

**Report of Director of Resources and Housing**

**Report to Corporate Governance and Audit Committee**

**Date: 7<sup>th</sup> April 2017**

**Subject: Annual Information Governance Report**

Are specific electoral Wards affected? If relevant, name(s) of Ward(s):	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Are there implications for equality and diversity and cohesion and integration?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Is the decision eligible for Call-In?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Does the report contain confidential or exempt information? If relevant, Access to Information Procedure Rule number: Appendix number:	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

**Summary of main issues**

1. There has been a re-structure of the Information Governance Management Team and the creation of a new post; Head of Information Management of Governance, to provide professional leadership on Information Management, Information Security, Information Risk Management, DPA and FOI and Knowledge Management
2. The Cabinet Office has placed the council into an 'escalation' process for PSN. The Cabinet Office has contacted Tom Riordan in this regard who is fully supportive of the work required to enable the Council to regard it's PSN certification.
3. The council continues to handle and process requests for information in accordance and compliance to appropriate legislation such as the Data Protection Act and Freedom of Information Act.
4. The General Data Protection Regulation (GDPR) will replace the current Data Protection Act 1998, and will pass directly into Member State law taking effect from 25th May 2018. The Regulation imposes new and significantly more stringent requirements for the handling of personal data.
5. The work required to address the recommendations of the Information Commissioners Audit report has been completed or is underway. Delivery against the remaining recommendations is being carried out by a small team of Information Governance professionals and completion is expected by March 2018.

## **Recommendations**

6. Corporate Governance and Audit Committee is asked to consider the contents of this report and the assurances provided as to the Council's approach to information governance. The Corporate Governance and Audit Committee is also asked to consider the request made in 3.2.11 to report back to Committee in September, specifically with regards to Cyber Assurance and Compliance.

## **1. Purpose of this report**

- 1.1 To provide Corporate Governance and Audit Committee with an annual report on the steps being taken to improve Leeds City Council's information governance in order to provide assurance for the annual governance statement.

## **2 Background information**

- 2.1 Leeds City Council recognises the need to protect its information assets from both accidental and malicious loss and damage. Information Governance is taken very seriously by the council and this is evidenced by the on-going work to improve the management and security of our information as outlined in this report.
- 2.2 The report provides Committee Members with an update on the more strategic and cross-council activity on-going to provide assurance on our approach to information governance.

## **3 Main issues**

### **3.1 Overall arrangements for Information Management and Governance Assurance**

- 3.1.1 The Council, in line with recommended practice for public authorities in the UK, continues to provide demonstrable arrangements which ensure that information assurance is addressed along with other aspects of information governance.
- 3.1.2 The council has an established and fully trained Senior Information Risk Owner (SIRO), the Deputy Chief Executive, who has overall ownership for information risk management across the council. Work is in hand to ensure that this role transitions smoothly from the 1st April when management arrangements in the Council change at the senior level. Neil Evans (currently Director of Environment & Housing Environment & Housing) will be taking on the role of SIRO from 1<sup>st</sup> April. The SIRO is supported by the Chief Digital and Information Officer who has delegated decision making powers for information governance. The Chief Digital and Information Officer chairs the council's Information Management Board which ensures good standard information management practice is embedded into business processes, and information standards and policy are fit for purpose and kept up to date. Decisions made by the Chief Digital and Information Officer at the Information Management Board are effectively communicated across each Directorate through the Information Management and Governance Team.
- 3.1.3 The Director for Adult Social Care is the council's Caldicott Guardian. This is a strategic role responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing across Health and Social Care.
- 3.1.4 Over the last 10 months the provision for how information governance is managed across the council has been re-structured. The new role of Head of Information Management and Governance has been established. The purpose of this role is:-

- To be accountable for developing and implementing frameworks that ensure that best value is achieved from the appropriate use of information to support the delivery of Council and City outcomes.
- To provide professional leadership on Information Management, Information Security, Information Risk Management, DPA and FOI and Knowledge Management to support improved service outcomes, through a 'One Council' approach to Information.
- To ensure there is a comprehensive set of Information related policies, strategies and ambitions in order to effectively direct and shape the service and ensure awareness and understanding for all officers, elected members and citizens where applicable across the Council.
- To act as the lead for enabling and supporting the councils Transparency and Open Data Strategy ensuring appropriate strategy and implementation across the council
- To oversee the effective underpinning of the Council's operations in the following areas:
  - Compliance and Cyber assurance
  - Information Risk Management
  - Information Quality
  - Information Access Law – Request Management
  - Arrangements for lawful disclosure of none public information
  - Open Data

3.1.5 This role also directly provides line management and leadership to four Information Governance leads and Information Governance teams across the Council.

- Cyber Assurance and Compliance
- Information Access and Compliance
- Records Management
- Change and Initiatives

3.1.6 Each of the Information Governance leads have developed work programmes, which are monitored and managed through the IM&G Management Team and in turn the Chief Digital and Information Officer.

## 3.2 Cyber Assurance and Compliance

- 3.2.1 The Public Services Network (PSN) was set up as an assured route for information sharing by central Government, to facilitate shared services and also serve as the assured route for GCSx mail. It acts as a compliance regime that serves as both a commitment to a basic level of information security for connecting authorities and also a level of trust between Leeds City Council and other public services.
- 3.2.2 A number of services are accessed via PSN, Blue Badge and CIS Revenues and Benefits and Tell Us Once for registrars. PSN certification is relied upon as a mechanism to support information sharing, where many of the requirements request that the council present a certificate prior to sharing, or evidence alternative, more time consuming compliance work to be completed. This has had an impact already on sharing with Health as a number of the controls are evidenced by a PSN certificate. For instance, GCSx mail depends upon PSN certification; JARD (Joint Asset Recovery Database) is presented over the PSN network; new ways of working with the Valuation Office Agency; and, the Family Information Service eligibility, which is a new legislative requirement from September 2017, relies on the council having PSN certification.
- 3.2.3 Due to more stringent compliance control brought in by the Cabinet Office in 2015 the council are presently unable to meet the PSN certification requirements. The Cabinet Office has placed the council into an 'escalation' process for PSN, a process by which the Cabinet Office seek commitment from the CEO and provide further support in remediation against the controls.
- 3.2.4 A PSN Remediation Board has been established with the Head of Information Management and Governance as SRO. The board meets bi-weekly to work through the compliance requirements and close down remediation tasks realised by the Cabinet Office auditors. Monthly meetings with Cabinet Office provide them with regular reports about the progress being made by the council.
- 3.2.5 The current status of remediation actions is as follows:
- Issues resolved: 98
  - Issues with a plan in place and on track: 38
  - Issues with a plan in place, but off track: 4 - currently working to a November 2017 end date for one issue, however working closely with the service area to bring this forward.
  - Issues with no plan: 4 – discussion currently underway in order to develop solutions.
- 3.2.6 Examples of issues include:
- Unsupported software such as Lotus Notes, which no longer receive security patches from the supplier

- Unsupported Windows 2003 servers, which no longer receive security patches from suppliers. Business applications sit on these servers and as a result could be vulnerable.

3.2.7 A further external audit was conducted on behalf of the Cabinet Office in February 2017. The Head of Information Management and Governance is still waiting for the outcome of this audit.

3.2.8 A Professional Lead for Cyber Assurance and Compliance has been appointed and is now working with the Information Management and Governance Management Team.

3.2.9 A Cyber Risk for the council has been agreed and is now presented for quarterly reporting on the corporate register. The council is keen to improve the security of the environment fundamentally, those improvements will be managed and prioritised via the PSN Remediation Board, and first steps include the procurement of a Vulnerability Management suite, which will provide the council with warnings on any slippage of security across the estate.

3.2.10 The Committee can be assured that work to regain PSN certification is the highest priority for the Information Management and Governance Service, the Digital Information Service, with the full backing of CLT. However, at this time and until all the actions required by the Cabinet Office are completed, only limited assurance can be given with regards to Cyber Assurance and Compliance.

3.2.11 It is requested that a report specifically regarding this area of compliance comes to this Board in September 2017, to update the position.

### **3.3 Information Access and Compliance**

3.3.1 Information legislation provides rights for citizens to access information held by the council. In respect of the Data Protection Act (DPA) this provides a statutory right for citizens to access information held about them within forty calendar days of submitting a request. Under the Freedom of Information Act (FOIA) citizens have a right to request information held by a public organisation, such as the council, and unless an exemption applies, the council is under a duty to provide this information within twenty working days of receiving a request.

3.3.2 The need to be able to locate and retrieve information is essential, both to enable the council to operate effectively and efficiently and to respond to information requests within the statutory timescales prescribed. The risk to the council of non-compliance would be enforcement action from the Regulator, the Information Commissioner's Office (ICO). The ICO has a range of enforcement actions it can impose, including issuing monetary penalty notices of up to £500,000 for serious breaches of the DPA; the issue of undertakings committing an organisation to a particular course of action in order to improve its compliance (DPA/FOIA); serve enforcement notices and 'stop now' orders on organisations (DPA/FOIA); and, prosecute those who commit criminal offences under the Act (DPA/FOIA).

3.3.3 A team of Information Practitioners ensure that all requests for information to the council are processed and dealt with according to respective legislation and within statutory timescales, and handle complaints from citizens and enquiries from the ICO. The ICO monitors the performance of all public authorities to ensure that they are compliant with legislation. The ICO's monitoring threshold for FOI is that an organisation should be processing 85% of its requests within the statutory 20 working day time limit; and, the monitoring threshold for SAR's is that an organisation should be processing 90% of its requests within the statutory 40 calendar day time limit. Therefore it is important the council performs well in dealing with citizens requests for information, and continues to improve information governance practice in information processes, systems and networks to improve access and availability of information. The council is currently meeting both of these thresholds. The table below outlines the numbers of requests received and handled by the council for both the DPA and FOIA during 2014/15 2015/16 and figures to date for 2016/17: These figures represent a 3% increase in the number of FOI requests and a 20% decrease in the number of SAR request received compared to the same period last year. SAR's are on average 525 pages per request.

	<b>2014/15</b>	<b>% compliance to statutory timescale</b>	<b>2015/16</b>	<b>% compliance to statutory timescale</b>	<b>2016/17 to Dec 2016</b>	<b>% compliance to statutory timescale</b>
DPA – Subject Access Requests	466	81.6	514	89.0	317	97.4
FOIA – Requests for Information	1986	92.9	2017	96.4	1518	97.6

3.3.4 The General Data Protection Regulation (GDPR) will replace the current Data Protection Act 1998, and will pass directly into Member State law taking effect from 25th May 2018. The rules are designed to give citizens across the EU control of their personal data and to create a high, uniform level of data protection across the 28 members' states, fit for the digital era. The Regulation imposes new and significantly more stringent requirements for the handling of personal data on all organisations which use personal data.

- 3.3.5 The government has confirmed that the UK will be implementing the GDPR regardless of Brexit (the Secretary of State Karen Bradley's MP appearance before the Culture, Media and Sports Select Committee on 24 October).
- 3.3.6 Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), so most of the council's current approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant new requirements so there will be some significant work to deliver to ensure the council is compliant with the new Regulation. These requirements will affect all parts of the council which handle personal or personal sensitive data.
- 3.3.7 Committee can be assured that the council has established a strategic working group which is in the process of conducting a personal data audit across the council to fully understand how services handle personal data and where there might be an impact. Existing resources such as the Information Asset Register and Applications Portfolio will be used to support other ongoing work streams. It is important the council is prepared for the implementation of GDPR on 28th May 2018 as failure to adhere to the Regulations would subject the organisation to the risk of an administrative fine. Public Authority fines will be the subject of separate derogation from the UK Government, and at the time of writing, this is yet to be issued. However, unlike with the current Data Protection Act, fines can be issued to organisations who cannot demonstrate compliance with GDPR, in addition to data breaches. This is a significant change.
- 3.3.8 The size and scale of both the GDPR and Leeds City Council means that this project needs to commence and gain momentum quickly if the council is to be able to make the required changes within the timescale. Whilst work has commenced, as outlined in paragraph 3.3.7, further resources are required quickly to undertake the required work. To this extent the strategic working group are assessing the requirements with a view to properly scoping and costing the council wide programme and informing a business case, which will be taken to a future CLT.
- 3.3.9 There is an embedded Information Security Incident Management and Reporting process across the council, which is coordinated by Information Compliance Officers. Since the Information Commissioner's audit in 2013, the council has a continued improved record and not experienced any incidents which have required involvement by the Information Commissioner. The Information Security Incident Management and Reporting procedure is currently being reviewed as one of the work streams under the GDPR Strategic Working Group's agenda, as GDPR will require changes to process; including the reporting of a breach to the ICO within 72 hours if there is a risk to an individual.
- 3.3.10 Staff awareness and training on information governance remains an important and integral part of the council's information strategy and is delivered through a series of training programmes. The Level One training is mandatory to all staff and is provided every two years. The latest version was launched in June 2016 and 92% of council staff has accessed the training programme. The ICO recommend regular staff training, as this helps, not only to make staff aware of their responsibilities for information, but to mitigate against information incidents. The next version which will be delivered in 2018 will incorporate any changes under the new General Data

Protection Regulations (GDPR) coming into force in May 2018. An Information Governance training and awareness programme for elected Members is also currently being delivered to all member groups so that they understand basic information governance practice around information security and information sharing

3.3.11 In 2013 the council was subject to an undertaking by the Information Commissioner in respect of an inadequately drafted contract under which the council required a supplier to process personal data its behalf. The undertaking required the council to embed measures to ensure that all contracts are properly drafted in line with the Data Protection Act when the contracts involve the processing of personal data on its behalf. All council contracts were checked as part of this undertaking and an interim measure was applied wherever required.

3.3.12 Since the last Corporate Governance and Audit Report in March 2016, a full training programme on Data Protection and Information Governance within Contracts has been rolled out and completed. This training was delivered to all Commissioners and Contract Managers within the council. Alongside this, new template procurement and contract documentation was embedded to ensure consistent and robust data protection and information governance.

3.3.13 Further work is required in this area in order to ensure compliance with the GDPR. All existing contracts that will continue into May 2018 and newly negotiated contracts between Leeds City Council and third parties will need to be reviewed and amended as appropriate to ensure compliance with the GDPR. In addition, procurement processes will need to ensure that technical requirements and assessments match the requirements of the GDPR. Directorates will also need to review how they commission services that handle personal data.

3.3.14 Regarding the area of Information Access and Compliance the Committee can be fully assured that process and procedures are in place regarding upholding citizen rights to request information and the Council is within the Information Commissioners Office thresholds for response times. Other areas articulated in this report, the Committee can be fully assured that the Council are compliant with current Data Protection legislation and that work is in hand to become compliant with the General Data Protection Regulations by May 2018

#### **3.4 Records Management**

3.4.1 Following the ICO audit in 2013 the council prepared and is delivering against a project plan to implement an Information Asset Register (IAR) and appoint Information Asset Owners (IAO's). The project plan has been approved by the council's Information Management Board, and is set out in a number of phases.

3.4.2 Phase one of the plan was completed in December 2016 and has ensured that all Directorates have identified their assets and nominated IAOs at a Head of Service level. This information is published on the IAR.

3.4.3 Phase two will strengthen existing arrangements and will embed the role of IAO further. By consolidating all the information in relation to each asset into one single source, this will enable IAO's to ascertain any risks associated with their information

assets. Throughout this phase of the project training materials will be reviewed and refreshed and delivered to all IAO's via a training programme to embed the role and ensure awareness about information risk management.

3.4.4 In conjunction with phase two, preparation work is underway with the Corporate Risk Manager to revise the procedure for reporting risks to information assets and notifying the SIRO about serious risks to the council.

3.4.5 The Records Management Team are currently finalising a programme of work which aspires to improve and ensure consistency of records management approaches across the whole organisation and maintain compliance with the Data Protection Act.

3.4.6 Priority areas within the work plan include:

- Information is everyone's business - To ensure that the council has an Information Asset Register in place and associated Information Asset Owners are in place and aware of their role in order to ensure information being managed accordingly;
- To ensure that all records are managed effectively as part of the Changing the Workplace programme in line with designated methodologies;
- Ensure consistency in the management of HR files across the council to ensure compliance with the DPA principles;
- Ensure that all scanning and digitisation provision by the scanning framework is effectively monitored, justified and co-ordinated;
- To cleanse the data and reduce the storage on our existing network drives and mitigate the risk of breaching DPA principles;
- Improve Paper Records management to enable effective management, tracking movement and destruction of paper records owned by LCC and reduce unnecessary storage costs;
- Raise awareness of Records Management across the council to ensure staff are aware of their roles and responsibilities in relation to the management of information.

3.4.7 As part of the ongoing work to develop the Information Asset Register and role of Information Asset Owners the retention periods for these assets will also be examined and linked accordingly. This will not only ensure managers are aware of how long they should be retaining their information assets for but will also help identify any inconsistencies of practice with the LCC retention schedule that was agreed by legal services 18 months ago.

3.4.8 Processes are in place to ensure that suggested changes to the retention schedule are sufficiently challenged by Records Managers and approved by Legal Services and work is also ongoing to simplify the way that we present our retention schedules to enable staff find and understand the relevant content more clearly.

3.4.9 With regards to Records Management the Committee can be assured that the Information Management and Governance Team are providing a reasonable level of assurance that processes and procedures are in place and delivering data protection compliance in this regard. Plans are in place to ensure continuous improvement as documented.

### 3.5 **Change and Initiatives**

3.5.1 Auditors from the Information Commissioner's Office (ICO) visited the Council in October 2013 to carry out an audit of its processing of personal data following enforcement action at the Council in 2012. Whilst, the audit provided the ICO with reasonable assurance about our data protection practices, auditors provided a list of 32 recommended improvements to current practice for the council to implement. Members of this Committee received a detailed report on 21st January 2014 regarding the audit, and further reports were considered on 20th March 2015 and 18th March 2016 outlining progress made to date. Appendix A to this report contains a summary and further update against outstanding actions with regards to these recommendations.

3.5.2 Work on twenty six of the thirty two recommendations is now complete and actions embedded into information governance standards and/or practice. . The remaining six recommendations constitute an investment in some fairly significant work but progress is being made. Since Committee received the last report, there has been a restructure of the IG Service and a realignment of resources, which is providing a more concentrated focus on delivery against the remaining recommendations. However it should be noted that this work continues to be undertaken against a backdrop of competing priorities. . The ICO are no longer monitoring progress, and will only take a further interest should the council be subject to a reportable information incident. The last recommendation is scheduled for completion by 31st March 2018 and the Head of Information Management and Governance will continue to monitor progress.

3.5.3 Corporate Governance and Audit Committee considered a report in September 2016 providing assurance about our continued compliance to DCLG's Local Government Transparency Code 2015. The report provided Committee with specific assurances about processes and procedures to publish the required 15 datasets being embedded to ensure continued compliance, and information regarding continued monitoring of these datasets by the Information Management and Governance Team. Furthermore, council officers are in regular contact with representatives at the LGA and are informed of any potential changes to this Code.

3.5.4 Through its Open Data agenda, the council continues to proactively publish datasets over and beyond that required by the Local Government Transparency Code 2015 and making data available in response to FOI requests where possible. This means that the council is one of the most open and transparent local authorities in the country, and also ensure it is compliant with the EU Public Sector Information Re-Use Directive focusing on making data from public authorities available for re-use.

3.5.5 Leeds City Council is required to make all INSPIRE\* related data (as is) and metadata available to view and download by December 2020. The council has

been using a software package using funds from DEFRA to enable it to publish the first 'most common' 20 datasets – an approach adopted by many local authorities. To date the council has published four datasets.

- 3.5.6 It is currently unclear which direction the UK Government will take with this Directive following the result of the EU Referendum on 23rd June 2016. The council is committed to doing as much as it can to work towards compliance. A review is currently being undertaken to review GIS software which the council has a licence for, which can be used to progress this work – an approach that York City Council and the Environment Agency have taken. Whilst this approach would not mean that datasets are published to exacting INSPIRE standards, it does mean that the council can quickly publish more of its geo-spatial datasets. Given that there remains an issue around the lack of resources and skills to focus on this work, and we are awaiting Government guidance on future compliance to the INSPIRE regulations, this approach will publish required datasets to a good standard, which can be adapted for INSPIRE if required. The creation of a GIS Steering Group, which consists of GIS specialists from across the organisation means that the agenda is now being discussed at a more senior level.
- 3.5.7 The Information Commissioners Office no longer requires Leeds City Council to report to them on the outcome of the 2013 Audit. They are assured and as such this Committee can also take assurance that all the recommendations are either complete or partially completed to a standard of which they approve. This report provides assurance to Committee that the council continues to comply with the mandatory Local Government Transparency Code 2015. Review work regarding compliance with the INSPIRE Directive is on-going, however we are waiting for further direction from UK Government as to whether full implementation should commence.

## **4 Consultation and Engagement**

- 4.1 Consultation on the development of strategies, policies, procedures and standards are extensively undertaken across a broad range of stakeholders including information management professionals, representatives from all Directorates via representatives of Information Management and Technology Teams and Information Management Board members.

## **5 Equality and Diversity / Cohesion and Integration**

- 5.1 Equalities, diversity, cohesion and integration are all being considered as part of delivering the Information Management Strategy. This refers to the way training is being delivered as well as how policies will impact on staff and partners.

## **6 Council policies and City Priorities**

- 6.1 The policies support the Information Management Strategy and contain areas of legal requirement. Furthermore, the implementation of the Information Management Strategy will improve the quality of the council's policy framework by ensuring the authenticity, integrity and security of the information contained therein.

6.2 Under the Code of Corporate Governance in Part Five of the council's Constitution, the fourth principle (taking informed and transparent decisions which are subject to effective scrutiny and risk management) requires decision making processes and enables those making decisions to be provided with information that is relevant, timely and gives clear explanation of technical issues and their implications.

## **7 Resources and value for money**

7.1 Capacity within Directorates to deliver, embed and monitor compliance to information governance and information risk management practice is to change from the 1<sup>st</sup> April 2017. All Information Governance employees currently embedded within Directorates will be moved under the newly established Information Management and Governance Management Team.

7.2 Three Directorate IM&G Hubs have been developed and will also be deployed from the 1<sup>st</sup> April. Whilst all IM&G employees will be managed centrally, each Hub will have the appropriate number of Compliance and Records Management employees in each to in order to maintain information governance assurance across the Council. The Directorate Hubs will be as follows:

- Adults, Children's and Health
- Shared Services and Housing
- Cities and Communities

## **8 Legal Implications, Access to Information and Call In**

8.1 Delegated authority sits with the Director of Environment & Housing Environment & Housing and Senior Information Risk Owner and has been sub-delegated to the Chief Information Officer under the heading "Knowledge and information management" in the Deputy Chief Executives Sub-Delegation Scheme.

8.2 There are no restrictions on access to information contained in this report.

## **9 Risk Management**

9.1 The risk associated with not implementing information governance policies, procedures and practice across the Council leaves the organisation more susceptible to breaches of legislative, regulatory and contractual obligations, affecting the confidence of its citizens, partners, contractors and third parties when handling and storing information.

9.2 Information risk is being systematically addressed by joining up the approach to risk required by information security standards, the need for the senior information risk owner to be clear about the risks he/she is accountable for and the council's standard approach to risk management.

9.3 Further work is being undertaken in conjunction with the Corporate Risk Manager to embed the recording and reporting of information risk monitoring and management. The Information Asset Register project will generate information required and an

automated dashboard will be produced to report risk assessments to the SIRO. This will provide the assurance required by the SIRO from the business and will allow risk mitigations to be prioritised.

## **10 Conclusions**

- 10.1 The work of the previous year, reported to this Committee on 18<sup>th</sup> March 2016, has been continued.
- 10.2 The establishment of information governance practice and procedures outlined in this report provides a level of assurance to Committee that the range of information risk is managed both in its scope and through to service delivery. It allows the council to work with partner organisations, third parties and citizens in a clear, transparent, but safe and secure way. It helps to protect the council from enforcement action and mitigate the impact of cyber incidents aimed at attacking and/or bringing down council information systems.

## **11 Recommendation**

- 11.1 Corporate Governance and Audit Committee is asked to consider the contents of this report and the assurances provided as to the Council's approach to information governance. The Corporate Governance and Audit Committee is also asked to consider the request made in 3.2.11 to report back to Committee in September, specifically with regards to Cyber Assurance and Compliance.

Background documents None

## Appendix A

### Leeds City Council: outstanding actions against recommendations made by the Information Commissioner

No	Recommendation	Current position as at February 2017	Status	Completion
1.	A6. Ensure IAOs are trained in line with proposed plans. Further advice on IAO training is available from The National Archives.	<p>Council's Corporate Leadership Team has approved the nomination of Information Asset Owners who will be responsible for managing information risk within their services and ensuring compliance with internal policy and external regulatory requirements.</p> <p>A Project plan has been developed and approved by the Information Management Board to refresh the Information Asset Owner role and to provide a full engagement programme to train IAIO's and support staff. This plan is in two phases.</p> <p>Phase One of the plan was completed by December 2016 and has ensured that all Directorates have listed their assets on a register within Sharepoint. The exception to this is City Development which has a list of their assets on a spreadsheet and this is being migrated across the council's Sharepoint register.</p> <p>Phase Two will involve implementing a training programme for all Information Asset Owners and ensuring the current Information Asset Register is maintained and kept up to date. A report outlining proposals is to be considered by the council's</p>	Partially Complete	31 December 2017

		Information Management Board in April.		
8	A23. Introduce a standard procedure for signing files out of the office and ensure the file returns are monitored.	A new corporate standard and procedure for tracking and tracing of files has been developed and agreed and is currently being implemented. Progress has slowed due to a combination of IG restructure and staff movement.	Partially Complete	31 March 2018
10	A28. Ensure all visitors to office buildings containing sensitive personal data are recorded in a visitor's book and ensure codes for doors with pin code access are regularly changed and this is recorded.	<p>In a review of buildings from which council services operate, 21 high risk buildings were identified and 25 medium risk. A small core team of IG professionals began auditing in 2015 and have now completed audits of 21 of the high risk buildings and 22 of the medium risk buildings. Auditing continues of the remaining high and medium risk buildings.</p> <p>During the audit the procedures relating to visitors have been reviewed and updated where necessary.</p> <p>Ongoing and continuous work on other council buildings deemed low risk is carried out by Directorate IM&amp;G teams.</p> <p>.</p>	Partially Complete	31 March 2017
21	A51. Ensure that PIAs are embedded across the Council at the implementation stage of any projects involving the processing of personal data.	<p>There is a new framework for the delivery of projects and programmes and also contracts and contract management. Council PIA's to be implemented as part of the process.</p> <p>The use of PIA's has been mandated by IMB.</p> <p>Training in their use in contracts was delivered to all contract managers and commissioning staff by the end September 2016 and a guidance resource published on InSite.</p> <p>Work is ongoing within IM&amp;T hubs to implement and embed PIA's as part of the programme and project</p>	Partially Complete	31 <sup>st</sup> December 2017

		<p>management process. To this extent a workflow has been piloted across the Central and Corporate IM&amp;T with a view to rolling out across the council during 2017.</p> <p>PIA forms are being reviewed as part of the council's preparations for the General Data Protection Regulations..</p>		
24	<p>B13. Ensure a formal information security risk assessment and management programme for all information assets on the Information Asset Register has been documented, is implemented by Information Asset Owners and regularly monitored and reviewed.</p>	<p>See action 1 above Preparation work is underway with the Corporate Risk Manager and a dashboard will be required to consolidate risk assessments to provide "heat maps" at various level of the council. It will also act as an action tracker at service level.</p> <p>A procedure to escalate the recording of risks to information assets is to be developed as part of Phase Two and delivered as part of training to IAO's during 2017/18.</p>	Partially Completed	31 March 2018
30	<p>B34. There is a risk that staff who have moved departments within the Council are not promptly removed from access to databases containing personal data which they no longer require. Ensure HR provide systems administrators with a list of staff who have moved departments to cross reference against staff access rights.</p>	<p>A newly formed project team has developed a draft procedure for staff leavers and for staff changing positions. This is in the process of being finalised before pushing out for formal consultation with council boards and steering groups.</p>	Partially Complete	31 December 2017