

**Report of Director of Resources and Housing****Report to Corporate Governance and Audit Committee****Date: 16<sup>th</sup> March 2018****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. Considerable progress has been made this year to resolve security issues. The Cabinet Office has de-escalated Leeds City Council's PSN (Public Services Network) status to Remediation, but we still remain non-compliant at present. Work is on-going to re-apply in May 2018.
2. 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.
3. 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.

**Recommendations**

1. Corporate Governance and Audit Committee is asked to consider the contents of this report and the assurance provided as to the Council's approach to information governance.

## **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 Director of Resources and Housing continues in the role of SIRO. 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 and Public Health 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 The Council's Head of Information Management and Governance has been appointed as Data Protection Officer (DPO). This decision was ratified by the Information Management Board on 9th August 2017, the appointment being made with immediate effect. The GDPR requires the council, as a public authority, to designate a Data Protection Officer. The main tasks of the DPO are: to inform and advise the council of its obligations under GDPR when processing personal data; to monitor compliance with the GDPR; to provide advice where requested, particularly, with regards to data protection impact assessments and other high risk processing activities; and to act as the contact point with the supervisory authority (the ICO).

3.1.5 The Head of Information Management and Governance role is now firmly 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

3.1.6 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

3.1.7 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 (secure) 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 Due to more stringent compliance control brought in by the Cabinet Office in 2014, Leeds City Council are presently unable to meet the PSN certification requirements. In January 2017, the Cabinet Office placed the Council into an 'escalation' process for PSN; a process by which the Cabinet Office seek commitment from the Chief Executive and provide further support in remediation against the controls.
- 3.2.3 A re-application for PSN Certification was made to the Cabinet Office on the 30<sup>th</sup> September 2017. The Cabinet Office responded to this submission on the 29<sup>th</sup> January 2018, stating that they were not able to renew our certificate at this time.
- 3.2.4 The Cabinet Office has 4 levels in which they work:
- In Certificate
  - Remediation
  - Escalation (Stage 1)
  - Escalation (Stage 2)

In January 2017, Leeds City Council was placed into the Escalation (Stage 2). Following our September 2017 submission the Cabinet Office has moved the Council out of the Escalation process and we are now in the Remediation process. This is recognising that whilst we still have some unresolved issues, we have comprehensive plans in place to deal with those issues. At the time of writing this report, the revised re-submission date is still to be determined.

- 3.2.5 Over the last 12 months the PSN Remediation Board, with the Head of Information Management and Governance as Senior Responsible Officer (SRO), reporting to CLT and the Senior Information Risk Officer (SIRO) monthly, has made significant progress. The board meets bi-weekly to work through the compliance requirements and close down remediation tasks realised by the IT Health Check (ITHC) audit. Monthly meetings with the PSN Authority (PSNA) provide them with regular reports about the progress being made by the council.
- 3.2.6 The ITHC in February 2017 highlighted a large number of issues on a sample of the network. This was due to process defects with patching and configuration management. The estate is now being actively monitored for vulnerabilities and patched appropriately. Compliancy is now above 90% for Windows hosts (which comprises of the bulk of the estate) and which is an acceptable level for the

Regulators. 146 unsupported or un-patchable Windows servers have been removed from the estate,

- 3.2.7 Telephony – All Polycom devices have been updated and a process has been established to ensure they are kept up to date in the future.
- 3.2.8 All out of support Solaris servers and all occurrences of out of support Siebel have either been removed from the estate or upgraded appropriately.
- 3.2.9 32 Cloud suppliers have been identified. They have all been contacted regarding their compliance with the 14 PSN Cloud Security Principles. Cloud Security Principles have been added into technical specifications for all new contracts and renewals. In development is a 'Cloud Readiness Assessment' for external suppliers to ensure that they meet the Principles prior to tender.
- 3.2.10 Mobile Device Management – 1800 mobile devices have now been upgraded to include superior security measures. The support documentation has been amended in light of feedback received. A temporary pause in the full rollout has been called due to issues regarding the roll out to iPhones.
- 3.2.11 Network Segmentation / Authentication – The procurement of a network access control software is complete, implementation is planned before the end of March 2018. Network segmentation will follow the completion of this work.
- 3.2.12 In November 2017, a mid-year IT Health Check was instigated in order to ratify the Council's position. The results of the ITHC show a significant improvement. We can confirm that between February 2017 and November 2017, we reduced the number of the critical and high cyber security issues referred to in the PSN correspondence from 67,000 to 3,200. The vast majority of these issues are related to patching, which are dealt with by the Vulnerability Management Team established last year specifically to address these issues. We have firm plans in place for areas of non-compliance not directly related to patching, examples of which are given in 3.2.5 – 3.2.10. Where vulnerabilities were highlighted, there was nothing that we were not already aware of and plans were already in place to rectify.
- 3.2.13 We have invested in a software product called SureCloud, which now means we can monitor our own compliance without having to commission external IT Health Checks and this will enable us to evidence our compliance to the PSN Authority.
- 3.2.14 Due to the "Remediation" state we do not foresee, at this time, this causing us problems with regards to connecting to other government services.

### **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 generally 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 currently 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 also has its own KPIs in relation to statutory requests and for 2017/18 these are 96% for FOI requests and 88% for SARs. 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 2015/16, 2016-17, and figures to date for 2017/18. These figures represent a 3% decrease in the number of FOI requests and a 37% increase in the number of SAR request received compared to the same period last year. SAR's are on average 300 pages per request.

	<b>2015/16</b>	<b>% compliance to statutory timescale</b>	<b>2016/17</b>	<b>% compliance to statutory timescale</b>	<b>2017/18 to Dec 2018</b>	<b>% compliance to statutory timescale</b>
DPA – Subject Access Requests	514	89.0	470	96.5	387	97

FOIA – Requests for Information	2017	96.4	2137	97.5	1327	98
---------------------------------	------	------	------	------	------	----

- 3.3.4 As from May this year, there will be a new data protection framework which will consist of the General Data Protection Regulation (“GDPR”) and the Data Protection Act 2018 (the Data Protection Bill is currently going through parliament). The latter replaces the current Data Protection Act 1998 and supplements the GDPR. This new framework builds on the principles contained within the 1998 Act with a greater emphasis on fairness, transparency, and accountability. A strategic working group was formed in August 2016 to scope out the work required for the Council to meet the compliance requirements set out in the GDPR and this working group, which is chaired by the Information Governance Lead for Access and Compliance, became the Strategic Implementation Board (“SIB”) in September of last year.
- 3.3.5 A project of this size is a significant programme of work and dedicated resource is required to make the relevant people, process and technology changes required across the council to enable us to be compliant by May 2018 and maintain that compliance thereafter. Furthermore, the GDPR contains increased enforcement powers with certain violations attracting a fine of up to 2% of annual worldwide turnover or 10 million euros (whichever is the greater) and others up to 4% of annual worldwide turnover or 20 million euros (whichever is the greater).
- 3.3.6 To help address the size and complexity of this work programme, a GDPR Implementation Team was established in August 2017 for a fixed term of 12 months. This team is led by the Information Governance Lead for Access and Compliance and currently consists of two Senior Information Governance Officers from within the IM&G Service and part time support from a project manager. The GDPR Implementation Team requires active engagement and support from core services within the council such as ICT, Legal, HR, Procurement, Communications and Internal Audit.
- 3.3.7 Since September 2016 much work has taken place to assess the requirements of the GDPR, and more recently the Data Protection Bill, against the Council’s current position and to scope out the work required. From this initial assessment 9 technical work streams were initiated to define the objectives and outputs required to achieve compliance with the relevant articles in the GDPR and to ensure that appropriate policies, procedures and guidance are updated or created. The 9 technical work streams, together with a brief description, are as follows:
1. **Demonstrating compliance** - requirement for the Council to be able to demonstrate how it meets the principles contained within the GDPR.
  2. **Security of processing** – requirement to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

3. **Security incident management** – requirement to notify the ICO of personal data breaches, without undue delay, and where feasible within 72 hours of becoming aware of it unless the breach is unlikely to result in risk to the data subject.
4. **Data Protection by design and default** – requirement to carry out data protection impact assessments (currently known as privacy impact assessments) whenever the Council is using new technologies, and the processing is likely to result in a high risk to the rights and freedoms of individuals.
5. **Contractual arrangements with data controllers / processors** – direct obligations on data processors for the first time and new requirements to be followed when using data processors.
6. **Individuals' rights** - key rights include the right of access (similar to the current rules for subject access requests); the right to restrict processing; the right to object; the right to rectification; and the right to erasure / be forgotten.
7. **Lawfulness, fairness and transparency** – requirement to have a legal basis for processing personal data with the threshold to utilize consent being higher than the current DPA; and to provide further information within privacy notices than is currently stipulated.
8. **Storage limitation** – see section on Records Management below.
9. **Accuracy and data quality** – requirements around data minimisation and accuracy including ensuring that inaccurate data is erased or rectified without delay.

There is a further work stream around communications and engagement with the business, partners, and third parties.

3.3.8 From November 2017 to January 2018, the GDPR Implementation Team delivered 7 two hour engagement sessions to which all senior management across the authority received invitations. The purpose of the events was to: 1) provide directors, chief officers and heads of service with an overview of GDPR and the Data Protection Bill including what the key changes are; and 2) to explain the Council's plans for implementation including highlighting the responsibilities of senior officers in terms of preparing their service areas. In total, 203 officers (173 senior officers and 30 HR and business partners) attended these implementation events which were very well received.

3.3.9 Critical to the success of the implementation programme is the role of the GDPR Service Leads whose key responsibilities are to:

1. support the GDPR implementation team by driving the GDPR agenda within service areas including the dissemination of key messages;
2. ensure that existing processing arrangements and systems are GDPR compliant and, where required, make the necessary changes including the implementation of appropriate technical and organisational measures proportionate to the risks involved;
3. assist with the embedding of new GDPR related policies and procedures across the council; and
4. report progress on implementation against key milestones to the GDPR implementation team including the reporting of risks and issues as they emerge.



Following discussions at the SIB, Information Management Board and CLT, Chief Officers were tasked with identifying a minimum of one GDPR service lead for the service areas under their responsibility. All of the GDPR Service Leads have now been identified and there are 57 Leads across the authority with high risk areas having a number of such Leads.

3.3.10 The 9 technical work streams each have their own work stream lead from within the Information Management and Governance Service and are producing outcomes in the form of tools; briefing notes; new or revised policies and procedures; changes to terms and conditions; or changes to procedures. All of the outputs are to be rolled out to the GDPR Service Leads via the GDPR Implementation Guide (“the Guide”) which explains what the business needs to do under the 9 technical work streams and where support for this can be found. At the time of writing this report, the first version of the Guide has now been released and this contains two tasks: the 7 steps to preparing for GDPR and a record of processing activities of which there are 92 in total to account for all the delegated functions. The Guide can be found on Insite where a dedicated GDPR tile has been established as part of a comprehensive communications programme. Further tools to be released in future versions of the Guide include:

- a revised data protection policy;
- a data quality policy;
- a briefing note on consent;
- a privacy notice generator;
- a new Data Protection Impact Assessment form with accompanying guidance;
- new procedures for managing a security incident;
- new procedures which govern how individuals can exercise the rights contained within the GDPR; and
- new terms and conditions when the Council is contracting with a Data Processor or Data Controller.

3.3.11 The GDPR requires the council, as a public authority, to designate a Data Protection Officer (“a DPO”). The main tasks of the DPO are: to inform and advise the council of its obligations under GDPR when processing personal data; to monitor compliance with the GDPR; to provide advice where requested, particularly, with regards to data protection impact assessments and other high risk processing activities; and to act as the contact point with the supervisory authority (the ICO). Furthermore, the GDPR establishes some basic guarantees to help ensure that DPOs are able to perform their tasks with a sufficient degree of autonomy within their organisation. The Council’s Head of Information Management and Governance (Louise Whitworth) has been appointed as DPO. This decision was ratified by the Information Management Board on 9th August 2017, the appointment being made with immediate effect.

3.3.12 Regarding the area of Information Access and Compliance the Committee can be fully assured that process and procedures are in place to ensure that statutory requests are responded to within the ICO’s and the council’s thresholds for response times. The Committee can also be fully assured that work is satisfactorily

progressing, under the governance of SIB, to meet the requirements of the new data protection framework.

### 3.4 Records Management

- 3.4.1 Following the ICO audit in 2013 the Council prepared and is delivering against a phased project plan and continues to make good progress in the implementation of the Information Asset Register (IAR) and raising awareness of the role of Information Asset Owners (IAO's).
- 3.4.2 As previously reported phase one of the plan is completed and all Directorates have identified their assets, nominated IAOs at a Head of Service level and this information is published on the IAR.
- 3.4.3 Work on phase two to embed the role of the Asset Owner is now well underway. A robust methodology for implementing the Information Asset Register and the role of the Asset Owners has been approved by the Information Management Board and all training materials have been refreshed and reviewed in readiness for a themed CLT workshop scheduled for the beginning of April 2018. This event will be opened by the Council's Senior Information Risk Officer (SIRO), Neil Evans. As well as launching the Information Asset Register the event will also illustrate the wider importance of records management and its importance to ensuring compliance with the General Data Protection Regulations (GDPR) and make people aware of their roles and responsibilities in relation to managing information.
- 3.4.4 Following the event all Records Managers will work with their respective directorate asset owners to help analyse their information assets and also identify associated risks which will feed into the council's wider risk management process.
- 3.4.5 The Records Management Team continue to monitor their annual work plan and aspire to improve and ensure consistency of records management approaches across the whole organisation and maintain compliance with the Data Protection Act/GDPR.
- 3.4.6 Other key priorities identified last year have all been progressing well as detailed below:

**To ensure that all records are managed effectively as part of the Changing the Workplace (CtW) programme in line with designated methodologies;**

Information Audits have been conducted for all services that have been or are subject to a CtW move to ascertain paper storage requirements and recommendations for future paper storage;

***Ensure consistency in the management of employee records across the council to ensure compliance with the DPA principles;*** A discovery project has been completed to ascertain the inconsistencies in approach council wide in relation to the management of employee records. The findings have been risk assessed and presented back the Chief Officer of Shared Services and other senior officers in HR for consideration and implementation;

**Ensure that all scanning and digitisation provision by the scanning framework is effectively monitored, justified and co-ordinated;** The team have led on and co-ordinated a number of scanning and digitisation projects in 2017/18 all justified in terms of ensuring compliance with the GDPR, enabling asset release and generating efficiency savings including:

- Digitisation of 57,000 Housing Leeds Live House files and all garage files onto a central repository with built in search and retention management capabilities;
- Digitisation of HR records which have enabled the asset release of Belgrave House;
- Digitisation of 1,100 client files belonging to the Estates and Deputyship Team, Adult Social Care to enable the imminent CtW move.

**To cleanse the data and reduce the storage on our existing network drives and mitigate the risk of breaching DPA principles; Discovery and cleanse;** The Discovery and Cleanse tool which is being developed by the Change and Initiative team and DIS ICT is almost complete. Once this tool is available the Records Management Team will be trained in its use and work can commence with services to cleanse network drives. This work will be carried forward into the 2018/19 plan.

**Improve Paper Records management to enable effective management, tracking movement and destruction of paper records owned by LCC and reduce unnecessary storage costs;**

Over the summer period the Records Management team completed a “paper mountain” project that focused on improving the management of the paper records identified as ‘high risk’ as part of the Changing the Workplace (CtW) programme. As a result thousands of paper records were sent for destruction or were organised for appropriate storage in line with the council’s records management policy and the Data Protection Act.

- Adult Social Care Records – 68,000 files checked for data quality and over 33,000 records held in Westland Road were identified for destruction due to them being beyond retention;
- Leonardo Basement – 946 linear metres of paper records sifted, archived or disposed of and 20,000 planning files sifted and prepared for scanning;
- Knowsthorpe Gate – 103 metres squared of space cleared through the appropriate destruction and correct archiving of appropriate records;
- Taxi and Private Hire - Over 4,000 vehicle files scanned;
- HR – Weeded 1,500 records in readiness for scanning
- Children’s Services – 16,000 files prepared and archived from Adams Court;
- Entertainment and Licensing – 3,100 files scanned freeing up 71 linear metres of space.

Funding has been allocated to conduct a project which seeks to explore and replace the various record management databases that monitor the management of records across the organisation to enable a cohesive and more compliant approach.

**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;** Awareness raising amongst Information Asset Owners is incorporated into the Information Asset project. In addition to this work to raise awareness across the wider organisation remains ongoing. Training material has been prepared in readiness for the forthcoming Information Management and Governance Training for elected members in May and June 2018 and the team are currently in the process of developing an in house records management training session for roll out to other council officers.

**Development of the Council's Retention Schedule;** The ongoing work to develop the Information Asset Register and role of Information Asset Owners includes the examination of retention periods. Historically the council's retention schedules have been published in PDF format on the Council's Intranet site. The presentation of these retention schedules has been simplified this year to enable staff understand the relevant content and also find what they require much easier. The new look retention schedules are to be launched by the end of March 2018. This will be followed up with a review of the retention schedule which will be challenged and assessed by Legal Services.

3.4.7 The Records Management Plan is scheduled to be reviewed and updated in April 2018 to reflect the changes in legislation and any organisational changes. Work has already commenced to develop specific objectives to ensure compliance with data minimisation and data quality requirements of the GDPR.

3.4.8 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; 18th March 2016; 7<sup>th</sup> April 2017 outlining progress made to date.

3.5.2 Work on twenty seven of the thirty two recommendations is complete and actions embedded into information governance standards and/or practice. The remaining five recommendations constituted an investment in some fairly significant work, and since the recommendations were made, the changes which have come about (particularly GDPR and PSN) have meant that these actions have been subsumed

into other projects. Progress is being made, but the direction of travel has had to reflect the changes to compliance regimes and therefore is taking longer to implement than previously anticipated. Appendix A outlines the outstanding recommendations, action to date and the project / workstream now tasked with its completion.

- 3.5.3 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 2019 and the Head of Information Management and Governance will continue to monitor progress.
- 3.5.4 Corporate Governance and Audit Committee considered a report in September 2016 providing assurance about our continued compliance to the Department of Communities and Local Government'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 Local Government Association and are informed of any potential changes to this Code.
- 3.5.5 The council continues to proactively publish datasets over and beyond that required by the Local Government Transparency Code 2015, however Committee should note that responsibility for the Open Data agenda transferred from the Head of Information Management and Governance to the Smart Cities team during 2017, and it is this team who now have responsibility for the proactive publication of the council's datasets.
- 3.5.6 The Change and Initiatives Team are working to a programme of work that aspires to improve how and when information governance is implemented and embedded across Leeds City Council, through a series of initiatives, in collaboration with services across the council and in collaboration with partners from across the wider local region. The team has built a series of Information Governance frameworks which have been used to implement information compliance and governance for projects such as the Activage project and to implement work to comply with the Gender Reassignment Act 2004. The work undertaken for the Activage project has provided the team with the opportunity to produce a generic Information Governance framework for all future projects involving Internet of Things initiatives. The team are currently working with DIS colleagues to develop an information governance framework to support the council's mobility programme, and ensure information compliance around the use of mobile devices.
- 3.5.7 Members of the Change and Initiative Team are representing the council on a regional programme to rationalise and standardise an approach to information sharing across the Yorkshire and Humber region. The Information Sharing Gateway was initially developed by Morecambe Bay NHS Foundation Trust, and has now been rolled out across a number of regions across the United Kingdom. The Information Sharing Gateway is an online portal that brings together a number of stages that support effective Information Sharing. Sixteen public authorities went live with the Gateway on 1<sup>st</sup> February 2018 and all new Leeds City Council information sharing agreements will be processed and stored on this platform,

providing a controlled and assured approach to information sharing by all signatories to each information sharing agreement. The Change and Initiatives Team have provided training on the Gateway to council staff, as well as, staff from other authorities. Recently the Information Management Board approved a member of the team to act as a regional 'Super-User' of the Gateway for member organisations across West Yorkshire. Further developments of the Gateway platform in the near future will mean that it will support other information related work at a regional level, and will act as an auditing tool to demonstrate compliance with legislation such as the General Data Protection Regulations.

#### 3.5.8 Priority areas within the work plan also include:-

- Ensure all necessary information governance requirements are considered to ensure the success of the City's Personal Healthcare Record (PHR) pilot. The aim of the PHR initiative, is to enable citizens to hold and manage medical information about themselves, in a safe, secure and governed space and the Change and Initiatives team are acting as lead IG advisors and support to the project;
- Monitoring the uptake of the council's new Movers and Leavers Guidance checklists and recommending any improvements which may become apparent and required;
- Development of an Information Security Standards publication to identify and group common elements of each standard by type in order to eliminate duplication of effort in demonstrating compliance;
- Development and management of an updated version of the IG e-Learning solution which will include information about GDPR and Cyber Security, for the mandatory staff training programme, which is to be rolled out in April/May 2018 just ahead of GDPR date of 25<sup>th</sup> May. The Change and Initiatives Team has successfully sold version 2 and 3 of this product to all public authorities across the Greater Manchester region, and at the time of writing, has other public authorities interested in purchasing this product;
- The development of the Discovery and Cleanse tool designed to identify and report on all information stored on the council's shared drives, with the ability to automatically cleanse some selected material. The project is near to completion and the team are confident that the product will be available to use by summer 2018. Use of this tool will enable the council to understand what information it stores; where this is; when it was last accessed; and, who owns it. This will help to demonstrate compliance against GDPR and provide assurance to the council in respect of what information assets it holds and the location of each information asset.

#### 3.5.9 In respect of the INSPIRE standards it is still unclear which direction the UK Government will take with this Directive and no information has been forthcoming from DEFRA. A full review and consultation of how the council should move forwards with a strategy for GIS (Geographic Information System) is being undertaken for the council by SOCITM Advisory, and the statement of requirements for this review include providing recommendations about how the council should

proceed with implementing INSPIRE data standards. No further work is being undertaken in relation to INSPIRE until these recommendations are received in the final report.

3.5.10 Throughout 2017/18 the Change and Initiatives Team provided Information Governance support to other organisations bringing income into the Digital and Information Service. This included the provision of classroom based information training and advisory support to West Yorkshire Joint Services and the preparation and undertaking of an information governance audit for West Yorkshire Combined Authority.

3.5.11 The Change and Initiatives Team are committed and dedicated to the development of products and solutions to ensure the council remains compliant with information governance related legislation, standards and regulations, and to promote the expertise and experience of the Information Management and Governance service to partners and other organisations.

## **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 All Information Governance related policies are currently being reviewed and a dedicated Policy Review Group has been established. As part of this review the Group will be consulting with internal stakeholders and external peer checking.

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 Legal Implications, Access to Information and Call In**

7.1 Delegated authority sits with the Director of Resources and 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.

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

## 8 Risk Management

- 8.1 Should action against the current PSN Remediation plan not be to the satisfaction of the PSN Authority, the Council will have to withstand a number of risks:
- The Head of the PSN has informed the Department of Works and Pensions of our non-compliance. Continued non-compliance could culminate in the switching off of GCSx mail and access to Revenues and Benefits data.
  - The Head of PSN will inform the Information Commissioners Officer, which could culminate in the revisiting of the audit conducted by the ICO in 2013 to ensure compliance against the Data Protection Act.
  - The Head of PSN will inform the Deputy National Security advisor to the Prime Minister, who would in turn conduct an assessment based on the national risk profile.
  - The Head of PSN could instigate an external audit of all our security systems by the National Cyber Security Centre. The Council could end up under partial commissioner control.
  - Ultimately, the Head of PSN could instigate a complete 'switch off' from PSN services
- 8.2 PSN certification is relied upon as an assurance 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 required for the NHS Information Governance Toolkit are evidenced by a PSN certificate.
- 8.3 Without a PSN certificate, there is significant risk to the council's National reputation as a Digital Innovator.
- 8.4 The risk associated with not implementing GDPR compliant 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.
- 8.5 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.
- 8.6 Further work is being undertaken in conjunction with the Corporate Risk Manager to embed the recording and reporting of information risk monitoring and management relevant to this project. 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.



## **9 Conclusions**

- 9.1 The work of the previous year, reported to this Committee on 7<sup>th</sup> April 2017, has been continued.
- 9.2 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.

## **10 Recommendation**

- 10.1 Corporate Governance and Audit Committee is asked to consider the contents of this report and the assurances provided as to the Council's overall approach to information governance.
- 10.2 Corporate Governance and Audit Committee is asked to be assured that considerable effort is being undertaken to rectify the current situation with regards to the Council's approach to Cyber and PSN compliance where significant progress has been made.
- 10.3 Corporate Governance and Audit Committee is asked to be assured of the Council's approach to implementation of the changes required to achieve compliance with the new Data Protection legislation from May 2018.

Background documents None

## Appendix A

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

<b>No</b>	<b>Recommendation</b>	<b>Current position as at February 2017</b>	<b>Project/ Workstream</b>	<b>Completion</b>
1.	A6. Ensure IAOs are trained in line with proposed plans. Further advice on IAO training is available from The National Archives.	Training material has been refreshed and the methodology for working with Information Asset Owners is agreed and determined. All Information Asset Owners have been invited to attend an Information Asset Register / Owner launch event in April 2018. Records Managers will then commence work with each Asset Owner on a 1:1 basis to embed their role and work with them to identify and analyse their assets and identify areas of risk to populate a risk management programme aligned to the council's risk	Records Management	31 Mar 2019

		management arrangements.		
2	A23. Introduce a standard procedure for signing files out of the office and ensure the file returns are monitored.	This has been completed in a number of services across the council on an ad-hoc basis. There is no standardised corporate procedure in place. This will form part of the RM plan for 2018/19	Records Management	31 Mar 2019
3	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.	All high and medium risk buildings have now undergone an audit and remediation plans put in place where required. The process for low risk buildings has been established, although is still to be embedded. As a consequence of changes to the national security status over the last 12 months, the Council's Building Security Policy was revised and endorsed by the CIO.	PSN	31 March 2019
4	A51. Ensure that PIAs are embedded across the Council at the	New Data Protection Impact Assessment forms	GDPR	31 <sup>st</sup> May 2018

	implementation stage of any projects involving the processing of personal data.	are designed to ensure compliance with GDPR. A new procedure to replace existing processes is to be introduced across IM&T hubs to embed DPIA's in the cultural practices of services across the council. To a large extent, work undertaken in the last two years has increased the use of PIA's by officers in projects and change management activities.		
5	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	As per item two above.	Records Management	31 Mar 2019

	reviewed.			
6	<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>The council has implemented a guidance checklist for managers with staff either moving across the council or leaving the organisation. The guidance checklists were approved by Information Management Board in October 2017 and Best Council Leadership Team informed in January 2018. The Guidance Checklist are published for managers to use on the BSC pages of InSite along with other related guidance for managers.</p>	Completed	31 Dec 2017