and role-based training needs analysis for all staff sharing personal data at CYC. Deliver appropriate training, including refresher training, thereafter.</p>	<p>Management response: Accepted CYC will link this with the identification of other local records management and data protection role specific responsibilities, and include it in the training/learning/development mandatory framework including induction, targeted dedicated sessions aligned to local or role specific responsibilities, and</p>		

	<p>refreshers as well as the PDR process. This means that progress of TNA will be aligned to the timescales for training development and delivery.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30th June 2016</p>		
<p>c10. Communicate individual responsibilities set out in MAISP to relevant staff.</p>	<p>Management response: Accepted CYC has published the MAISP on the intranet. CYC team has already advised on responsibilities to those services/ areas/ staff who have requested advice on information sharing. Further roll out is planned as set out in the MAISP implementation strategy which will be amended and finalised from the draft version provided during the audit.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st December 2015</p>		
<p>c12. Update the data sharing elements of the Data Protection Policy.</p>	<p>Management response: Accepted CYC will include this is the review underway of the data protection policy.</p>		

	<p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 29th February 2016</p>		
<p>c13. Develop a comprehensive up-to-date suite of policies, procedures and guidance for data sharing.</p>	<p>Management response: Accepted CYC is underway with a review of full suite of policies and processes, training packages, guidance, checklists, toolkits, templates, monitoring and compliance reporting (with KPIs and targets) which includes data sharing.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30th June 2016</p>		
<p>c18. Finalise the draft Project Management Approach, and associated documents. Develop a specific policy for PIAs. See also c13.</p>	<p>Management response: Accepted CYC will finalise the draft PM approach and associated documents. CYC will finish development of a PIA policy which will include the current PIA toolkit and guidance material and updating the information available on the intranet.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team</p>		

	<p>Manager</p> <p>Date for implementation: 31st December 2015</p>		
<p>c21. Cascade PIA requirements and guidance throughout CYC, once finalised.</p>	<p>Management response: Accepted CYC is underway with the cascading of PIA requirements and guidance, by publishing on the intranet and provision of advice and support in conducting PIAs. PIAs will be monitored via the IAR and the IMB.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st December 2015</p>		
<p>c22. Ensure PIAs are carried out for individual applications of Doqex, as planned.</p>	<p>Management response: Accepted CYC is underway with the further PIA requirements for Doqex.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager Transparency & Feedback Team Manager.</p> <p>Date for implementation: 31st December 2015</p>		
<p>c24. Establish governance arrangements at CYC to systematically review ISAs.</p>	<p>Management response: Accepted CYC will include this in the IAR monitoring process and has</p>		

	<p>included the monitoring/compliance in the new terms of reference for the IMB.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st December 2015</p>		
<p>c25. Formalise the terms of reference for the MAISP cross-county Information Governance Monitoring Group. Ensure the MAISP cross-county Information Governance Monitoring Group and/or MAISP “Information Sharing quarterly review” group periodically review the membership and workings of MAISP.</p>	<p>Management response: Accepted The terms of reference for the MAISP being formalised and the comment regarding incorporating periodic review of the membership and workings of MAISP by the relevant group, was raised at the September meeting. This will be formalised at the next relevant meeting.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st January 2016</p>		
<p>c27. Develop service level and a central, register of all ISAs, which detail the nature of the sharing, authorisation, and the partners. This should include information about the legal basis for data sharing.</p>	<p>Management response: Accepted CYC is underway with implementing a register of all ISAs using the IAR process and the development of data sharing request and decision templates.</p>		

	<p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st January 2016</p>		
<p>c28. Ensure there are corporate controls in place to ensure the data shared is of appropriate quality and is not retained for longer than necessary by all parties. This requirement should also be reflected in relevant policies and guidance.</p>	<p>Management response: Accepted CYC will include the requirement for controls for quality within both the review of the data protection policy and processes and records management policy and processes.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 29th February 2016</p>		
<p>c29. a) Update MAISP to explicitly discuss the requirement that shared data is minimised to agreed data sets or redacted. b) Ensure ISAs, relevant policies and guidance include the requirement that shared data is minimised to agreed data sets or redacted.</p>	<p>Management response: Accepted (a) This recommendation will be shared at the next relevant MAISP group meeting (b) CYC will include this requirement within the review of the relevant policies and processes.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 29th February 2016</p>		
<p>c30. Issue common guidance to</p>	<p>Management response:</p>		

<p>CYC about clearly distinguishing between fact and opinion when recording personal data.</p>	<p>Accepted CYC will update existing guidance where required and include in the relevant policy and processes reviews e.g. as part of the development of training materials and packages.</p> <p>Owner: Lorraine Lunt Transparency & Feedback Team Manager</p> <p>Date for implementation: 29th February 2016</p>		
<p>c31. Ensure that where appropriate, the sender informs recipients when shared data has been amended or updated.</p>	<p>Management response: Accepted CYC will update existing guidance where required and include in the relevant policy and processes reviews e.g. as part of the development of training materials and packages.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 29th February 2016</p>		
<p>c34. Ensure common retention and disposal arrangements are included in all ISAs and that these are adhered to by all parties to any given ISA.</p>	<p>Management response: Accepted CYC will include the requirement for retention and disposal arrangements to be included in all new ISAs and be part of the review for existing ISAs. The</p>		

	<p>IAR process will enable monitoring of this.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 30th June 2016</p>		
<p>c36. Ensure that all ISA and supporting procedures set out specifically how personal data will be shared securely.</p>	<p>Management response: Accepted The partner information sharing agreement template in the MAISP has a section to detail how information will be shared at section 7. CYC has included this in the development of the data sharing request and decision templates. It will also be reflected in the review of the data protection policy and processes, training material etc.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 29th February 2016</p>		
<p>c38. ISAs should ensure that access to shared personal data is restricted to authorised personnel within each organisation where possible, on the basis of business need, e.g. a nominated point-of-contact.</p>	<p>Management response: Accepted CYC will include this requirement in the review of the data protection policy and processes, training material etc. and in the data sharing request and decision templates.</p>		

	<p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 29th February 2016</p>		
<p>c41. Include a clause in data processor contracts requiring them to notify CYC of any data security breaches.</p>	<p>Management response: Accepted CYC will write a clause to be included in new tender documents to provide us with this notification and for existing contracts. We will include this at the point of renewal.</p> <p>Owner: Andy Docherty, Assistant Director</p> <p>Date for implementation: 29th February 2016</p>		
<p>c42. Develop a policy for disclosing personal data to third parties. This should be communicated to staff and updated regularly.</p>	<p>Management response: Accepted CYC is underway with a review of the data protection policy and processes (and Access to Records policy) which will include provision for disclosing to 3rd parties. This will be reflected in training packages and guidance.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 29th February 2016</p>		
<p>c45. Establish a central register</p>	<p>Management response:</p>		

<p>for information requests from third parties. This should record the steps taken to identify the nature of the disclosure, the requester and the reason for any disclosure.</p>	<p>Accepted CYC will create a central register for third party information requests as part of the review of the data protection policy and processes. This will be created and managed using the case management system currently used for FOI, EIR, SAR etc. enquiries.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 31st December 2015</p>		
<p>c46. Ensure third party disclosure decisions are quality assured and/or approved by appropriate staff.</p>	<p>Management response: Accepted CYC is underway with a review of the data protection policy and processes which will include provision for quality assurance monitoring. Quality assurance monitoring will include the checking of appropriate approvals for disclosure decisions to third parties.</p> <p>Owner: Lorraine Lunt, Transparency & Feedback Team Manager</p> <p>Date for implementation: 29th February 2016</p>		