Report author: Louise Whitworth &
Shona McFarlane
Tel: 0113 37 83978

Report of Director of Resources and Housing and the Director of Adults and Health
Report to Corporate Governance and Audit Committee

Date: 16th March 2020

Subject: Annual Information Governance Report, including the Annual Report of the Caldicott Guardian

Are specific electoral wards affected? If yes, name(s) of ward(s):	☐ Yes ☒ No
Are there implications for equality and diversity and cohesion and integration?	☐ Yes ☒ No
Is the decision eligible for call-in?	☐ Yes ☒ No
Does the report contain confidential or exempt information? If relevant, access to information procedure rule number: Appendix number:	☐ Yes ☒ No

Summary of main issues

This annual report presents assurances to the Corporate Governance & Audit Committee on the effectiveness of the council's information management and governance arrangements: that they are up to date; fit for purpose; effectively communicated and routinely complied with. It explains the current arrangements and an update on programmes of work undertaken during 2019/20.

The Caldicott Guardian is assured of the arrangements in place with regards to the confidentiality of patient and service-user data.

Recommendations

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 management and governance.

1. Purpose of this report

1.1 To provide Corporate Governance and Audit Committee with an annual report on the steps being taken to maintain and 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.

2.3 The manual for Caldicott Guardians, produced by the Caldicott Guardian Council (2017), recommends that the Caldicott Guardian works as part of a broader Information Governance function with appropriate support

3 Main issues

3.1 Overall arrangements for Information Management and Governance (IM&G) 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 Senior Information Risk Officer (SIRO). The Head of Information Management and Governance meets monthly with the SIRO to keep him up to date and also has active support regarding high risk matters. The SIRO is supported by the Chief Digital and Information Officer who has delegated decision making powers for information management and governance. The Chief Digital and Information Officer chairs the Council's Information Management Board (IMB) 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 who work closely with the Heads of Digital Change and the Digital and Information Services (DIS) Hubs. Reports and updates are taken to Hub and / or directorate level Steering Groups as appropriate.

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. Meetings are held with the Caldicott Guardian on a monthly basis to give updates on information sharing arrangements between health and social care partners, staff training and any high risk matters.

3.1.4 The Council's Head of Information Management is the Council's Data Protection Officer (DPO). The General Data Protection Regulations (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 Information Commissioners Office (ICO)).

3.1.5 The Head of Information Management and Governance also oversees the effective underpinning of the Council's operations in the following areas:

- 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 This professional strand deals with the management of information and data risk corporately and manages the corporate risk for Major Cyber Incident. The compliance regimes mandated by the Council's regulations, contracts, information sharing and connection agreements are numerous and include the Public Services Network (PSN) Code of Connection, Data Protection and Security Toolkit for Health and a number of others which, in part, are addressed by PSN Compliance. As such, section 3.2 of this report concentrates on compliance to PSN.

3.2.2 The Public Services Network (PSN) was set up as an assured route for information sharing by central Government to facilitate shared services. 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. It is expected as Central Government services become accessible over the internet that the requirement for PSN services will diminish, removing the requirement for PSN compliance. We are however, assured by Central Government that a replacement compliance regime will follow. The controls are expected to be similar, but may be more stringent as Cyber threats are always changing.

3.2.3 PSN accreditation was awarded in 2018 and in 2019 with the assurance that the Council will remove Access databases running on 2003. Corporate Governance and Audit Committee are monitoring the progress of this separately and is therefore not documented in this report.

3.2.4 Governance for IT Security and Information Assurance is managed by the Information Security, Assurance and Compliance (ISAaC) Group. Following an internal audit on the management of cyber risk, this Group has been expanded to include delegates from Finance, Procurement, Facilities and HR. New Terms of Reference are being trialled to include scorecard reporting to improve the measurement of cyber risk and management. This group meets four-weekly and addresses the programmes of work in place to improve compliance to the PSN standard, including the output from the IT Health Check (ITHC), the projects that

affect cyber risk and other aspects of information Security. Escalation is to the Information Management Board (IMB).

3.2.5 Vulnerabilities discovered as a result of the ITHC over the past two years are reducing year on year. Due to this lower volume the Digital and Information Service (DIS) is now able to focus on assessing the root cause of issues that arise. Improvements to process are being implemented operationally and the adoption of virtualised teams is supporting this work. This moves the maturity of the organisation forward, allowing more focus on resolving long-standing issues.

3.2.6 DIS continues to utilise an automated scanning engine which lists vulnerabilities found on the estate allowing DIS to push updates to devices ahead of the ITHC which provides an external check of this control.

3.2.7 The windows server estate is being maintained above 90% compliance which is an acceptable level for the PSN regulators.

3.2.8 The Council's IT service management system, Remedy, is being utilised to ensure correct closure codes are appropriated to pieces of work, to provide improved reporting, but also to ensure business as usual activity that contributes to PSN compliance can be managed.

3.2.9 Work to ensure the secure boundary is maintained by upgrading all firewalls has been completed this fiscal year.

3.2.10 There are however, a number of projects yet to complete, which will further strengthen the security posture of the technical environment and may affect PSN Compliance:

a) Mobile Device Management – Upgrades to the majority of compatible mobile devices has been completed. A number of devices are too old to accept the upgraded controls. As the lifecycle for mobile devices continues, central funding of upgrades has been sought and agreed; this funding is in place for three years and is expected to be approved in the following years. This will ensure timely upgrades without impacting on services' budget. This project is being managed as business as usual.

b) Network Segmentation / Authentication – The network access control (NAC) product, which prevents unauthorised devices from getting on to the network, has been deployed within the Leeds City Council environment. All known devices are now understood by the system. Phase two of this project requires remediation networks to be created. Therefore, if a device does not meet the council's predetermined compliance criteria, including patching levels, then it is virtually placed in a separate network, which prevents access to corporate assets. The device will then be patched if identified as a corporate device, or quarantined (will only be granted internet access) until such time as the risk has been reduced, following which the device will be released onto the corporate network.

c) **Active Directory Management** - This remains a large piece of work to maintain the structure of the role based access controls in place at standard user level. The work to ensure people have only rights and ability to see the information they need to complete work activity. Active Directory management software will be procured to assist in this ongoing task.

d) **Microsoft 2008 lifecycle –** This project aims to upgrade unsupported servers and data bases to meet compliance requirements. In 2019, extended support was purchased to ensure compliance, this will run out for some of the devices in August 2020, the other in January 2021. Service areas are required to engage with DIS to ensure their hardware is upgraded.

e) **Corporate reporting tools –** This project looks to standardise reporting and decommission aging reporting tools such as e-discoverer which impact on PSN compliance. Reports are being built at an acceptable rate and the out of support server was decommissioned in February 2020.

f) **Customer Access Transactional Services (CATS) –** This project looks to replace and decommission non-compliant systems in Customer Access. The complexity of the forms required for the service result in slow progress, however this project will be delivered in Microsoft's Azure which brings with it a new support model.

g) **Cloud Security Principles -** The Cloud Security Principles (CSP) compliance project was initiated to assess the security arrangements for those applications currently in use by Leeds City Council where they are hosted in the cloud. 64 applications have been assessed out of a total of 74. One has already been replaced due to security concerns. This work continues, producing remediation plans for those not felt to meet full compliance, but where it is felt that the risk can be managed. Contract management & supplier engagement are concerns for some systems.

h) **Active Directory Raised Privilege Accounts** – Raised privilege accounts are those that afford greater authority within the estate, allowing the account holder to make changes to the configuration of devices and services within the council's network. Following an internal audit realising a need for improvement, a project has been instigated which will address the findings of the report. DIS recognises there are other actions required to bring the management of raised privilege to an acceptable assurance control and will continue to close-out gaps beyond the scope of the audit report, but ensuring the audit findings are closed first. It is understood that activities will be dependent upon what tooling can be procured, as such only high level actions are documented at present. This project is expected to take at least 2 years to complete due to the complexity of activities across services, including aspects of people, process and technology. Cabinet Office are aware of issues with Active Directory and continue to support us in our compliance to PSN.

High Level, documented plan to date:

Raised Privilege Project	Commence	To Complete	Completed
Identify and Procure Tooling Solution			
Supplier Meetings	07/01/2020	21/02/2020	Y
Requirements Matrix	21/02/2020	28/02/2020	Y
Product Trialling	02/03/2020	30/03/2020	
Produce Options Paper	02/03/2020	30/03/2020	
Procurement	01/04/2020	30/09/2020	
Communication Plan	01/08/2020	30/09/2020	
Establish Technical Solution/Prototype	01/10/2020	30/03/2021	
Communication Plan	01/08/2020	30/03/2021	
Installation	21/04/2020	30/03/2021	
Training and configuration	01/05/2020	30/03/2021	
Draft Implementation Plan	01/05/2020	30/03/2021	
Implementation	01/06/2020	30/03/2021	
Documentation/OAC as part of implementation.	01/06/2020	30/08/2021	
Phase 1 Services (AD) Infrastructure Mgmt	01/06/2020	30/08/2021	
Phase 2 to be determined based on relative importance	01/01/2021	30/08/2021	
Phase 3 Workstations	01/04/2021	30/08/2021	
Closure			
Lessons Learned			

It is expected that the findings of the internal audit will be closed out by August 2021.

3.2.11 The 2020 ITHC report has been analysed and it is likely that new projects will be commissioned to address root causes, these will be added and reported to Corporate Audit and Governance Committee as required.

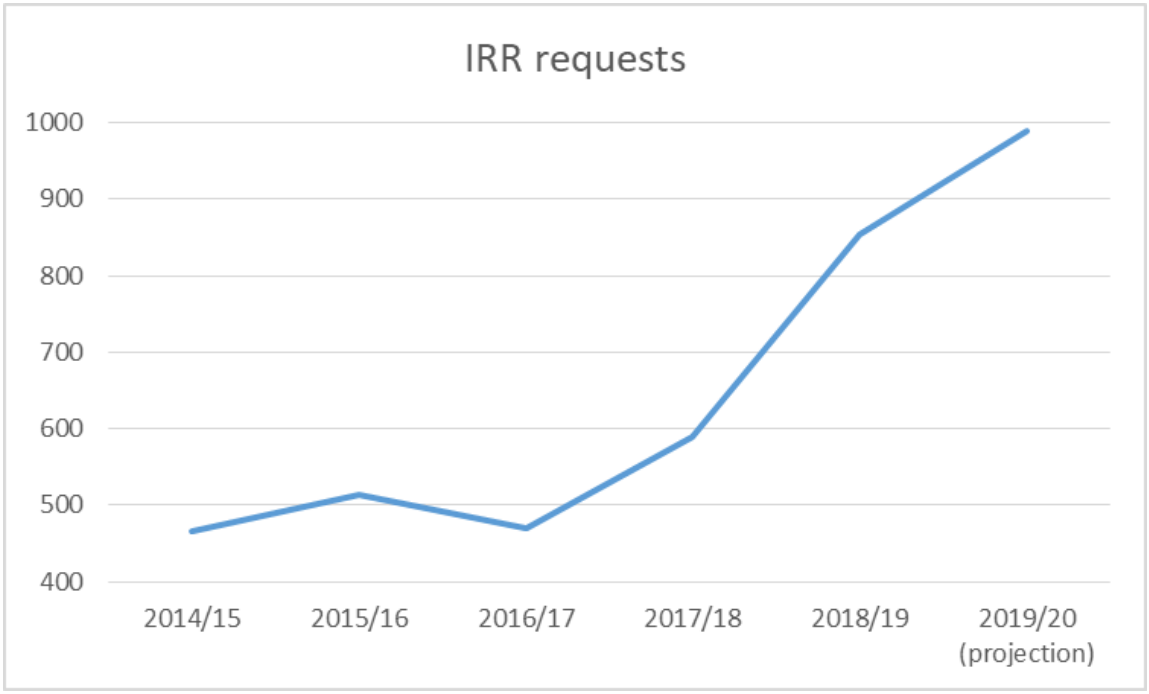
3.2.12 Due to ever increasing maturity of information assurance and compliance, including but not limited to, the re-prioritisation of workloads, a centralised Compliance Programme, improved process, increased reporting and the ISAaC Group new ways of working, Information Management and Governance have increasing confidence that Leeds City Council will maintain the required standard for PSN compliance in July 2020.

3.3 Information Access and Compliance

3.3.1 A central requests team has been established within the Information Management and Governance service (IM&G) to respond to all statutory requests for the Council, which previously had been dealt with by directorate IM&G hubs. This team currently consists of 1 PO4, 1 PO2, 6 SO2's (one part time 32hrs), 2 B3's and 1 apprentice post. The team respond to all requests, which include Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIRs), General Data Protection Regulation (GDPR) & Data Protection Act 2018 (DPA), as well as requests from the police, the courts, and other government bodies.

3.3.2 Individual Rights Requests

Below is a trajectory of the number of individual rights requests (IRR's) received by the Council since financial year 2014/15 to 2018/19, with projected figures for 2019/20 based on the first three quarters of the year. 98% of IRRs are subject access requests (SARs).



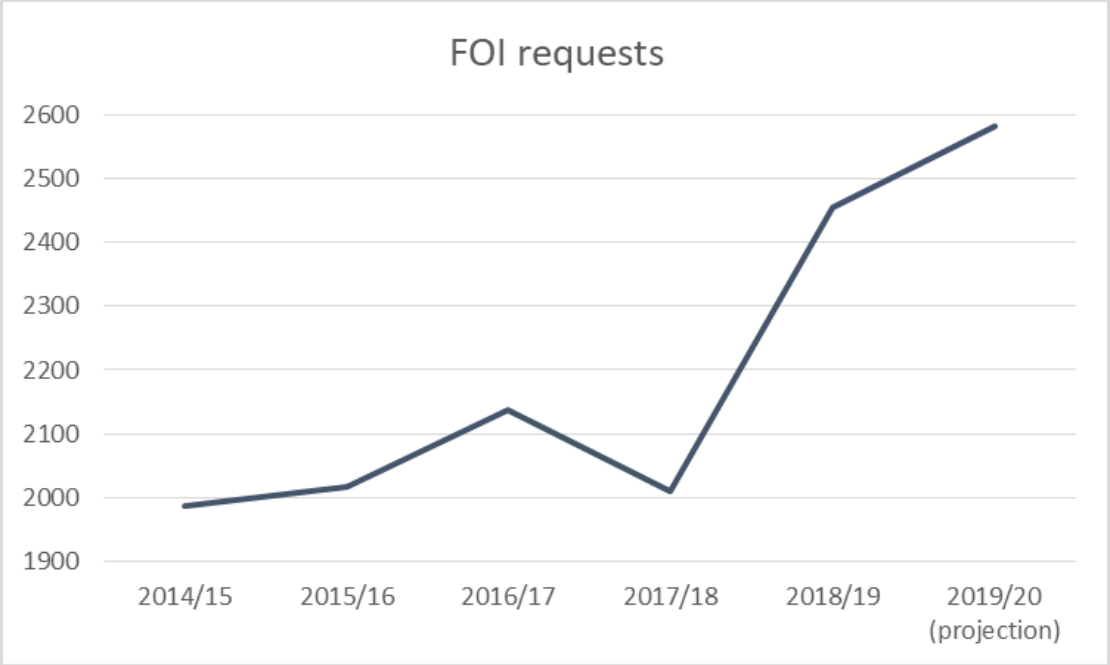
3.3.3 Since GDPR & DPA18 the Council has seen a 68% increase in the number of IRRs received. Although a spike was predicted when the legislation became enforceable in May 2018, the number of IRRs is not diminishing. At any one time the council has on average 75-80 open IRRs. Within the year 2019/20 this has peaked at 98 open requests. The average page count this financial year for SARs is 1,264.

3.3.4 48% of IRRs are for access to historical children's social care records by the individual who was in care. Due to the sensitive nature of these records the requests are highly complex and frequently run into thousands of pages, with the largest this financial year at 13,391 pages. Every page has to be read and decisions made in respect of applying the GDPR/DPA including redaction, with some extremely difficult information in respect of child protection matters.

3.3.5 In financial year 2019/20, to date 83.4% of all IRRs have been sent within the statutory deadline of 1 calendar month (a table is provided at 3.3.9). The Council has previously been monitored by the ICO for its compliance with subject access requests.

3.3.6 Freedom of Information/ Environmental Information Regulation requests

Below is a trajectory of the number of Freedom of Information (FOI) and Environmental Information Regulations (EIR) requests received by the Council since financial year 2014/15 to 2018/19, with projected figures for 2019/20 based on the first three quarters of the year.



3.3.7 FOI/ EIR legislation did not change when GDPR became enforceable, however the numbers of requests received has increased 29% since this time. At any one time the council has 130-140 FOI and EIR requests open. In 2019/20 the amount open at one time peaked at 170.

3.3.8 In financial year 2019/20, to date 93.2% of all FOI and EIR requests have been sent within the statutory deadline of 20 working days. The ICO threshold for monitoring of organisations is when it is found that compliance is below 90% responded to within statutory timescales.

3.3.9 The table below sets out the numbers of requests received and handled by the council for both the DPA 1998 (and GDPR post May 2018) and FOIA during 2017-18, 2018-19 and figures to date for 2019/20.

	2017/18	**% compliance to statutory timescale**	**2018/19** **Note: from May 2018, these figures include the new rights under GDPR**	**% compliance to statutory timescale**	**2019/20**	**% compliance to statutory timescale**
DPA / GDPR – subject access requests & new rights requests post May 2018	590	97	855	90	748 (to Dec 2019)	83.4
FOIA & EIRs requests	2009	97.9	2455	93.5	1938 (to Dec 2019)	93.2

3.3.10 Police, Court & CCTV Requests

The Council receives on average 120 requests per month from the police, other local authorities, HMRC and the Home Office for access to information, primarily to assist in the prevention, investigation, detection or prosecution of criminal offences. There are no indicators to show that these requests will reduce. The requests vary in their complexity from a quick address check, to arranging access to social care records, which involves access to paper and electronic files in the office. The time taken to process police requests is significant, with 1 full time B3 officer, and the 1 apprentice post dedicated to responding to these requests full time each week. To support responding to these requests along with the other workload at support officer level, other IM&G hub resource (1 apprentice and 1 B1) have been brought into the requests team.

3.3.11 ICO & Internal review cases

If a requester is unhappy with the initial response to or handling of their request they are able to ask for an internal review at stage 2 of the council's complaints policy. Currently the PO4 and PO2 officer are responsible for responding to these reviews. To date this financial year the council have received 90 internal review requests for IRRs, FOIs, and EIRs, the highest open at any one time being 23. The time taken to respond to internal reviews is significant due to their complex nature.

3.3.12 Requesters are also able to contact the information commissioner's office if they have concerns about the way the council have responded to their request. This financial year to date 15 requesters have raised complaints against the council to the ICO. Of the 15 some are persistent complainants who have raised a number of concerns with the ICO over the course of several years. The ICO give the council 10 working days to respond to any concerns they receive, and a substantial amount of the capacity of the PO4 and PO2 officer within the team is required to respond to these concerns.

3.3.13 The Council is currently struggling to respond to IRR and FOI/EIR requests within the statutory time limits primarily on account of the volume of requests and the amount of staff allocated to undertake these requests. The requests team are working at full capacity, however the demand is too high for the team to sustain this level of requests within statutory guidelines. Attempts have been made to improve compliance statutory obligations by utilising colleagues from elsewhere within Information Management and Governance, and employing agency staff, however this is not a long term solution.

3.3.14 As such a plan has been put in place to ensure compliance with statutory obligations can be met and to prevent potential enforcement action from the ICO.

3.3.15 Additional permanent staffing allocation of 1 PO2, 1 SO2, 1 B3, and 1 B1 have been approved to sustain the council's compliance with all requests at each stage. Recruitment will commence with immediate effect once the additional posts have been established on the Council's structure.

3.3.16 The Digital and Information Service has commissioned an external resource to assess the current operation and processes of the team to see if efficiencies can be made to further improve performance and possibly automate some tasks. This work started in the first week in February and is due to conclude by the end of March 2020.

3.3.17 Corporate Govenance and Audit Committee can be assured that every effort has been taken to provide for greater resilience in handling the large number of information requests the Council receive.

3.4 Records Management

3.4.1 The Council continues to make progress against the phased project plan to implement the Information Asset Register (IAR) and raising awareness of the role of Information Asset Owners (IAO's) council wide.

3.4.2 Phase one was completed in 2018 where all Directorates identified their assets and nominated IAOs at a Head of Service level.

3.4.3 Work on phase two to embed the role of the Information Asset Owner has progressed exceptionally well using the approved methodology launched in April 2018. Some slippage has been incurred with finalising this work as a result of under-estimating the time required to conduct this extensive exercise. Records Managers have spent the past 18 months working intensively with their respective directorate IAOs to help identify, validate and analyse their information assets (including those on the council's network drive). Work has also progressed to identify associated risks with each asset which will feed into the council's wider risk management process.

3.4.4 As at mid- February 2020 over 1,100 assets have been identified council-wide and are now on a purpose built Information Asset Register. The review of the Information Asset Register was approved at the Information Management Board on 12th February 2020.

3.4.5 The Records Management Team also 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 2018/GDPR.

Key priorities identified last year have all been progressing well as detailed below:

a. **To ensure that all records are managed effectively as part of the Changing the Workplace (CtW) programme in line with designated methodologies;** All phase 1 and phase 2 moves have been successful. Phase 2 office moves have included decanting both Hough Top Court and Navigation House.

   A series of further office moves have been announced by Asset Management which the Records Managers are now supporting. Asset management are now working in collaboration with the Records Managers to ensure they are aware of all forthcoming office moves and decants with an adequate notice period;

b. **Conduct procurement for the provision of an external storage provider** – A new three year contract has been put in place with Iron Mountain. This contract commenced in June 2019.

c. **Development of a Council Data Quality Policy Statement and supporting protocols and guidance** – The Council's Data Quality Policy Statement was

finalised and approved in April 2019. Work is now ongoing to develop the supporting protocols and guidance to support the statement.

d. Ensure consistency in the management of employee records across the council to ensure compliance with the DPA principles; Following a discovery project, a project brief was presented to the Best Council Leadership Team determining the scope of a "Managing Employee Records" project. Some initial work has been conducted on this, however elements of this will now form part of the wider Core Business Transformation project.

e. 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 further scanning and digitisation projects in 2019/20 all justified in terms of ensuring compliance with the GDPR, enabling asset release and generating efficiency savings using the Council's approved scanning framework including the digitisation of the Council's pension records and contaminated land records.

The scanning framework is due to expire in autumn 2020 and therefore work is now commencing to develop the relevant documents for a re-tendering exercise.

f. 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 corporate project to cleanse the Council's network drives has been completed.

Phase one the project focussed on the deletion of personal non – business related data (examples include holiday photos, music and movie collections). Staff deleted 2.5 million files in response to a targeted communications push urging them to remove these files in line with the Acceptable Use Protocol. During April 2019 the council experienced the first ever drop in the amount of files on the drives and staff appeared to be more accountable for their files helping to foster a culture change around information management. The project slowed down the growth of the files on the network drive from 0.8TB to 0.5TB (October 2019).

Phase 2 focussed on working with service areas to identify deletions by reviewing redundant, obsolete and trivial files (ROT) outside retention. During this phase thousands of files were identified on the drives which belonged in a case management system (these have since been migrated).

Throughout the project there were small scale deletions of unusable file types (temporary files) that are not required by applications or users. As the project drew to a close the focus shifted onto 'common records' such as time sheets and meeting minutes as there are a significant number of these residing on the drives and these hold no value and were beyond retention.

g. Improve Paper Records Management to enable effective management, tracking movement and destruction of paper records owned by LCC and reduce unnecessary storage costs; This priority continues but has changed in scope. The priority is now linked to the Council's three year paper records rationalisation programme.

Considerable work has continued in this area since the last report and there is now a clear 3 year paper rationalisation programme in place which targets all

"high risk" areas and also aims to reduce off contract spend, reduce paper records and is aligned to the council's asset release programme.

Over the 2019/20 Christmas period the Records Management team completed a project that focused on ensuring that all the Children's Services records (over 2,500 boxes) stored in Domestic Street in units at risk of flooding have been securely transferred into a more secure facility managed by contractors. This has also resulted in two units becoming free and available for the council to rent at an approximate cost of £12.5k per annum per unit.

- Work has been undertaken in the following areas to remove off contract spend with Restore Storage.
    - Planning Team – Approximately 850 boxes have all been re-boxed, re-indexed and transferred to a secure council premise in readiness for sifting and scanning later in 2020.
    - PPPU - 163 boxes
    - BSC – 115 boxes of employee advisory service records have been re-directed or destroyed as they are past retention.
- Property and Contracts - 14,500 unstructured electrical certificates stored in cabinets at Navigation House have been checked for data quality against the e record and prepared for storage at the Council's Westland Road document storage facility.
- Work continues to replace the various record management databases to enable a cohesive and compliant approach. A large scale data quality exercise is ongoing to cleanse the data held in the existing systems around file types and retention as well as conducting destructions on records which have passed retention that still remain in the system before any information is migrated.

h. 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 continues to be incorporated into the Information Asset project. In addition to this work to raise awareness across the wider organisation remains ongoing. Training material was included in the latest version of the IG e learning package and records management staff are involved in the ongoing content review of the training in readiness for the next version roll out. A records management / retention management session for elected members was held in May 2019. This year we are looking at the development of a bespoke records management package to cover the fundamentals of Records Management. This will be updated accordingly in line with the roll out of O365.

i. 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 retention schedules has been simplified this year and the new look retention schedules were launched in April 2018 and published on Insite. The review of the retention schedules is now in its final stages. Completed retention schedules have been forwarded to Legal

Services for approval. We are still awaiting approval on a number of schedules.

3.4.6 The Records Management Plan was subject to annual review in January 2019 and reviewed and updated in April 2019 and January 2020 to reflect the changes in legislation and any organisational changes. The work in this plan is prioritised and reflected in the objectives of the Records Management Team.

3.4.7 With regards to Records Management Corporate Govenance and Audit Committee can be assured that the Information Management and Governance Service continue to provide 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. All commitments are regularly reviewed and monitored by the Information Management Board. Additional priorities identified for 2020/21 include:

- Ensure suitability of applications in line with the requirements of the GDPR Article 5 (personal data shall be: "processed lawfully, fairly and in a transparent manner in relation to individuals")
- Conduct a review of the Records Management Policy and associated protocols and procedures in line with the IG Policy Review programme and O365 roll out.

3.5 Change and Initiatives

3.5.1 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.

3.5.2 As previously reported to Committee a number of Information Governance frameworks are in development to proactively deliver information compliance and governance for a range of programmes and initiatives. The team has worked with Smart Cities and the Government Digital Services', to test the capabilities of a new IG Framework for Internet of Thing's (IoT) devices through the GovTech programme initiated across Social Care and Housing last year. A positive reaction was obtained by all of the digital companies using the IG Framework, and a report will be considered by the Information Management Board later this year to approve wider use of the IG Framework as a corporate assessment information compliance tool for the installation of IoT's devices. Similar work is progressing on an IG Framework to assess the secondary use of personal data for business intelligence and analytical work, and the team continue to build an IG foundation to support the Transgender Project.

3.5.3 The Change and Initiatives Team continue to lead on projects to enable the Council to share information with Health and other public authorities. An annual assessment of the mandatory Data Security and Protection Toolkit for 2109/20 is nearing completion, which has to be submitted for assessment to NHS Digital by 31st March 2020. The Leeds Information Governance Steering Group comprises of IG professionals from most of Leeds' Health organisations, and members of the Change and Initiatives Team represent the Council on this Group, which is responsible for ensuring a consistent and standardised approach to information governance across the City. The team continue to provide IG support to the Leeds Care Record and HELM (Leeds Personal Healthcare Record). Furthermore, during 2020 it is likely that the team will be responsible for providing IG support to a new

initiative aimed at providing IG readiness for voluntary and third sector organisations applying for access to the Leeds Care Record.

3.5.4 The Change and Initiatives 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 (ISG) is an online portal that brings together a number of stages that support effective information sharing. Leeds City Council together with North Yorkshire County Council are coordinating actions to enlist public authorities from local government; health; police and fire and rescue sectors, in order to bring about a standardised and simplified approach to information sharing across the region. Funding was secured from the Yorkshire and Humber LHCRE (Local Health and Care Record Exemplars) programme for 2020, which secured 200 licences for use by public organisations across the regions. To date 41 organisations are signed up to using the ISG, of which some of these have registered a further 23 supported organisations involving 290 registered users.

3.5.5 A member of the Change and Initiatives Team has been nominated as the region's coordinator on the national ISG forums, which allows direct input into new developments and technical changes for the Gateway, and networking with the numerous other Gateway users across the country. Future developments include changes to allow Part 3 of the Data Protection Act 2018, Law Enforcement to allow more detailed use of the Gateway by law enforcement agencies such as the Police, Crime Commissioners, Prison Service and Probation Services; changes required to accommodate the Information Commissioner's new mandatory code of practice on data sharing; and hosting internal information sharing agreements. Use of the ISG for information sharing is now embedded in the Council's recently reviewed Information Sharing policy. The Change and Initiatives team continue to support LCC staff to use the Gateway for information sharing purposes.

3.5.6 Further priority areas within the Change and Initiatives work programme include:-

a) Implementation of new information sharing arrangements in the Registrars Service to ensure compliance with Part 5 of the Digital Economy Act 2017;
b) Implementation of compliance checklists for managers with staff leavers or staff moving across the Council. A communications programme was undertaken in 2019, and a survey has been launched in February 2020 to find out how effective the communications have been. Consideration of the survey returns will determine whether further work is required to embed the Movers and Leavers checklists across the council;
c) New content for the Council's staff IG e-Learning solution version 4 is being developed and the bi-annual mandatory training will be launched during an eight week period in September and October 2020;

d) A new IG e-Learning solution for elected Members was developed and launched on two occasions for use by the Council's elected Members. Unfortunately uptake of this training has been disappointing. Proposals are being developed for a further relaunch, comprising of alternative training methods to encourage Members to undertake the training, which will be following the local elections in May 2020. It is essential that councillors undertake IG training in order to protect themselves from unwittingly breaching data protection rules and bringing enforcement action against the Council or themselves;

e) Development of a process to implement cyber security training designed by the National Cyber Security Centre (NCSC) called 'Exercise in a Box'. This is an online tool which helps organisations find out how resilient they are to cyber-attacks and practice their response in a safe environment. A report outlining proposals to coordinate this training across the council is ready for consideration by DIS Senior Leadership Team on 26th February 2020;
f) The development of a three year workforce development and training programme for the Information Management and Governance Team to enable staff to acquire the necessary skills and knowledge in a planned and coordinated manner to assure the Head of Information Management and Governance and Chief Digital and Information Officer that the council has the necessary skilled workforce to meet oncoming information and digital challenges.

3.5.7 The Change and Initiative Team will each year receive new projects and initiatives to either research and/or develop for wider use across IM&G, DIS or the organisation, and 2019/20 has been no different. Two major new initiatives assigned to the team during this period include a request to develop a framework to assess digital and data ethical standards. A process for undertaking this work is in design mode and with the Head of Information Management and Governance for assessment.

3.5.8 Also with the Head of Information Management and Governance for consideration are plans to undertake further research on companies that are able to provide facilities to test live personal data, and pseudonimyse personal data. Testing data on systems and applications is an essential process conducted by the council, but undertaking such tests involving personal data on live systems is a risk, and so research is being undertaken as to whether there are facilities to do this in a controlled environment, and whether the same facilities might offer the council an opportunity to anonymise personal data without recourse to a third party under a contract.

3.5.9 The Professional IG Lead for Change and Initiatives continues to act as a chair at two regional Information Governance Groups; the Yorkshire and Humber Information Governance Group and the West Yorkshire Information Management Forum, which provides the council with the opportunity to share and standardise IG practice, along with obtaining early indicators of regulatory changes, or new information risks. This association has also brought benefits whereby invitations to attend Health Regional IG Group and a Greater Manchester Information Group have been eagerly accepted, bringing about further chances to network and collaborate on IG initiatives.

3.5.10 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.

3.6 Report of the Caldicott Guardian

3.6.1 The Caldicott Guardian assumes overall responsibility for ensuring the confidentiality of patient identifiable information and that the highest standards are maintained when handling such information.

3.6.2 The Council's Caldicott Guardian is the Director of Adults and Health. Due to the size of the Council and the complexities brought about by such a large organisation, this role has been sub-delegated to senior officers within the Adults and Health and Children and Families Directorates.

3.6.3 The Council's Caldicott function maintains a strong working relationship with the Council's Senior Information Risk Owner (SIRO) as the roles are regarded as complimentary to each other by the National Guardian Council. As such, both the Caldicott function and the SIRO are continually kept abreast of high risk data protection / confidentiality matters by the Information Management and Governance team and provide strong leadership and strategic guidance as appropriate.

3.6.4 The Caldicott function continues to be fully supported by the Council's Information Management and Governance (IM&G) Service particularly by those officers within the Adult's, Children's and Health IM&G Hub. This support includes but is not limited to:

- providing the Caldicott function with regular reports and briefings on high risk data protection and confidentiality matters. Such briefings cover information requests, such as freedom of information and data protection requests, and overall performance of requests; projects with IG implications; security incidents; and consideration of trends discerned.
- ensuring that there are stringent corporate and local Information Governance policies and procedures in place.
- ensuring that all staff handling personal data, and special category data, are suitably trained.
- ensuring that appropriate, proportionate, and accountable information sharing takes place and that barriers to sharing are addressed via advice, guidance or policy.
- ensuring that information governance risks are properly addressed through data protection impact assessments and that the appropriate supporting documents are in place, such as, information sharing agreements and contracts setting out data processing arrangements.
- ensuring that the Council's procedure for managing security incidents, including personal data breaches, is followed and that 'lessons learned' exercises are undertaken and remedial actions implemented, such as, revisions to practices and procedures, and reminder communications to all staff within the Directorates affected.

3.6.5 In the Corporate Govenance and Audit Committee of the 25th June 2019, the Caldicott Guardian was asked to provide an update at a future meeting, setting out the steps taken to undertake benchmarking with regards to the Caldicott function. The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

3.6.6 The Data Security and Protection (**DSP**) Requirements are ten standards applying to all health and care organisations. These are:

- Personal Confidential Data. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.
- Staff Responsibilities. All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
- Training. All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised Information Governance Toolkit.
- Managing Data Access. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
- Process Reviews. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
- Responding to Incidents. Cyber-attacks against services are identified and resisted and security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
- Continuity Planning. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.
- Unsupported Systems. No unsupported operating systems, software or internet browsers are used within the IT estate.
- IT Protection. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
- Accountable Suppliers. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

3.6.7 Organisations are scored as follows

- Not published – the organisation has not submitted a completed DSP
- Standards Not Met – the organisation does not meet all the mandatory criteria set by the National Data Guardian
- Baseline – the organisation has provided a baseline submission, but as yet does not meet all the mandatory criteria
- Standards not fully met action plan agreed – the orgnaisation does not meet all the mandatory criteria, but has an action plan, approved and monitored by senior leaders in the organisation, which will lead to compliance with the criteria within a defined timeframe (all organisations which submit an action plan are subject to increased rigour from NHS Digital).
- Standards Met – the organisation meets all the mandatory criteria set by the National Data Guardian
- Standards Exceeded – the organisation meets all the mandatory criteria, plus all the non-mandatory criteria set by the National Data Guardian.

3.6.8 Comparisons of other Local Authorities and local NHS organisations are given below (please note Local Authorities only submit once a year (March), whereas some NHS organisations are expected to submit twice a year (October and March).

Organisation	**Status**	**Date Published**
City of Bradford MDC	Standards Met	03/04/2019
Calderdale MDC	Standards Met	15/02/2019
Kirkless Council	Standards Met	25/02/2019
	Standards Met	03/05/2019
Leeds City Council	Standards Met	26/03/2019
Wakefield Council	Standards Not Fully Met (Plan Agreed)	28/03/2019
Leeds and York Partnership NHS Foundation Trust	Baseline	31/10/2018
	Baseline	14/03/2019
	Standards Met	28/03/2019
	Baseline	04/11/2019
Leeds Community Healthcare NHS Trust	Baseline	31/10/2018
	Standards Met	29/03/2019
	Standards Met	31/03/2019
	Baseline	31/10/2019
NHS Leeds CCG	Standards Met	27/03/2019
	Baseline	31/10/2019
Leeds Teaching Hospitals NHS Trust	Baseline	30/10/2018
	Standards Met	25/03/2019
	Standards Met	27/03/2019
	Baseline	28/10/2019

3.6.9 Leeds City Council's performance is consistent with other regionally local Council's and NHS organisations. Local Authorities known to be 'Standards Exceeding' are Barnsley MBC, Bolton MBC, Liverpool City Council, Derby City Council, Nottingham City Council, Norfolk County Council and Oxfordshire County Council.

3.6.10 A group of Leeds City Council employees visited Barnsley MBC colleagues in December 2019 to learn and share best practice and to compare in more detail information management and governance policies and processes. The IM&G Management Team have committed to further investigate a number of the practices and processes currently applied in Barnsley, to determine how these can be implemented in LCC in order to further improve our standards.

3.6.11 In order to continue this more detailed comparision of policies and processes, IM&G have committed to working with one of the core cities which are known to be 'Standards Exceeding', in the coming year.

3.6.12 The Council is currently on track to submit its DSP Toolkit in March 2020, expecting a 'Standards Met' outcome.

4 Corporate considerations

4.1 Consultation and engagement

4.1.1 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 Digital and Information Service Hubs and Information Management Board members.

4.2 Equality and diversity / cohesion and integration

4.2.1 There are no issues in relation to equality and diversity or cohesion and integration

4.3 Council policies and best council plan

4.3.1 All IM&G programmes of work are working towards ensuring the Council meet statutory and regulatory requirements.

4.3.2 All Information Management and 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.

4.4 Resources and value for money

4.4.1 There are no issues in relation to resources and value for money.

4.5 Legal implications, access to information, and call-in

4.5.1 Delegated authority for Information Management and Governance sits with the Director of Resources and Housing and Senior Information Risk Owner and has been sub-delegated to the Chief Digital and Information Officer under the heading “Knowledge and information management” in the Deputy Chief Executives Sub-Delegation Scheme.

4.5.2 Delegated authority for the Caldicott function sits with the Director of Adults and Health and has been sub-delegated to i) the Deputy Director, Social Work and Social Services, ii) the Director of Public Health and, iii) to the Director of Children’s Services with a further sub-delegation to the Chief Officer, Partnerships and Health. These delegations can be found in the Director of Adults and Health sub-delegation scheme under the heading ‘Local Authority Circular 2002(2) Implementing the Caldicott Standard into Social Care’.

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

4.6 Risk management

4.6.1 Non-compliance with PSN standards could leave the Council vulnerable to the following risks:

- The Head of the PSN could inform the Department of Works and Pensions of our non-compliance. Continued non-compliance could culminate in denial of access to Revenues and Benefits data.
- The Head of PSN could inform the ICO, which could culminate in the revisiting of the audit conducted by the ICO in 2013 to ensure compliance against the Data Protection Act / GDPR.
- The Head of PSN could 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

4.6.2 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.

4.6.3 Without a PSN certificate, there is significant risk to the council's National reputation as a Digital Innovator.

4.6.4 The risk associated with not implementing GDPR / DPA18 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.

4.6.5 Non-compliance with the Caldicott function could leave the Council vulnerable to the following risks:

- compromises to the security of confidential patient identifiable data.
- damage to the Council's reputation and the trust which individuals place in the Council to safeguard their data.
- infringements of data protection legislation / law on confidentiality and subsequent complaints / claims from individuals affected.
- non-compliance with the Data Security and Protection toolkit which would restrict the sharing of patient data with the NHS.
- enforcement action from the Information Commissioner's Office.

4.6.6 Further work is being undertaken in conjunction with the Corporate Risk Manager to embed the recording and reporting of information risk. 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.

5. Conclusions

5.1 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.

5.2 Considerable progress has been made this year to resolve security issues. The Council regained its PSN certificate in July 2019. Work is on-going to ensure continued compliance, working towards re-submission for 2020 certification.

5.3 An internal audit has found a need for improvement regarding raised priviledge active directory accounts. A project has immediately been established, with high level project plan documented to resolve this matter.

5.4 The volume of requests for information to the Council has increased significantly over the last two years and continues to rise. A plan has been developed, including the recruitment of additional resources for the Central Requests Team to address this issue.

5.5 The Council's Caldicott Guardian is an established role which is appropriately implemented through the Caldicott function of 3 senior leaders and robustly supported by the IM&G Service.

6. Recommendations

6.1 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 management and governance.

7. Background documents[1]

N/A

[1] The background documents listed in this section are available to download from the Council's website, unless they contain confidential or exempt information. The list of background documents does not include published works.