Leeds
CITY COUNCIL

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: 15th March 2021

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

1. 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.

- The Caldicott Guardian give assurance to Committee of the arrangements in place with regards to the confidentiality of patient and service-user data.

2. Best Council Plan Implications (click here for the latest version of the Best Council Plan)

- Specific KPI'S forming part of the measures of performance againt the Best Council plan are –

  Percentage of information requests received responded to within statutory timescales (Freedom of Information, Subject Access Requests and Environmental Information Regulations)

3. **Resources implications**
   The systems and processes in place and described within this assurance report have been established to manage the allocation of resources and to manage resource conflicts.

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 and suggest areas where they would like to see further focus.

1. Purpose of this report

1.1. To provide Corporate Governance and Audit Committee with an annual report on the arrangements in place within Leeds City Council with regards to information governance in order to provide assurance for the annual governance statement.

1.2 This year the Information Commissioner's Office (ICO) introduced the Accountability Framework. This is divided into 10 categories to aid demonstration of compliance with relevant legislation (including, but not limited to the Data Protection Act 2018, General Data Protection Regulations 2016, Freedom of Information Act 2000), government standards, codes of conduct and best practice for both the CCG and our member practices.

1.3 This report includes assurances aligned as required by the ICO's Accountability Framework and this Committee's terms of reference:

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.

2.2 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

2.3 The main body of this report focuses on the main issues of data access requests and PSN and highlights some of the key successes over the last 12 months namely the mandatory IG Level training and the work undertaken to support the Council and the wider health community through the pandemic. The appendix provides wider information to support the accountability and assurance framework.

3. Main issues

Appointments

3.1 From the 23rd December 2020, the Council's newly appointed Chief Digital and Information Officer has taken over the role as the Council's Deputy Senior

Information Risk Officer (SIRO). This is a jointly appointed role with NHS Leeds Clinical Commissioning Group (CCG).

Democratic Oversight

3.2 The Executive Member for Resources has oversight of executive decision making with regards to Information Governance.

Data Access Requests

3.3 For over 12 months the Information Management and Governance (IM&G) Team have not responded to FOI/EIR and SAR requests within the statutory time limits. This is due to the increase in number of requests since May 2018 (GDPR), some staff absences and latterly the pandemic which has compounded the issue and services across the Council not always being able to provide the Requests Team with the relevant information to respond to the requestors in a timely manner.

3.4 This issue is currently tracked by CLT with the figures presented in the quarterly Performance Report and will form part of the Annual Corporate Performance Report, to be presented to the September 2021 Executive Board.

3.5 Following a robust examination of all the existing process, conducting benchmarking with other local authorities including some core cities, undertaking customer satisfaction surveys and analysing performance statistics, it is felt that some fundamental changes need to take place in order to get the council back on track with its statutory performance measures. As a result 42 recommendations have been made for consideration / implementation, detailed in the ‘Review and Refine’ section of the Appendix to this report.

3.6 These recommendations for change primarily relate to:- amending the existing incoming process for statutory requests including robust triaging of all requests, ensuring all working processes are clearly documented and all IM&G staff are trained in their use, ceasing the provision of what can be classified as “administrative tasks” on behalf of services and introducing a culture of performance management which encourages accountability, ownership and effective reporting in relation to statutory requests across the organisation.

3.7 The IM&G service are currently in the process of a restructure, the consultation phase of which concluded on the 19th February 2021. The approved recommendations have informed and will be embedded as part of the new structure proposals. The newly developed KOLOMBO system will simplify and replace a number of existing manual and overly-complicated processes.

IMG Training

3.8 The mandatory Level 1 Information Governance training cycle for all who work for or on behalf of Leeds City Council has concluded for 2020/21, the results of which are split into two categories’; 1) Elected Members 2) All employees and others who have access to LCC data. This training is updated and launched every two years and a lessons learned report is produced at the end of every iteration (please see Appendix). On instruction of the SIRO, anyone (with the exception of Elected

Members) who does not complete this training within the given timeframe, has access removed from the LCC network, until such time as they complete the training.

3.9 The outcome of the 2020/21 training cycle is commendable.

Elected Members

- 66 Elected Members out of 99 have completed the training
- Regarding the remaining members to complete the eLearning, the recommended approach is to firstly engage them through a questionnaire/learning needs analysis document to obtain direct feedback. This will provide valuable feedback as to why they've not completed the requirements and various learning interventions provided for them to support completing the eLearning.
- Following obtaining feedback, this will be analysed to help identify the next appropriate action or solution.
- For newly elected members, it has been agreed in principle that IM&G staff will provide guidance and initial support to the group officers who are designing the new induction programme to help them incorporate the eLearning into the modules. This will set the expectation in the future for completing the eLearning.

All employees and others who have access to LCC data.

- Everyone instructed to complete this training did so, with the exception of one individual, who was removed from the Council network, as per the directive of the SIRO.

PSN Certification

3.10 The 2020 PSN submission was deferred with Cabinet Office due to COVID-19 pressures. This issue has been brought to the attention of this Committee on two previous occasions; 14th December 2020 and 8th February 2021. An action plan, documenting all the outstanding work to be completed and a firm submission date of July 2021, was submitted to the Cabinet Office on 31st December 2020. This action plan was signed off by the Chief Digital and Information Officer and shared with the Director for Resources and Housing and with the Chair of this Committee.

Covid-19 work

3.11 Since March 2020, the IM&G service has supported services across the Council's Directorates to ensure they are able to provide a timely response to the Covid-19 pandemic, delivering at pace to ensure that data compliance is adhered to without causing a barrier to the support required for the citizens of Leeds. To support this work, the IM&G service introduced a shortened version of its Data Protection Impact Assessment template to enable risks to be highlighted and mitigated in a timely way. The IM&G's Covid-19 work programme contains over 100 pieces of work which range from updating existing guidance / producing new guidance; advising on new ways of working; modifying existing services; and introducing new services and schemes as a result of the pandemic. Substantial IM&G resource has been invested in advising on the Council's work to support the clinically extremely vulnerable cohort and advising on test and trace matters such as the implementation of the test and trace support payment scheme and the implementation of a local contact tracing service.

3.12 All Covid-19 work is regularly reviewed to ensure that any corresponding risks are appropriately addressed.

3.13 The IM&G service has received considerable praise for the work it has undertaken in supporting the pandemic.

Caldicott Guardian

3.14 Between September – December 2020, an extensive benchmarking exercise was undertaken with a number of local authorities including two core cities; Birmingham City Council and Newcastle City Council. This benchmarking not only looked at statistical comparisons (used to inform the review of the Requests Team), but also looked at policies, procedures and the structures of the teams (used to inform the service restructure). The highlights of this benchmarking can be found in the Meaningfully Monitor section of the appendix.

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, Elected Members 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 the Best Council Plan

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

4.4 Climate Emergency

4.4.1The paper rationalisation and retention projects, detailed in the Effectively Embed section of this report, will enable the Council to reduce paper storage and consequently reduce the carobon footprint.

4.5. Resources, procurement and value for money

4.5.1 Effective management of the IM&G workforce and IT assets isundertaken and managed through a combination of performance reporting and governance arrangements as set out within this report.

4.6. Legal implications, access to information, and call-in

4.6.1 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 Director of Resources and Housing Sub-Delegation Scheme.

4.6.2 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'.

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

4.7. **Risk management**

4.7.1 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

4.7.2 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.

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

4.7.4 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.

4.7.5 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.

4.7.6 Further work is being undertaken in conjunction with the Intelligence and Policy 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.

4.7.7 There are two corporate risks and two directorate level risk associated with Information Governance;

- AH 12 - Information Management and Governance
- CH 11 – Information Management and Governance
- LCC 26 - Information Management and Governance
- LCC 31 - Major Cyber Incident

These are articulated in full in the Meaningfully Monitor section of the Appendix

4.7.8 The Head of Information Management and Governance is currently giving consideration to raising a separate PSN risk in light of the current deferment.

5. Conclusions

5.1 mnjThis report provides assurance on the management, governance and control mechanisms which support the delivery of Information Management, Cyber and Caldicott requirements within the Council.

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 and suggest areas where they would like to see further focus.

7. Background documents

7.1 None

Appendix – Internal Control of Information Management and Governance

Define and Document

Information Management and Governance Policies and Procedures

Policy	Protocol	Procedures	Interim Measures for Covid-19
Information Compliance Policy • Data Protection Policy Statement • Freedom of Information and Environmental Information Regulations Policy	Filming and Photography Protocol	• General Data Protection Regulation (GDPR) Toolkit • Toolkit for managers of leavers and movers	
Data Quality Policy			
Information Assurance Policy • Remote Working Policy • ICT Equipment Disposal Policy	• Acceptable Use Protocol • Password Protocol • Information Security Incident Protocol	• Encrypted memory sticks Toolkit • Sending Letters and Parcels Toolkit • ICT Equipment Disposal Procedure • Procedure for the Secure Storage of Filing Cabinet Keys (Children's and Adult Social Care only) • Procedure for Taking Personal Data and Special Category Data Off LCC Premises (Children's and Adult Social Care only)	• Information Security – Covid 19 Working from Home • Information Security – Covid 19 Staff Guidance for Handling Customer Enquires when Working from Home • Information Security – Covid 19 WhatsApp Guidance • Information Security – Covid 19 Printing Guidance
Information Sharing Policy		• Sharing information Toolkit • High Security File Transfer Procedure	

Policy	Protocol	Procedures	Interim Measures for Covid-19
		- Sharing Information for research Projects Procedure - Peer Checking for Post Procedure	
Records Management Policy - ICT Back-up Retention Policy	Office Move Protocol	- When and how to dispose of information Toolkit - Using the records management facility Toolkit - Track and Trace Procedure for Hard Copy Files - Creation, storage and disposal of information Toolkit	

Roles and Responsibilities

Decision making

Place from where function derived	Function Delegated	Officer to whom delegated	Terms and Conditions
Director of Resources and Housing			
HMG Security Policy Framework Version 1.1 – May 2018	Undertake role of Senior Information Risk Owner (SIRO)	Chief Digital and Information Officer	Where the SIRO is not available: have ultimate responsibility for the acceptance, or otherwise, of information risks for the council; responsible for approving, and ensuring implementation of, all policies and procedures relating to the Information Governance Framework
HMG Security Policy Framework Version 1.1 – May 2018	To approve Information Governance (IG) policy exemptions	Chief Digital and Information Officer	Level 3 exemptions where it is anticipated there will be a high business impact. In consultation with Information Management Board Level 1 and 2 exemptions where it is anticipated there will be a low or medium business impact. In consultation with key stakeholders
HMG Security Policy Framework Version 1.1 – May 2018	To investigate information security breaches	Chief Digital and Information Officer	In liaison with HR and other key stakeholders
HMG Security Policy Framework Version 1.1 – May 2018	Approve Information Sharing Agreements, Data Processing Agreements, Non-disclosure agreements when sharing information with third parties	Information Asset Owners	For the information assets for which they have been identified as the responsible officer.
		Directorate Information Compliance Officers in relation to matters within their remit	Where the relevant IAO is not available

Place from where function derived	Function Delegated	Officer to whom delegated	Terms and Conditions
Director of Adult Social Care and Public Health			
Local Authority Circular(2002)2 Implementing the Caldicott Standard into Social Care	To act as Caldicott Guardian for Adult Social Care	Deputy Director Social Work and Social Care Services	For matters relating to Adult Social Services
	To act as Caldicott Guardian for Public Health	Director of Public Health	For matters relating to Public Health and to sub-delegate as necessary
	To act as Caldicott Guardian for Children's Services	Director of Children's Services	For matters relating to Children's Services and to sub-delate as necessary
Data Protection Officer			
DPA (Data Protection Act) 2018 and UK GDPR (General Data Protection Regulation)	N/A	N/A	The Council's Head of Information Management is the Council's Data Protection Officer (DPO). The DPA 2018 and UK 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)).

Leadership and Oversight

Democratic Oversight	
Executive Member for Resources	Oversight of executive decision making with regards to IM&G
Corporate Governance and Audit Committee	Annual Information Governance Reporting, including the Annual Report of the Caldicott Guardian Ad hoc reporting on request of the Committee, for example: • PSN Compliance

	• International Transfers and Data Adequacy • Access Project
Management Oversight	
Information Management Board (IMB) (The IMB has 4 sub-groups articulated below)	Chaired by the Deputy SIRO. The purpose of this Board is: • Provide leadership, oversight and an approval mechanism of Information Management and Governance strategy and policy, ensuring regular reviews through the appropriate sub groups • Ensuring that an appropriate comprehensive Information Management and Governance framework and systems are in place throughout the Council which helps the Council deliver value from the use of information and monitors a cycle of data management improvements in a way that is compliant with the law and in line with national standards • The development and oversight of Information Management and Governance across the Council • Providing high level oversight and support to the Senior Information Risk Owner (SIRO) • Provide leadership, oversight and an approval mechanism of Information Management and Governance strategy and policy, ensuring regular reviews through the appropriate sub groups • Monitoring progress against strategy and policy and providing assurance on such to the SIRO and the Data Protection Officer (DPO) • Providing strategic leadership and direction on Information Management and Governance work prioritisation • Demonstrating how the above is enabling the Council to deliver most value from information, to effect better outcomes for citizens and business. • Establish an information management risk appetite for the Council.
Records Management Group	Chaired by the Corporate Records Manager. The purpose of the group is to: • Ensure that Leeds City Council Records Management policies, procedures and protocols are in place throughout the Council which helps the Council deliver value from the use of information in a way that is compliant with the relevant legislation and regulations and are in line with national standards and best practice; • Undertakes or commissions periodic assessments and audits of all Records Management policies, procedures, supporting documents and arrangements, and recording the rationale for any changes to any of the documentation; • Ensures policies, guidance, standards and supporting documentation are presented and published in a way that informs all staff about their responsibilities of managing information and technologies available to them. • Develop a framework of protocols, procedures, guidance and tools to enable all staff to recognise the importance of good records management, ensure records are effectively managed throughout their lifecycle from creation to disposal and to understand their roles and responsibilities with respect to compliance with the council’s records management policy; These will cover the following areas: - naming conventions - governance - roles and responsibilities - training and awareness - how and where to store records - records retention

	- records disposal. • To develop measures to be put in place to mitigate risks to information.
IM&G Policy Review Group	Chaired by the Head of Information Management and Governance. The purpose of this Group is: • Ensuring that an appropriate comprehensive Information Management and Governance framework is in place throughout the Council which helps the Council deliver value from the use of information in a way that is compliant with the law and in line with national standards • Support the Information Management and Governance strategy and policy and ensuring regular reviews
Data Practitioners Group	Chaired by the Head of Service, Legal Services. The purpose of this Group is: • looking at and responding to consultations; • reviewing new ICO guidance / codes of practice; • reviewing recent case law • reviewing ICO decisions
Information Security Assurance and Compliance (ISAaC) Board	Chaired by the Head of Information Management and Governance. The purpose of this Board is: • To make recommendations regarding operational oversight and direction for Leeds City Council (LCC) in all matters of Information Security and Assurance. • To act as an escalation point for serious, non-emergency, security matters where improvements have been identified. • To monitor the degree to which LCC complies with its own security policies, current national standards for compliance and best practice using statistics and descriptive narrative generated by Operational Services' Service Centre (to guide current and future development work). • To agree key messages related to Information Security that need to be disseminated and/or escalation through the organisation, or any part thereof. • To manage the implementation of the information security priorities, aligned to the council's vision and city's strategic outcomes. • To manage and assign activities to the Cyber Team to ensure compliance to industry standards listed in the Objective section. • To review and determine policy and process related to Information Security and Assurance.
Compliance Board	Chaired by the Head of Information Management and Governance. The purpose of this Board is: • Review identified high priority Security and Compliance Projects – dashboard and key milestone plans • Ensure success criteria for projects are sufficiently defined for compliance projects • Deep dive projects going off track • Remove blockers / constraints preventing project progress • Escalate issues such as resource limitations to the Programme Delivery Board and provide recommendations • Retain visibility of the compliance risk register and latest IT Health Check – act when necessary • Mitigate risks impacting progression towards sufficient compliance levels across the estate • Ensure Security and Compliance projects are prioritised effectively • Agree compliance related risk tolerance levels for projects and LC estate

Clearly Communicate

Format	Outline
Leadership	The SIRO is corporately responsible for Information Risk. The SIRO communicates to all employees on high risk matters and on compliance matters such as training. The DPO is corporately responsible for informing and advising 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)). The DPO meets with the SIRO on a monthly basis. The DPO communicates to all staff via the Managing Information Toolkit on InSIte At a more local level in Information Management and Governance, communication takes place in weekly Information Management and Governance Management Team Meetings and information is cascaded to all members of staff, as appropriate
Training	There is an Information Governance Training Strategy. The was last reviewed and approved by IMB in February 2020. The strategy documents the training requirements of all those who work for or on behalf of LCC including those on temporary contracts, secondments, volunteers, Elected Members, students and any staff working on an individual contractor basis and/or who are employees for an organisation contracted to provide services to LCC. The strategy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions. There are four levels of training which are described below: **Level 1.** All LCC staff are mandated to undertake this basic training in Information Governance. Training is available through two channels; • an e-learning package for PC users, • a brochure or leaflet for other staff. The Level 1 training is generic and covers IG related legislation, local policies and information security generally. **Level 2.** This is targeted at staff who have access to special category information as part of their everyday duties. It consists of a number of packages each tailored to the issues specific to a policy/service area. These packages; • build on the Level 1 training, • are classroom based, 'face to face' and interactive (these have been conducted remotely during the pandemic). They provide staff with a high level of understanding about appropriate data handling and their own responsibilities when handling council information.

Format	Outline
	Level 3. Bespoke training packages are developed and delivered to implement specific information governance programmes of work such as; • the responsibilities of Information Asset Owners • Cyber – Exercise in a Box & Hacking and Cracking training • Records Management • Data Protection Such packages may be supplemented by briefings, discussion groups and newsletters. Subject Matter Experts may be bought in, or staff may attend external training courses or events. **Level 4.** The following positions within the Council have the 'expert' level training necessary to provide the roles. This training is commissioned for the individuals as and when required and is usually provided by an external training provider: • SIRO - To assist staff whose roles involve responsibility for the confidentiality, security and availability of information assets, in understanding and fulfilling their duties. • Caldicott Guardian - To fully understand the role and function of the Caldicott Guardian. • Data Protection Officer - In depth understanding of the General Data Protection Regulation and Data Protection Act (and associated legislation) and information security • Cyber Assurance and Compliance Manager - In depth understanding of the General Data Protection Regulation and Data Protection Act (and associated legislation) and information security All staff have on-going refresher training, the level and frequency of which will be decided on an individual/service area/need basis. Level 1 refresher training is undertaken at least every two years.
Guidance	The Managing Information Toolkit on InSite provides access to guidance, procedures and instruction for all employees covering the following areas: • Creation, storage and disposal of information • GDPR • Information about staff • Information incidents • Looking after information • What to do if you receive a request for information • Sharing information • Using the Records Management Facility • When and how to dispose of information

Effectively Embed

Statutory and non-statutory information requests

Data protection law gives individuals greater control over their personal data through several rights. Individuals are informed of their rights through the Leeds City Council Privacy notice, available on the internet. All staff are made aware of these rights through the data security awareness training and the policies and procedures.

Since 2018, a central requests team has been in place within the Information Management and Governance (IM&G) service to respond to all statutory requests for the Council. The team respond to all information requests, which include those made under the Freedom of Information Act 2000 (the FOIA) and the Environmental Information Regulations 2004 (the EIRs), the UK General Data Protection Regulation (the UK GDPR) and the Data Protection Act 2018 (the DPA), as well as requests from the police, the courts, partner agencies and other government bodies and regulators.

Individual Rights Requests	The Council has received 477 Individual Rights Requests (IRRs) in the first 3 quarters of the financial year 2020/21 and the majority of these, approximately 98%, are subject access requests (SARs). The Council had seen a 20% increase in the number of IRRs received in the 2019/20 financial year. It should be noted that the number of requests received decreased at the start of the Covid-19 pandemic for the 2020/21 financial year but has since risen steadily peaking in November 2020 with 104 IRRs received in just one month. In the current financial year to date, the Council has on average 55-60 open IRRs which compares with this time last year. However, in quarter 3 this has increased to 79 requests open at any time. 35% of IRRs are for access to children's social care records by the individual who was in care or from the parents whose family have social care involvement. Due to the sensitive nature of these records the requests are highly complex and frequently run into thousands of pages. Every page has to be read and decisions made in respect of applying any necessary redactions as provided for in the UK GDPR/DPA, with some extremely difficult information to be reviewed in respect of child protection matters.
Freedom of Information/ Environmental Information Regulations requests	The Council has received 1459 Freedom of Information (FOI) and Environmental Information Regulations (EIR) requests in the first 3 quarters of the 2020/21 financial year. FOI/ EIR legislation did not change when GDPR became enforceable, however the number of requests received had increased in the last financial year (2019/20) by 8%. Again since the pandemic, the number of requests did initially decrease but the numbers have been slowly increasing. At any one time the council has on average of 160-170 FOI and EIR requests open compared to an average of 190 this time last year. In 2020/21 the amount of requests open at one time peaked at 230 requests received in October 2020. The pandemic has impacted not only the number of requests received but also the Council's ability to respond to them. Many

	services could not provide a response within the statutory timescales and some services could not respond at all at the start of the pandemic. In November of last year, it was agreed at the Information Management Board and with subsequent approval by the Council's SIRO (Senior Information Risk Owner), that the Council's KPI for responding to FOI / EIR requests within the statutory timescale be reduced from 96% to 90%.
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. A total of 1062 requests have been received in the first 3 quarters of this financial year. The number of requests have been consistent over the last 3 years with 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, and the team is currently receiving support from staff displaced by the Covid-19 pandemic. Additionally, the team at Westland Road are supporting viewings which reduces the need to move paper archived records around the city, saving on transport costs and also reducing the IG risks of moving sensitive records.
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 which is dealt with as a stage 2 complaint under the council's complaints policy. The Council has on average between 10 and 15 appeals open at any one time. To date this financial year the council has received approximately 65 internal review requests for IRRs / FOIs / EIRs with the highest open at any one time being 17. This figure of 65 also includes other data protection complaints, aside from those which relate to a request, which follow the Council's normal two stage process. The time taken to respond to internal reviews / complaints is significant due to their complex nature. As such, these complaints are currently being allocated to staff across the service in addition to the PO4 currently supervising the requests team. Requesters are also able to complain to the Information Commissioner's Office if they have concerns about the way the Council has responded to their request or complaint. In this financial year to date, 12 requesters/complainants have submitted complaints against the Council to the ICO. As with appeals, a substantial amount of capacity is required to respond to ICO complaints as these tend by their very nature to be complex and often span a considerable timeframe of involvement with the Council.

The table below sets out the number of statutory requests received and handled by the Council for both the DPA 1998 (and GDPR and DPA 2018 post May 2018) and FOIA / EIRs during 2017-18, 2018-19, 2019-20 and figures to date for 2020-21/21.

	2017/18		**2018/19 (Note: from May 2018, these figures include the new rights under GDPR)**		**2019/20**		**2020/21***	
	No of requests	**% compliance to statutory timescale**	**No of requests**	**% compliance to statutory timescale**	**No of requests**	**% compliance to statutory timescale**	**No of requests up to quarter 3**	**% compliance to statutory timescale**
DPA / GDPR –subject access requests & new rights requests post May 2018	590	97	855	90	949	83	477	66
FOIA & EIRs requests	2009	97.9	2455	93.5	2535	91	1459	86

*Please note that the reporting calculations are different this financial year due to the new case management system. The figures for 2020/21 do not include any requests which were on hold or cancelled and, therefore, this figure is lower.

Records of processing activities

It is a legal requirement that the processing activities of the Council are documented. The Council does this through its Information Asset Register.

Within the register the following requirements are included:

- lawful basis for processing
- the purpose of the processing
- categories of personal data
- retention details
- Data controller or data processor
- Information asset owner

As at December 2020 over 1,500 assets have been identified council-wide. 30 Information Asset Owners have received reports/presentations regarding the status of all of their assets.

In the summer of 2020 Internal Audit conducted an audit on the Information Asset Register. The auditor report was positive and provided the following outcome ratings:

Control Environment	Acceptable - There are some control weaknesses that present a medium risk to the control environment.
Organisational Impact	Moderate - The weaknesses identified during the review have left the council open to medium risk. If the risk materialises it would have a moderate impact upon the organisation as a whole.

Objective Assessed	**Control Environment**
The Council is aware of all information held by the Council that identifies whether it includes personal or special category data.	Acceptable
The Information Asset Register includes all relevant details and has been developed in line with appropriate best practice.	Acceptable
Appropriate reporting arrangements are in place for the progress being made in developing the Information Asset Register.	Good

The following recommendation were made to close the gaps and control weaknesses:

Recommendation 1

Information Asset Owners should instruct their staff to check whether they have saved any files to their G:\Everyone folder and if so instruct them to either delete it if no longer required or move it to a more appropriate location. The Information Asset Owners should then undertake a risk based review their directorates G:\Everyone folder to identify whether any of their information assets containing personal or special category data are saved there. Any identified should be immediately moved to a more appropriate secure location or deleted if outside of retention requirements. Record Managers should then undertake checks to ensure all unstructured information assets potentially containing personal or special category data have been removed from each directorate G:\Everyone folder and report any issues to the relevant director. Going forwards procedures should be updated and communicated to all staff on the appropriate use of unsecured folders and how such procedures will be managed. This should include any potential action that could be undertaken to address this issue, e.g. disciplinary action and removal of the files to a secure location. Implementation of these recommendation should help ensure staff save information in the correct location with suitable access controls in place for the data involved. This would also reduce the risk of a data breach.

A subsequent action plan which aims to ensure the implementation of the auditor recommendations has been developed and was agreed by the Information Management Board in November 2020.

Recommendation 2 All fields within the IAR must be completed for all information assets to ensure a comprehensive asset register is maintained, even if this is just to record a field is not applicable. The implementation of this recommendation should ensure the IAR meets the requirements of the business and allows information assets to be appropriately managed and safeguarded**.**

Recommendation 3 It must be ensured progress on this project continues to be regularly reported to senior management within the authority. The implementation of this recommendation should ensure the project is completed in a timely manner with appropriate support and governance oversight.

Recommendation 4 Consideration should be given to the level of formal assurance required by the SIRO on the implementation of the recommendations made in the reports to the various Information Asset Owners. A process should then be put in place to ensure the required level of assurance can be provided. The implementation of this recommendation should ensure the SIRO is provided with the required level of assurance that recommendations made have been actioned.

A subsequent action plan which aims to ensure the implementation of the auditor recommendations has been developed and was agreed by the Information Management Board in November 2020.

Records Management

Changing the Workplace (CtW) programme/Asset Rationalisation

A series of further office decants announced by Asset Management have been supported by Records Managers including Shire View, Navigation House and Osmandthorpe. Asset management are now working in collaboration with the Records Managers to ensure they are aware of all forthcoming office moves and decants in line with the asset rationalisation programme with an adequate notice period starting with St George House which is to be vacated by 1st April 2021;

Clear protocols have also now been developed and approved to provide a standardised approach amongst Records Managers and also to support services prepare records in readiness for any office closures.

Development of the Council's Retention Schedule

This work is now completed and the retention schedule is available on insite to all staff. IM&G are currently expanding on this work and mapping the retention schedule against the Local Government Classification Scheme (LGCS) to ensure standardisation with other government bodies and councils. The Records Managers will then be seeking to use these classifications as part of the O365 Share point on-line roll out to ensure council documents are appropriately categorised and retention rules are applied when saving documents.

Whilst the project to the get the Council's retention schedule up to date and in an accessible format for all Council employees is now closed, the retention schedule is undergoing continuous review to ensure that any changes to legislation or business requirements are represented accurately.

Cyber Assurance

In August 2020, the Digital and Information Service (DIS) formed a Cyber Team as part of a pilot, with the remit of working to resolve vulnerabilities on the estate that are understood to be ‘Business as Usual’ work; work outside funded projects for example, desktop and server patching.

The Cyber Team has made significant progress, embracing a new way of working for Operational Services. A number of systemic issues have been unravelled, addressing at source, an issue that was preventing 1500 laptops from patching. The focus this team provides is enabling speedier resolution of configuration errors. Vulnerabilities are addressed in a prioritised approach in order to reach compliance across the majority of the estate prior to PSN submission, as per Cabinet Office instruction.

This Cyber Team consists of technical and coordination resources that work specifically on the resolution and mitigation of vulnerabilities that are discovered by both the annual IT Health Check and the vulnerability management system.

The Cyber Team meets twice a week. Setting and monitoring of tasks is governed by the Information Security, Assurance and Compliance Board (ISAaC). The Cyber Team works on an 8 weekly cycle. Each tranche of work is approved by DIS SLT along with the resources required.

All projects with compliance or cyber dependency are governed via the Compliance Board and given appropriate priority within the DIS portfolio priority matrix.

Information Management Board is the escalation route for both ISAaC and the Compliance Board.

Meaningfully Monitor

Reviews of the requests team function

The requests team has undergone 2 specific reviews over the last year. One of these was undertaken by an external consultancy company and resulted in a new case management system, Kolombo, for handling all types of information requests. This case management system has been custom built internally and is designed to bring about digital efficiencies at all stages of the requests process. Kolombo went live in October of last year and phase 2 of the project is currently underway.

The second review, which has only recently taken place, is a comprehensive in-house review of how requests are handled and has examined: 1) the scope of the central requests team; 2) scrutiny of all types of request undertaken by the team and their associated processes; 3) scrutiny of roles and responsibilities of staff at all levels; 4) analysis of performance, costs of delivery and best practice; and 5) customer satisfaction.

Benchmarking

As part of the examination work a number of city councils, including 2 core cities were contacted to determine their approach to conducting information requests. The following Councils responded:

Organisation	Response Type
Birmingham City Council	Telephone interview
Bradford City Council	Email
Newcastle City Council	Telephone interview
Nottingham City Council	Email
Sheffield City Council	Email
Wakefield City Council	Telephone Interview
York City Council	Email

A number of questions were put towards the organisations of which the results are summarised below:

FOI and DPA Stats

All the organisations IG services centrally record information requests for their respective councils. Below is a breakdown of statistics received by each Council for 2019/20.

Organisation	FOI & EIR Received	% in time	*DP Received	% in time	FOI/EIR Internal Reviews	SAR Internal Reviews	FOI/EIR ICO Review	SAR ICO Review
York City Council	1909	82%	204	78%	Not Provided	Not Provided	Not Provided	Not Provided
Sheffield City Council	1941	93%	Not Provided	Not Provided	45	5	7	6
Bradford City Council	1767	88%	386	79%	53	16	Not Provided	Not Provided
Birmingham City Council	2666	79%	406	72%	40	Not Provided	Not Provided	Not Provided
Wakefield City Council	1393	82%	224	95%	9	4	Not Provided	Not Provided
Nottingham City Council	1416	94%	142	68%	29	8	Not Provided	Not Provided
Newcastle City Council	1600	88%	80	90%	15	Not Provided	Not Provided	Not Provided
Leeds City Council	2535	91.4%	1322 (non SAR) 949 (SAR only)	83.4%	63	40	Not reported on	Not reported on

*It should be noted that there is no standard approach on how each authority categorises what is a DP request or a SAR, therefore for the purpose of this exercise these have all been grouped as DP requests. Similarly some corporate IG teams do not deal with all SAR's on behalf of the authority, therefore SAR's dealt with by individual services in other authorities will not be captured in the figures above.

Internal Process

- Five of the seven councils pass information requests to their service areas to manage once logged by the IG service, this includes obtaining senior officer sign off and responding to the requestor (York, Sheffield, Bradford, Birmingham, and Newcastle).
- York council passes requests to the service but signs off the final response, this council is trialling information requests being fully managed by the service areas.
- Of the five councils, three (Birmingham, Sheffield, Newcastle) have teams which sit outside IG, and sit within Children's services where social care workers undertake Children's service SARs

- Two councils (Wakefield and Nottingham) manage the end to end process from acknowledging, to managing the information from the service to sending out the response, Nottingham actually gains IAO approval before the response is sent out. All Councils deal with high profile requests (e.g. those with press interest, member request etc.) via their main information processes described above.

Exemptions

- Four of the Councils IG services advise the service if they wish to apply exemptions and/or undertake a public interest test, with one of the councils providing final sign off on any exemptions (York, Sheffield, Bradford, and Newcastle).
- One of the councils utilise their legal team to advise their services on exemptions (Birmingham).
- Two of the Councils utilise their IG service to undertake the exemption work. (Wakefield and Nottingham).

Logging system

- There is no consistent logging system any of the IG teams use, with the majority of councils using a casework management based system.

Reviews

- All IG teams support the management of the review process.
- Four IG teams undertake reviews end to end (York, Sheffield, Wakefield, Nottingham).
- Three IG teams support the review process, which is led by the service, including the arrangement and support of an independent panel and organisation of service leads (Bradford, Birmingham, and Newcastle).

Team Structures

- IG teams vary from 3 to 9, with the majority of teams consisting of approximately 6 staff.
- With all teams, requests form part of the wider IG service (with the exception of those local authorities where children's services look at SAR's only).

Data Security and Protection Toolkit

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

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 organisation 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.

Comparisons of other Local Authorities and local NHS organisations are given below (please note Local Authorities normally only submit once a year (March), whereas some NHS organisations are expected to normal submit twice a year (October and March) Due to the Covid pandemic NHS Digital extended the submission deadline to September 2020).

This year comparisons have been made with additional Local Authorities as part of the benchmarking exercise articulated above

Organisation	Status	Date Published
City of Bradford MDC	Standards Met	03/04/2019
Calderdale MDC	Standards Met	20/02/2020
Kirklees Council	Standards Met	16/03/2020
Leeds City Council	Standards Met	30/03/2020
Wakefield Council	Standards Exceeded	24/09/2020
York City Council	Standards Met	28/09/2020
Sheffield City Council	Standards Not Fully Met (Plan Agreed)	30/09/2020
Birmingham City Council	Standards Met	28/09/2020
Nottingham City Council	Standards Exceeded	28/09/2020
Newcastle City Council	Standards Met	23/03/2020
Leeds and York Partnership NHS Foundation Trust	Standards Met	25/09/2020
Leeds Community Healthcare NHS Trust	Standards Met	21/08/2020
NHS Leeds CCG	Standards Met	01/09/2020
Leeds Teaching Hospitals NHS Trust	Standards Met	21/09/2020

Cyber Assurance

IT Health Check

The IT Health Check is a requirement of PSN compliance. It serves as an external audit of a point in time representation of the security posture the Council’s technical estate. From this assessment conclusions can be drawn based on the objective evidence presented around potential gaps in security controls. The majority of vulnerabilities are given a score based on an international standard (CVSS); all critical and high vulnerabilities (CVSS 7-10) must be resolved or mitigated against prior to successful PSN submission.

The last IT Health Check took place in January 2021. The full report cannot be shared publically as it documents any vulnerabilities on the estate. The high level data is given below, this will be extrapolated across the estate and progress tracked using the vulnerability management system.

Section	Critical	High	Medium	Low	Total
Internal	3	5	4	1	13
10% Scan	20	41	37	10	108
Host build	5	5	9	0	19
Wireless	0	0	1	1	2
Mobile	0	0	0	14	14
External	0	0	4	3	7
Firewall	0	1	3	1	5

Activities are tracked and monitored via the governance articulated in the Effectively Embed section of this report.

The risk score as at 8th February 2021 (following the IT Health Check) was 282,440,498. This is a reduction of over 400m, since the Cyber Team assembled in August 2020.

Corporate and Directorate Level Risks

Probability	Impact	Risk Score	Controls
LCC 31 - Major Cyber Incident: Risk to Citizens, Council and City as a result of digital crime, process failure or peoples actions			
4 - Probable	4 - Major	Very High	There are a wide range of controls that can affect the efficacy of Cyber resilience. Those include People, Process and technological controls. A summary of the key controls can be found below. - Configuration of devices - Training of staff. - Governance meetings with IM&T leads - Strong technical employees - Vast potential in software portfolio for improvement with resource investment alone - Strong planning culture - Existing Process and policy The Information assurance compliance standards have detailed and numerous controls, to which LCC are required to meet. Those include: PCI-DSS PSN CoCo Cyber Essentials Plus Data Security and Protection Toolkit for Health HMG SPF and related documentation. Partner / Contractor: - Contract clauses - Memorandums of understanding - Data sharing agreements - Cyber Team, focussing on vulnerabilities.
LCC 26 - Information Management and Governance: Risk of harm to individuals, partners, organisations, third parties and the council as a result of non-compliance with Information Governance legislation and industry standards.			
3 - Possible	3 - Moderate	High	The City Council's controls aimed at mitigating the Information Management Risk are evidenced in: (a) the Information Governance Framework; (b) the policies made under it (for example, the Information Security Policy); (c) other rules and Codes of Conduct; (d) Information Technology systems which contain or provide access to Council information; (e) physical asset protection measures; (f) other, system or risk specific, controls. (g) staff training on induction and every 2 years.
AH 12 - Information Management and Governance:			

Probability	Impact	Risk Score	Controls
Risk of harm to individuals, partners, organisations, third parties and the council as a result of non-compliance with IG legislation and industry standards.			
3 - Possible	3 - Moderate	High	Mandatory IG training for all LCC staff - IG toolkit (CareCert) - IM&G Service - appropriately trained and skilled - IG Policies and procedures - Peer checking - Compliance with the Legal framework - Steering Group - Caldicott guardian - Audit reviews (Internal and External e.g. CQC file review) - Information Asset Owners and Information Asset register - Inbuilt system controls e.g. access and security - Contractual obligations, terms and conditions around IG with 3rd parties - Physical security/buildings and assets etc. - Shielding policy - Investment in IM&G - HR checks and procedures - Employee obligations e.g. contractual, Code of Conduct
CH 11 – Information Management and Governance: Risk of harm to individuals, partners, organisations, third parties and to the council as a result of non-compliance with IG legislation and industry standards.			
3 – Possible	3 – Moderate	High	- Mandatory IG training for all staff - IG toolkit (Carecert) - IM&G Team - appropriately trained and skilled - IG policies and procedures - rolled out, embedded and easily accessed within C&F directorate - Peer checking - Legal framework - Steering group - Coldicott guardian - Audit reviews (internal and external) - Information asset owners - Information asset register - Inbuilt system controls e.g. access and security - Contractual obligations, terms and conditions around IG with 3rd parties - Physical security controls in place to prevent unauthorised access to information and to help ensure it's securely held e.g. staff ID badge challenge, locked doors, swipe card access, records locked away securely etc - Shielding policy - On-going investment in IM&G Level 2 IG training for Children's staff – this is mandatory for access to the Leeds Care Record - Data Security and Protection toolkit - CareCert

Review and Refine

Level 1 Information Governance Training

The mandatory Level 1 Information Governance e-learning is updated and launched every two years and a lessons learned report is produced at the end of every iteration. This is a summary of the lessons learned from the latest iteration.

Main Issues	
Data quality	Although managers were asked for information about staff on long-term sick, maternity leave etc., the Information Management and Governance (IM&G) team were still receiving information up to the deadline. This information should be recorded appropriately in SAP, but there are clearly gaps and the IM&G team have to gather this information from managers in advance.
	Recommendation: Managers to keep BSC up to date with information about staff. Communication to come from BSC
Training content	A very small number of staff had issues with some content in the training. All of these were dealt with at the time and staff were assured that their concerns would be recorded for the lessons learned exercise .Aside from some minor technical ‘glitches’ a common issue was that staff thought that they had completed the training when they hadn’t. This was to do with not clicking on links in a particular module because the links were not obvious so the system did not recognise the training as complete. This is easily remedied and will be for the next iteration of the training.
	Action: All concerns will be investigated/considered when planning for the next iteration of the training.
Access to PAL	There were some issues with staff struggling to access PAL; this was usually because of a lack of familiarity with using PAL and involved not remembering passwords etc. These were all dealt with on a 1-2-1 basis at the time.
Outside agencies	Queries for example, from the Grand Theatre about staff who have access to some LCC data- does the nature of the data mean that they need to undertake the training? DWP were doing an audit of one of our systems- did they need to do the training?
	Action: For the next iteration of the training develop a criteria used for outside agencies who are expected to undertake the training.
The use of other devices in the future	There will come a point when we expect all staff to undertake the training electronically. If all staff are issued with LCC devices then this should not pose a problem; however in the event of staff using their own devices there will be IG implications.
	Action: Ensure appropriate controls are in place, including a Data Protection Impact Assessment
Conclusion	
By the final deadline everyone instructed to complete the training had completed apart from one individual. Communications between the members of staff involved were excellent, with regular meetings to make sure that everyone was up to speed and able to make suggestions/observations. There now seems to be a culture within the council that this training is regular, mandatory and necessary. Apart from the issues raised above (all of which can be dealt with) the required outcome was achieved.	

Records of processing activities

Following the internal audit of the Information Asset Register an action plan which aims to ensure the implementation of the auditor recommendations has been developed and was agreed by the Information Management Board in November 2020. This action plan is tracked by the Information Management Board on a Bi-monthly basis.

Recommendation	Action	Timescales
Information Asset Owners should instruct their staff to check whether they have saved any files to their G:\Everyone folder and if so instruct them to either delete it if no longer required or move it to a more appropriate location. The Information Asset Owners should then undertake a risk based review their directorates G:\Everyone folder to identify whether any of their information assets containing personal or special category data are saved there. Any identified should be immediately moved to a more appropriate secure location or deleted if outside of retention requirements.	Ensure that all reports to be presented to the Information Asset Owners contain a standard section informing them to instruct staff to move files in the G:\everyone accordingly. Need to update the IAO handbook to include a short section around the role of the asset owner to include conducting a review of their G:\everyone folders to identify whether any of their assets containing personal or special category data are saved there. Update the guidance around the drives on the “What to store where” to include this message. The work ongoing in relation to the O365 project needs to take account of this recommendation. “Move it or lose it messages” need to form part of the comms plan for the project. File structures to be developed in line with the appropriate classification schemes.	March 2021 December 2020 December 2020 March 2021
Record Managers should then undertake checks to ensure all unstructured information assets potentially containing personal or special category data have been removed from each directorate G:\Everyone folder and report any issues to the relevant director.	This will be undertaken as part of the O365 migration review plan where all unstructured content will be addressed. Ensure that the compliance centre in M265 is developed to identify and prevent unstructured data going forward. As highlighted above the “Move it or lose it” messages need to form part of the comms plan	March 2021 and ongoing
Going forwards procedures should be updated and communicated to all staff on the appropriate use of unsecured folders and how such procedures will be managed. This should include any potential action that could be undertaken to address this issue, e.g. disciplinary action and removal of the files to a secure location.	Already included in above guidance Acceptable use policy Expand on the comms to go out corporately. O365 migration plan will include details on the removal of files – we need to see the capabilities of O365	March 2021

Recommendation	Action	Timescales
All fields within the IAR must be completed for all information assets to ensure a comprehensive asset register is maintained, even if this is just to record a field is not applicable.	Identify the extent of the gaps in the asset register. Review the number of blanks quarterly. Records Managers to ensure that prior to any final meetings with asset owners there are no blank fields within the asset register.	Dec 2020 Ongoing Ongoing whilst meeting are ongoing with asset owners.
It must be ensured progress on this project continues to be regularly reported to senior management within the authority. *The implementation of this recommendation should ensure the project is completed in a timely manner with appropriate support and governance oversight.*	Ongoing reporting requirements to senior management will form part of phase 3 of the project. Update reports to be presented to the Head of IMG and the Information Management Board on the progress with the Information Asset Register	Ongoing Ongoing
Consideration should be given to the level of formal assurance required by the SIRO on the implementation of the recommendations made in the reports to the various Information Asset Owners. A process should then be put in place to ensure the required level of assurance can be provided.	Update reports are routinely presented to the Information Management Board on the progress with the Information Asset Register will subsequently form part of the monthly DPO update with the SIRO. Phase 3 of the project to be scoped out to ascertain the frequency, content and mechanism for ensuring the SIRO is kept informed of the information asset register risks identified. Ensure discussions take place with the SIRO to determine whether the proposed reporting mechanism provides the relevant assurance.	December 2020 January 2021 February 2021

Review of the Requests Team and benchmarking exercise

A full list of recommendations arising from this review and benchmarking exercise are given below:

Area of Work	Recommendation	Implementation 1= 1-3 months 2 = 4-6 months 3 = 6 months +
Governance	R1 – That officers at B1/B3 grades are more involved in the provision of responding to low level information requests (including FOI and SARs) as per their job descriptions. This will help ease pressures from Officers who may need to deal with more complex requests as well as provide development for lower graded officers. This will need to be balanced to ensure the support staff work is still completed as the request team are also currently dependent on support from non IMG staff. Similarly if staff are expected to deal with more complex request these need to be reflected in the relevant job descriptions.	1
	R2 – A review the job descriptions for staff needs to be performed to take into account any new structures arising from the service restructure and any new working practices and processes (including escalations) arising from this examination.	1
	R3 – That all working processes are documented and agreed and signed off by the IMG Management Team. Any changes to agreed working practices will need to be agreed and managed either by IM&G Management Team prior to be communicated across the wider team.	1 – Utilise existing process maps
Benchmarking	R4 - With the resources and the level of requests comparable to core cities, it is recommended the Information Management and Governance service continue to provide a co-ordinating role and seek to review which elements of the request and exemption process can be delivered by service areas.	1
	R5 - R5 - IMG service continue to undertake independent internal and ICO reviews in the short term, however we need to work towards services conducting FOI/EIR internal reviews with IG input going forward to improve transparency in the process.	3

Area of Work	Recommendation	Implementation 1= 1-3 months 2 = 4-6 months 3 = 6 months +
FOI/EIR/SAR	R6 - Discussions should be undertaken with Chief Officers/Heads of Services to ascertain who the most appropriate points of contact within their service are for specific requests (both FOI/EIR and SAR. Where possible, central points of contact should be agreed with services.	1/2
	R7 - The Service Contact spreadsheet should be regularly updated, and the updating of this spreadsheet should form part of the Requests Team's and the services formal processes to ensure contacts are accurate.	1
	R8 - Officers within the Request Team should avoid overreliance on the spreadsheet when allocating requests. It is acknowledged that many requests will often not have an obvious first point of contact. In these situations, officers should instant message or phone potential service contacts (or experienced members of staff within the Information Governance Service) to see if they are appropriate, rather than simply allocating to a name.	1
	R9 - Allocations should be formally checked within 24h by a more senior officer within the team (this could form part of the daily stand ups mentioned in the section below)	1
	R10 - SARs should ideally be allocated to services to gather the information required, this would be the same process as FOI/EIR. In the short term IMG will continue to deliver SARs as is, however we need to work towards SARs being allocated to services to gather the information required, this would be the same process as FOI/EIR and improve accountability in the process.	1
	R11 - Requests to be triaged by the request team in a daily stand up meeting, with a 'complexity' level of 1 to 3 applied (1 being the least complex, 3 being the most complex).	1
	R12 - Formal criteria to be drawn up as to the nature of the requests that will fall into each complexity level. As a guide, Complexity Level 1 should concern FOI requests for which the information is available in the public domain (e.g. on the data mill) and to basic questions, for SARs, simple requests for copies of council tax/benefits documents. Complexity Level 3 should concern requests of high sensitivity; FOI- including those from journalists and those which will involve direct liaison with Chief Officers/Directors, SAR - Social Care records - A pilot could be conducted in the first instance utilising a fail fast / change approach if the process is not working.	1
	R13 - Formal process to drawn up and re-instigated to ensure that services with complex requests are given timely reminders to ensure the Request Team have adequate time to process the responses.	1
	R14 - Requests to be allocated to specific officers at daily stand up meetings.	1
	R15 - Services to be provided with the specific name of the officer dealing with their request to ensure a 'start to finish' process.	1

Area of Work	Recommendation	Implementation 1= 1-3 months 2 = 4-6 months 3 = 6 months +
	R16 - Customers to be provided with a tailored acknowledgement advising of the request number, the time scales for the request, details of which officer is processing their request and their contact details.	1
	R17 - Officers to be provided with the opportunity to work on complex requests with the Request Team lead and experienced colleagues to learn how to handle complex requests. This would be best achieved as part of the triage process (with officers each being offered the opportunity to process complex requests with support).	2/3
	R18 - Officers to be encouraged to rely less on FOI/EIR template responses prior to understanding exceptions and to write their own arguments (with support). Officers to query services if they do not understand the information provided to them.	2/3
	R19 - Consideration to be given to re-instigate the creation of a 'CPD' item in team meetings during which officers can share best practice with each other on interesting requests.	2/3
	R20 - A formal process to be put in place to ensure that complex requests are reviewed by the Team leads prior to disclosure. This, again, could be dictated by the triage process (with the Request Team lead reviewing all Level 3 responses).	1
	R21 – Consider exploring a formal process change not requiring Heads of Service to review low complexity requests so as to ease their workload and also to enable quicker processing of responses.	3
	R22 - Press Office should always be provided with weekly list of FOI/EIRs received, and officer discretion to notify specific press officers of a complex request to form part of triage process.	1
	R23 - Formal timescales (we will endeavour statements) to be put in place for requests for clarification.	1
	*R24 - Requests Officers and Support Officers should be invited to the same team meetings/events, to ensure collaborative working. Further opportunities should be created for collaborative working (for example, where capacity allows, enabling support officers to work with Requests Officers on basic responses to enable them to understand the legislation and upskill themselves).	1 (initial set up of meetings)
	R25 - SAR: consideration should be given to transferring the responsibility of collating the information required to services as the Information Asset Owners. Welfare checks with customers and determining what can be/cannot be redacted from social care files should be made by a social worker professionals. When determining what can and can't be redacted from files the request team should consult with social care professionals in the first instance and only contact customers following this advice.	1/2

Area of Work	Recommendation	Implementation 1= 1-3 months 2 = 4-6 months 3 = 6 months +
CCTV	R26 - Roll out one process for CCTV enquiries and provide training to all staff to enable them to more confidently handle all CCTV enquiries /requests. In the interim as part of this review the Principal; Information Governance Officer and Senior Information Governance Officer has developed and implemented a process chart based on previous expertise to avoid an adhoc process continuing (Appendix D). In the short term utilise the interim process to manage the requests which come into the IM&G team as services have indicated is currently working well for them.	2
	R27 - To hold a workshop(s) with CCTV compliance/enquiries team and LBS to understand and capture the varying process and consider if there is a more streamlined approach – working group.	3
	R28 - Consider if any of the CCTV enquiries handled by IM&G would be more appropriately aligned to Leedswatch and/or LBS.	3
Schedule 2	R29 - That a centralised recording of requests and a standardised approach are maintained. However it should be noted that the work required - receiving, logging, collating and responding – does not all necessarily need to be undertaken by IMG or staff with advanced Data Protection knowledge however there will be requests where IM&G need to be involved to ensure the necessity and proportionality tests have been met.	2
	R30 - That IMG document a standard procedure for handling such requests but then work with the relevant service areas for them to take appropriate responsibilities: a) all CCTV requests could be centrally handled by LeedsWatch (as noted in R28) b) simple Council Tax checks, currently done by IMG, could be done by Council Tax. C) LASBT, Benefits, Licensing, Trading Standards, Business Rates are already handled by the service who could also take on responsibilities for logging and responding too. Note: Social Care requests will be less easy reallocate given the above noted records management situation and would need more discussions between the records management facility, IM&G RM staff and the appropriate asset owners.	2
	R31 - IMG should remain involved in the schedule 2 request process but in a more advisory capacity as required and also auditing to ensure processes are followed and reportable figures are accurate. There will be requests where IM&G need to be involved to ensure the necessity and proportionality tests have been met.	2
Miscellaneous	R32 – As per the approach taken by other authorities IM&G to provide more of an advisory role in the in relation to Serious Case reviews, relative Tracing, Home Office Checks, Fostering and Adoption Checks, DBS Checks and Continuing Health care checks - with responsibility for these requests being managed within the service.	3
	R33 - That the scope of the work undertaken by the request team is documented so it is clear which request types the request team remain responsible for and that there are documented processed developed for each process retained.	2
	R34 – That discussions regarding record retrievals, viewings, scanning currently being performance at Westland Road	2

Area of Work	Recommendation	Implementation 1= 1-3 months 2 = 4-6 months 3 = 6 months +
	continue with the intent this arrangement can continue.	
Performance	R35 - Implement an appropriate performance framework and routine performance reporting mechanism which ensures directorates, the SIRO, DIS CO and DPO are aware of their performance in relation to requests and also enables issues and exceptions to be appropriately escalated both within the directorate and to the SIRO. A central document which outlines all reports to be produced and all reporting deadline dates should be produced and communicated. R36 - Reporting should report on the response times for all types of requests managed by the team and should clearly articulate any reasons for late responses.	2
	R37 – Enhance existing reporting using Power BI which will enable links containing the relevant performance data to be sent directly, following review only from IM&G staff, to stakeholders, reducing officer time running and producing monthly/quarterly performance reports for stakeholders and weekly reports for members.	2
	R38 – As part of the ongoing development of Kolombo (Phase 2) implement an overarching report (dashboard) to be reported into IMB which will give a high level summary of request numbers and response times (KPIs);	2
	R39 – A data verification report with Power BI should be created to assist with data quality checks;	2
	R40 - Develop and implement a communication strategy which will inform Departments and services about which staff deal with requests and the need to respond to statutory requests and performance reporting to enhance a change of behaviour in the services.	2
	R41 - Before Phase 2 of the Kolombo work starts, a review of critical fields in the previous CCM system should be finalised and included in the Phase 2 requirements to allow for more meaningful dashboard reports to be produced. This may require input from other Access and Compliance Officers within IM&G.	2
	R42 – Kolombo developments – Recommendations within the report are aligned to ongoing Kolombo developments which should also be reported to the Head of IM&G	1

The final draft report with recommendations was presented to the IM&G Management Team for comment on the 12th February 2021. The Head of Information Management and Governance subsequently provided a copy of the report to the CDIO and discussed the high level recommendations with the wider DIS Senior Leadership Team on the 16th February. A decision was made by DIS SLT to start implementing a number of the recommendations put forward.

Given that the IM&G service is currently in the middle of a restructure it may not be viable to start work on putting some of the recommendations in place at this current time. Therefore the IM&G Management team met on the 1st March 2021 to discuss.

The IM&G Management Team have carefully considered each of the 42 recommendations and categorised the high level timescales for implementation as follows:

Category 1 – IM&G will put work towards putting these recommendations in place immediately as a matter of priority - (R3, R6, R7, R8, R9, R12, R13, R20, R22, R23, R24, R26, R41, R42)

Category 2 – IM&G will undertake some introductory work on these tasks for further development and finalisation once the IM&G Management structure is in place – May 2021 (R34, R35, R36, R38, R39, R40)

Category 3 – IM&G will implement these recommendations once the restructure is completed and the new teams are established (R1, R2, R11, R17, R18, R19, R27, R28)

Category 4 – These recommendations will be implemented following wider discussions at Corporate Leadership Team as these recommendations require ownership and buy in from wider council services (R4, R5, R10, R25, R29, R30, R31, R32, R33, R37)

Category 5 – Dependency recommendations– Further discussions to commence on how this will work once R11 is place (R14, R15, R16)

One recommendation was not approved as agreed by the Senior Information Risk Officer (R21).