Report author: Louise Whitworth & Shona McFarlane

Tel: 01133783978

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

Date: 4th February 2022

Report of: Director of Resources and the Director of Adults and Health

Report to: Corporate Governance and Audit Committee

Will the decision be open for call in?	☐ Yes ☒ No
Does the report contain confidential or exempt information?	☐ Yes ☒ No

What is this report about?

Including how it contributes to the city's and council's ambitions

- 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.
- Specific KPI'S forming part of the measures of performance against 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)

Recommendations

a) Corporate Governance and Audit Committee is requested to consider this report and the assurances provided within it and the attached appendix 1, accepting that the information governance arrangements are fit for purpose, up to date, are routinely complied with, have been effectively communicated and are monitored.

Why is the proposal being put forward?

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.

2. Last 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, UK General Data Protection Regulation, Freedom of Information Act 2000), government standards, codes of conduct and best practice.
3. This report includes assurances aligned as required by the ICO's Accountability Framework and this Committee's Terms of Reference.
4. Key Issues
   a) Improvements have been made, compared to last year, on responding to Freedom of Information (FOI) / Environmental Information Regulation (EIR) and Individuals Rights(IR) requests within the statutory time limits.
   b) The service has had a change of structure and working practices and has been renamed the Information Governance and Cyber service (IG&C).
   c) The mandatory Level 1 Information Governance eLearning development and roll out cycle is currently underway, with a provisional launch date to staff mid-September 2022.
   d) IG&C are leading on a project to review and update the current Data protection impact assessment template and process
   e) PSN certification was awarded in October 2021.
   f) In August 2021, the National Data Guardian issued guidance on the appointment of Caldicott Guardians, their role and responsibilities in respect of data processing activities undertaken within their organisations. Further details can be found in the Appendix.

What impact will this proposal have?

Wards affected:		
Have ward members been consulted?	☐ Yes	☒ No

5. The council processes a considerable amount of citizen data and has a duty to process this data in accordance with legislation, government standards and good practice. Effective corporate information governance arrangements should help prevent any risks arising or mitigate their impact on citizens should they occur.

What consultation and engagement has taken place?

6. 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 business partner colleagues, elected members and Information Management Board members.

What are the resource implications?

7. 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.

What are the legal implications?

8. Delegated authority for Information Management and Governance sits with the Director of Resources 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 Sub-Delegation Scheme.
9. 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'.
10. There are no restrictions on access to information contained in this report

What are the key risks and how are they being managed?

11. 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
12. 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.
13. Without a PSN certificate, there is significant risk to the council's National reputation as a Digital Innovator.
14. The risk associated with not implementing UK 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.

15. 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.
16. 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 is ongoing and 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.
17. There are two corporate risks associated with Information Governance;
    - LCC 26 - Information Management and Governance
    - LCC 31 - Major Cyber Incident

    A number of associated Directorate level risks are also managed. These are articulated in full in the Meaningfully Monitor section of the Appendix.
18. RES 33 is a new directorate risk created in 2021/22 in respect of the risk of the council's failure to meet legal statutory timeframes for responding to information rights requests.

Does this proposal support the council's three Key Pillars?

☒ Inclusive Growth ☒ Health and Wellbeing ☒ Climate Emergency

19. Appropriate collection, storage, use, security and sharing of information supports each of the council's three Key Pillars. Each pillar requires information and therefore poor information governance practice could impact on their achievement. The information governance arrangements aim to ensure that all council information is managed appropriate and lawfully.

Options, timescales and measuring success

What other options were considered?

20. N/A

How will success be measured?

21. N/A

What is the timetable for implementation?

22. N/A

Appendices

23. Appendix 1: Corporate Information Governance Arrangements

Background papers

24. None

1.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 • International Transfers – Practitioners Guide • Looking after information Toolkit • Information Requests Toolkit	
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 • 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) • IMG Training Strategy	• 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 • 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	

Policy	Protocol	Procedures	Interim Measures for Covid-19
		• Creation, storage, and disposal of information Toolkit	

2.Roles and Responsibilities

2.1 Decision making

Place from where function derived	Function Delegated	Officer to whom delegated	Terms and Conditions
Director of Resources			
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.
		Information Governance Officers in relation to matters within their remit	Where the relevant IAO is not available
Director of Adults and 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-delegate as necessary

Place from where function derived	Function Delegated	Officer to whom delegated	Terms and Conditions
Data Protection Officer			
DPA (Data Protection Act) 2018 and UK GDPR (UK General Data Protection Regulation)	N/A	N/A	The Council's Head of Information Governance and Cyber 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 UK GDPR when processing personal data; to monitor compliance with the UK 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)).

2.2 Leadership and Oversight

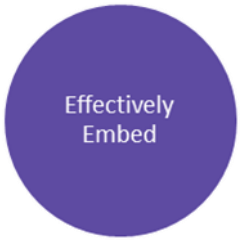
Democratic Oversight	
Executive Member for Resources	Oversight of executive decision making with regards to IM&G
Corporate Governance and Audit Committee	Annual Information Governance Reporting, including the Annual Report of the Caldicott Guardian Ad hoc reporting on request of the Committee, for example: • PSN Compliance • International Transfers and Data Adequacy • Access Project
Strategy and Resources Scrutiny	Ad hoc reporting on request of the Committee, for example: • Performance with regards to Freedom of Information Requests
Management Oversight	
Information Management Board (IMB) (The IMB has 3 sub-groups articulated below)	Chaired by the Deputy SIRO. The purpose of this Board is: • Providing leadership, oversight and an approval mechanism for Information Governance and Cyber strategy and policy, ensuring regular reviews through the appropriate subgroups • Ensuring that an appropriate comprehensive Information Governance and Cyber framework and systems are in place throughout the Council. • Monitoring a cycle of information and data management improvements in a way that is compliant with the law and in line with national standards • Providing assurance to the Council's Senior Information Risk Officer (SIRO) and Data Protection Officer (DPO) in relation to the Council's arrangements for creating, collecting, storing, safeguarding, disseminating, sharing, using and disposing of information in accordance with its: ○ stated objectives / purposes.

	○ legislative responsibilities ○ risk appetite • Providing strategic leadership and direction on Information Governance and Cyber work prioritisation
IM&G Policy Review Working Group	Chaired by the Head of Information Governance and Cyber. The purpose of this Group is: • Ensuring that an appropriate comprehensive Information Governance and Cyber 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 Governance and Cyber strategy and policy and ensuring regular reviews
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.
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

3. Communication

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 UK Data Protection legislation 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 Governance and Cyber, communication takes place in weekly Management Team Meetings and the DPO Forum and information is cascaded to all members of staff, as appropriate in a weekly messages meeting.
Training	There is an Information Governance Training Strategy. The was last reviewed and approved by IMB in February 2020, with a light touch review undertaken in April 2021. 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. **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

Format	Outline
	• 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 • IDS Security Lead – In depth understanding of all technical information security and assurance. Due to the Covid-19 pandemic all training will be delivered either online or virtually, until such time as it is determined safe to resume face to face / classroom-based training. All staff will 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 mandatory and will be 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 security 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
Newsletter	Since April 2021, a monthly Cyber newsletter has been produced called the 'Cyber Sentinel'. The aim of the newsletter is to increase awareness around Cyber and why it is so important. The Cyber Sentinel highlights the work the team are doing to improve our security position, demonstrate why what we do is already excellent, and the protection it provides against cyber-attacks around the clock. The Cyber Sentinel contains regular topics every month focusing on what is going on in Cyber around the world, our own experiences in Leeds, and looks to make technical jargon more understandable. The Cyber Sentinel was first circulated to the council's CLT, but since due to demand circulation has widened to Best Council Leadership Team and beyond.



4. Statutory and non-statutory information requests

4.1 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 information governance e-learning level 1 and information governance policies and procedures.

4.2 The IG&C service 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.

4.3 Improvements have been made, compared to last year, on responding to Freedom of Information (FOI) / Environmental Information Regulation (EIR) and Individuals Rights(IR) requests within the statutory time limits. This has in part been due to the change of structure and working practices of the newly named and formed Information Governance and Cyber service (IG&C).

4.4 A new operational structure was implemented in IG&C in Q2 2021/22 which supports the move towards a more agile way of working with a new operational management layer responsible for managing and prioritising all IG&C work. This new management layer is also leading on a rolling program of change, which is currently underway, to review all operational processes relating to this area of work and to create standard operating procedures which will drive efficiencies in terms of the time taken to deal with information rights requests.

4.5 The previous external review of the service and internal examination of the requests team function, both undertaken in 2020/21 and reported to Committee in last year's Annual Report, highlighted a number of recommendations for change in order to increase delivery capacity, improve working practices and compliance with statutory requirements. In Q2 2021/22 the dedicated Requests Team was disbanded as part of the new operational structure with clearly defined roles and responsibilities of all IG&C staff. This new operational model supports the development of a multi-disciplinary workforce, intended to increase capacity to deal with information rights requests in a more efficient manner, without the need to increase overall staffing numbers.

4.6 The outcome of this program of change is intended to inform other recommendations to greater ownership with information asset owners for processing and responding to information requests.

4.7 By the end of the financial year 2021/22, the IG&C are intending to submit a report to Corporate Leadership Team outlining the council's recommended approach to further improving performance in handling statutory information requests.

4.8 The table below sets out the number of statutory requests received and handled by the council from 2018/19 to 2021/22(year to date).

	2018/19 FULL YEAR		2019/20 FULL YEAR		2020/21 FULL YEAR		2021/22 YTD	
	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
IRR (including SARs)	855	90	949	83	715	60.8	548	68.5
FOI & EIR requests	2455	93.5	2535	91	2158	84	1438	80.4

The Early Leavers' Initiative in 2019/20, had a significant impact on services' ability to respond to requests. Large numbers of key contacts across the authority left through ELI and this left substantial gaps within services, both in terms of knowledge and capacity to respond to requests. Then Covid in 2020/21, placed increased pressure on front line services, especially services with high volumes of requests to work within statutory timeframes against a backdrop of reduced resources. In many services the coordination of these requests has over time become more and more de-centralised which makes it increasingly difficult to effectively manage these requests. Discussions are under way with services to address this as a priority and to streamline and standardise processes to bring about much needed efficiencies.

4.9 Summary of Requests Received

Individual Rights Requests	The council has received 548 Individual Rights Requests (IRRs) in the first 3 quarters of the financial year 2021/22 and the majority of these, approximately 98%, are subject access requests (SARs). The council had seen a 15% increase in the number of IRRs received in the 2021/22 financial year to date compared to the same period last 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. In the current financial year to date, the council has on average 55-60 open IRRs which is comparable with the same period last year. 37% of IRRs are for access to children's social care records by an 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 1438 Freedom of Information (FOI) and Environmental Information Regulations (EIR) requests in the first 3 quarters of the 2021/22 financial year, this is comparable to the same period in the last financial year. At any one time the council has on average of 100-110 FOI/EIR requests open compared to an average of 170 this time last year. Also at the end of Quarter 3 (2021/22) the performance was at 80.5% against a KPI of 90%. There has been an improvement in

	performance in Quarter 3 which can be attributed to the new ways of working introduced within the IG&C service which are starting to show positive results.
Police, Court & CCTV Requests	The council receives on average 100 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. The number of requests has 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 at Westland Road are supporting viewings which reduces the need to move paper archived records around the city, saving on transport costs, contributing to the reduction of climate and biodiversity impacts and also reducing the IG risks of moving sensitive records.

4.10 ICO & Internal review cases

If a requester is unhappy with the initial response to, or handling of their request, they can 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 55 internal review requests for IRRs/FOIs/EIRs. We have also received 5 other data protection complaints, excluding those which relate to a request, which follow the council's normal two stage process. This represents an 8% decrease compared to the same period last year. The time taken to respond to internal reviews / complaints is significant due to their complex nature. As such, these complaints are handled by Principal Information Governance Officers within the service.

4.11 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, the same number as received in the same period last year. 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.

4.12 Of the 12 cases submitted to the ICO, 4 are still pending and awaiting allocation to an ICO case officer. Of the other 8, 3 were closed as local resolution, 2 were partly upheld and 3 were upheld. Local resolution is where the ICO asks the council to review the request and to contact the requestor to resolve their concerns. In regard to the 3 cases that were upheld, 2 were issued with decision notices. 2 of the upheld cases were in relation to the council's failure to comply with statutory timeframes, and in the third case the ICO instructed the council to disclose some data which it had previously withheld.

Local resolution	3
Partly upheld	2
Upheld - decision notice issued	2
Upheld – No decision notice issued	1
Waiting on ICO to appoint case officer	4

5. Records of Processing Activities

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

5.2 Within the information asset register the following requirements are included:

- Information Asset Owner (directorate and service)
- Name and purpose of asset.
- Categories of personal data/special category data.
- Format it is in, where it is stored, access permissions and volume.
- Retention details.
- If it is shared, internationally transferred or hosted.
- How critical it is and its risk rating.

5.3 As of December 2020, over 1,500 assets had been identified council wide. 30 Information Asset Owners had received reports/presentations regarding the status of their assets. It is acknowledged that there is further work to be done on providing the remaining Information Asset Owners with their reports, risk assessing all assets and amending data within the register regarding service names and Information Asset Owners, following staff leaving the organisation and service redesigns. Work on the project slowed down over 2021, owing to the pandemic, home working and staff shortages.

5.4 It is envisaged the above tasks will be completed by the end of 2022/23 Q1. Following this phase of the Information Asset Register implementation, work will commence on updating the register following the move of data to cloud facilities, producing a dashboard for reporting to the SIRO and linking the assets with the ROPA forms, to provide a holistic picture of data assets and their associated processing activities. The annual review of the Information Asset Register by Information Asset Owners will then commence in 2023.

6. Data Protection by Design and Default

6.1 Data Protection Impact Assessments (DPIAs)

IG&C are leading on a project to review and update the current Data protection impact assessment template and process. The review will encompass all current DPIA templates used by other areas of the business e.g. CCTV DPIAs, ICT Applications DPIAs. The review will also include the digitisation of the form and merging all templates into one smart form.

6.2 Internal Audit have recently carried out an audit of the DPIA process in order to provide assurance that there are appropriate controls in place to ensure that Data Protection Impact Assessments are completed where required. This project will encompass Internal Audit's findings and recommendations.

7. Records Management

7.1 Paper Rationalisation Programme/Asset Rationalisation

Following the pandemic there has been a large amount of work to rationalisation the estate of the organisation. St George House was successfully vacated by the asset management deadline and handed over to the new owners.

7.2 To give an example of the volume of work required to empty council buildings of paper records, St George House had 134 boxes to be moved to new workplace or archived. 30 boxes of files (307 files) to be transferred to Westland Road Records Management Facility. 17 boxes moved to storage prior to being scanned. 69 files destroyed; these were all staff files.

7.3 IG&C will continue to work with Asset Management to support services with office moves and closures over the next year. Facilities management have moved teams/services into Team Zones within Merrion House and Civic Hall and IG&C will conduct an audit to ensure any paper records have been accounted for within these moves, given the services were working from home during this activity.

7.4 IG&C work in partnership with the Corporate Records Management Facility to ensure the secure and appropriate management of our archived records. This has included the implementation of a new SharePoint system to support the management of the records, for both archive inputting and searching and requesting records. We are working with the facility to ensure destructions of paper records beyond their retention are carried out to meet our statutory obligations of not holding data for longer than is necessary and also to free space up at the facility. We are also supporting the facility in coming out of a third-party record storage contract and look to move records in house if possible.

7.5 The council have a scanning framework with Restore Digital to provide scanning contracts where needed across the organisation. This will be married up to the businesses Digital Road Maps to forecast where scanning of records may be needed. Any paper rationalisation work will also look to see where there are digitisation opportunities which may require scanning of records.

7.6 Microsoft 365 and Retention

The Council's Retention Schedule and functions have been mapped against the Local Government Classification Scheme (LGCS) to ensure standardisation with other government bodies and councils. IG&C have been working with the M365/Community Cloud project to use these classifications as labels on the data within Teams Collaboration sites and SharePoint Online sites to add retention policies to automate deletion of records in the M365 environment. Currently the capability of the information management functionality within M365 is being investigated and tested. Once data has been migrated into M365, further work will be done on the data which is 'left over' in the network drives, to delete, archive or transfer for permanent preservation to the West Yorkshire Archive Service

8. Cyber Assurance

8.1 In August 2020, the Integrated Digital Service (IDS) 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.

8.2 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.

8.3 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.

8.4 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 IDS SLT along with the resources required.

8.5 Information Management Board is the escalation route for ISAaC.

8.6 PSN certification was awarded in October 2021.

8.7 The council have completed compliance statements for Cyber Essentials Plus. Cyber Essentials Plus is a UK Government-backed, industry-supported certification scheme introduced in the UK to help organisations demonstrate operational security against common cyber-attacks. These have been signed off by the CDIO (Chief Digital information Officer) and the SIRO (Senior information Risk Officer) and the council's assessment is scheduled for February 2022.

9. Caldicott Guardian

9.1 In August 2021, the National Data Guardian issued guidance on the appointment of Caldicott Guardians, their role and responsibilities in respect of data processing activities undertaken within their organisations. As it is published, under the National Data Guardian's power to issue guidance described within the Health and Social Care (National Data Guardian) Act 2018, those organisations that it applies to, need to give it due regard. The guidance underlines that the relationship between with the Caldicott Guardians and other information governance professionals within an organisation and with decision makers is very important. Further details about these roles and responsibilities can be found in the Appendix – Internal Controls of IG&C.

9.2 The council's Caldicott Guardian and delegates receive a quarterly performance report from the IG&C service, covering all aspects of information governance, including directorate projects, information security incidents and information rights requests.

10. Cyber Assurance

10.1 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.

10.2 The last IT Health Check took place in January 2021. The full report cannot be shared publicly as it documents all vulnerabilities on the estate. The risk score as at 8th February 2021 (following the IT Health Check) had reduced significantly from the previous year.

10.3 The next IT Health Check commences on 21st January 2022 and concludes 21st February 2022. This Committee will be updated when new findings are published.

10.4 Current focus remains on reducing risk from the estate by addressing the findings from vulnerability scanning. Activities are tracked and monitored via the governance articulated in the Effectively Embed section of this report.

10.5 As part of the Council's audit for ITHC and the PSN, additional checks are being introduced in order to provide assurance to the standard 'Cyber Essentials Plus'.

11. 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 people's 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

Probability	Impact	Risk Score	Controls
			- 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: 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. - CIS Shielding policy - HR checks and procedures

Probability	Impact	Risk Score	Controls
			- Employee obligations e.g., contractual, Code of Conduct
CF 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 - Caldicott 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 - Mosaic Shielding policy (currently under review) Level 2 IG training for Children's staff – this is mandatory for access to the Leeds Care Record - Data Security and Protection toolkit - CareCert
RES 33 – Statutory Information Requests: Failure to meet the legal statutory timeframes for responding to information rights requests (FOI/EIR/IRR requests)			
3 – Possible	3 – Moderate	High	– Weekly directorate reports sent to all directorates of all current and late requests – Weekly/monthly monitoring of performance within IG&C service – Creation/implementation of an IG&C SharePoint site to manage and monitor day to day processing of information rights requests – Daily route of internal escalation established within IG&C to reduce late requests – New IG&C management tier to prioritise and manage workloads and ensure appropriate resources in place to manage statutory information rights requests – Rolling program of change to review all operational processes relating to this area of work and to create standard operating procedures which will drive efficiencies in terms of the time taken to deal with information rights requests. – The development of a multi-disciplinary workforce, intended to increase capacity to deal with information rights requests in a more efficient manner – All IG&C staff appropriately trained and skilled through internal workforce development program – Future report to Corporate Leadership Team in regard to greater ownership with information asset owners for processing information rights requests
CD 18 - Lack of compliance with the General Data Protection Regulation (GDPR) Failure to implement and embed effective information management structures, policies, procedures, processes and controls to support the council's business, regulatory and legal requirements to comply with the GDPR			

Probability	Impact	Risk Score	Controls
2-Unlikely	3-Moderate	Medium	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

12. Level 1 Information Governance Training

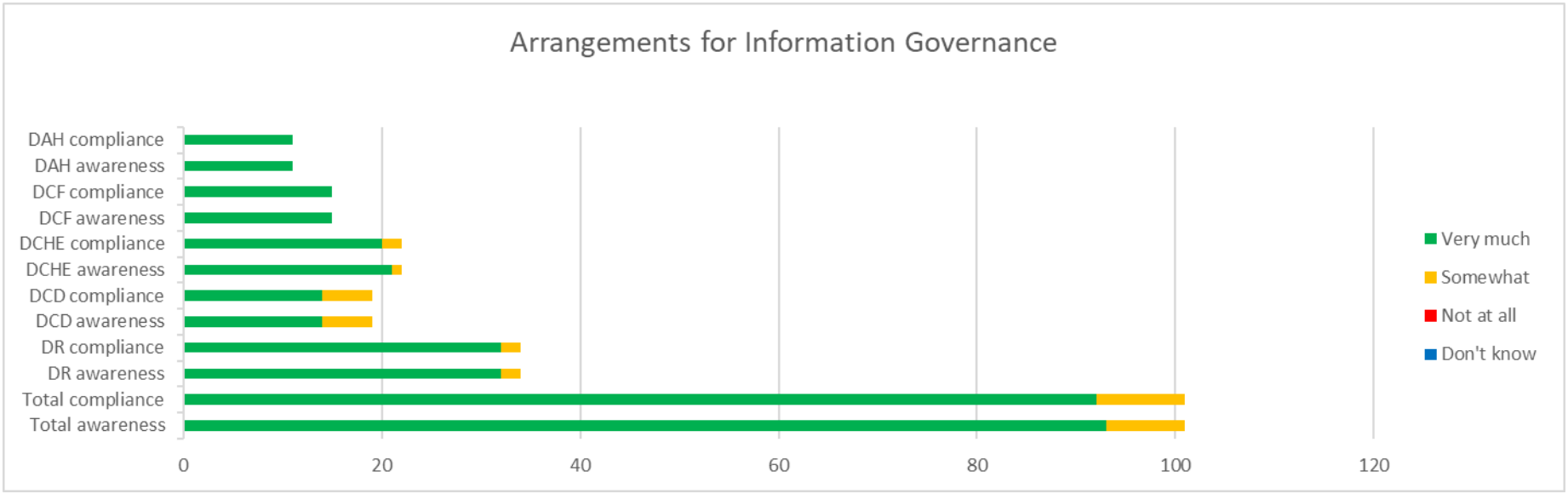
The mandatory Level 1 Information Governance e-learning is updated and launched every two years and a lessons learned report is produced at the end of every iteration. Version 5 of the eLearning product is currently under development with an expected launch date of Mid September.

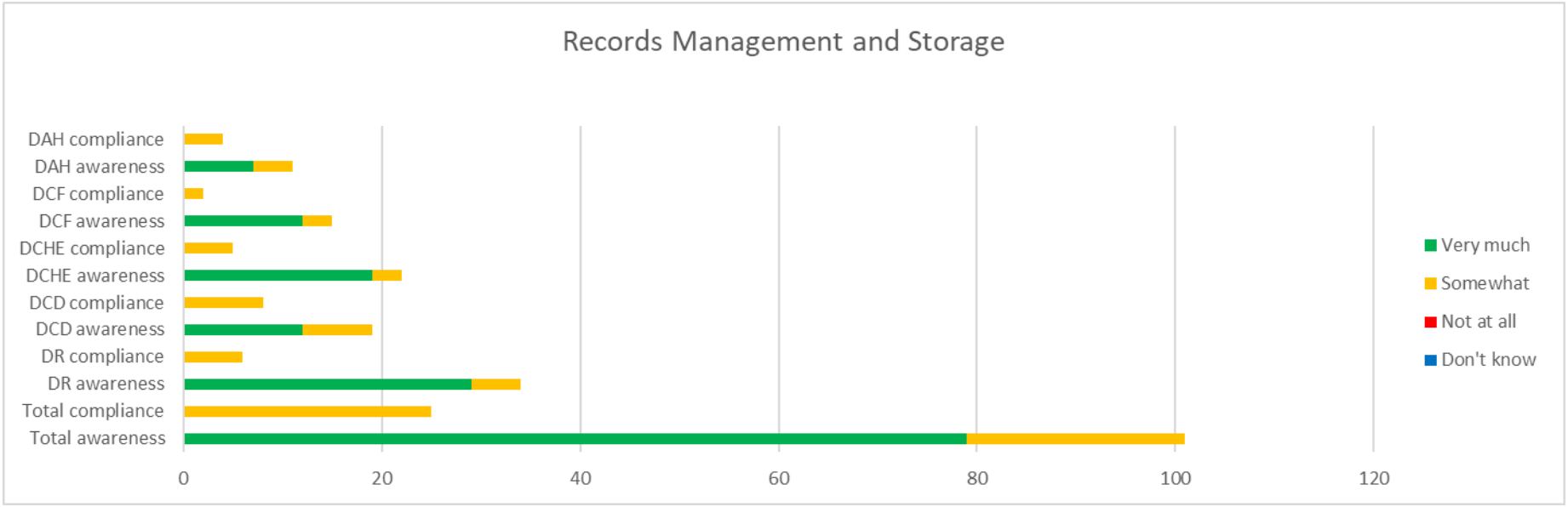
13. Survey of Internal Control

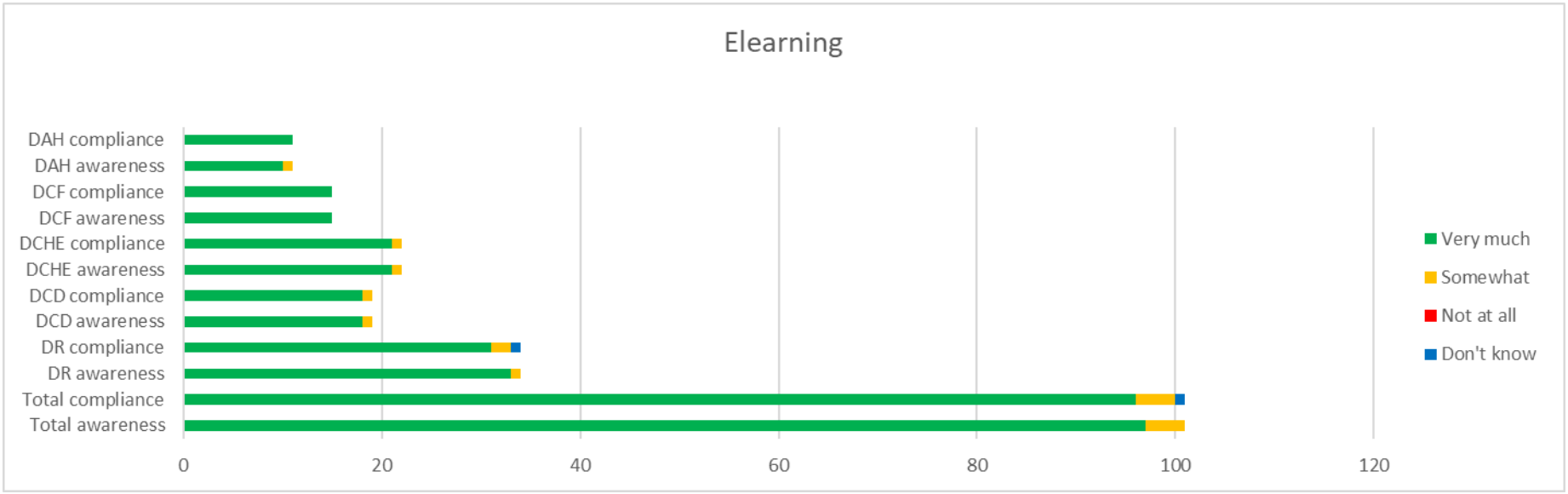
13.1 In May 2021, the council undertook a new Survey of Internal Control in order to provide first line assurance in relation to all key systems of internal control by seeking an assessment from operational managers as to how the arrangements underpinning the Corporate Governance Code and Framework are working on the ground. The survey included questions relating to arrangements for Information Governance. Respondents were asked to rate the extent to which staff were aware of and working in accordance with the following:

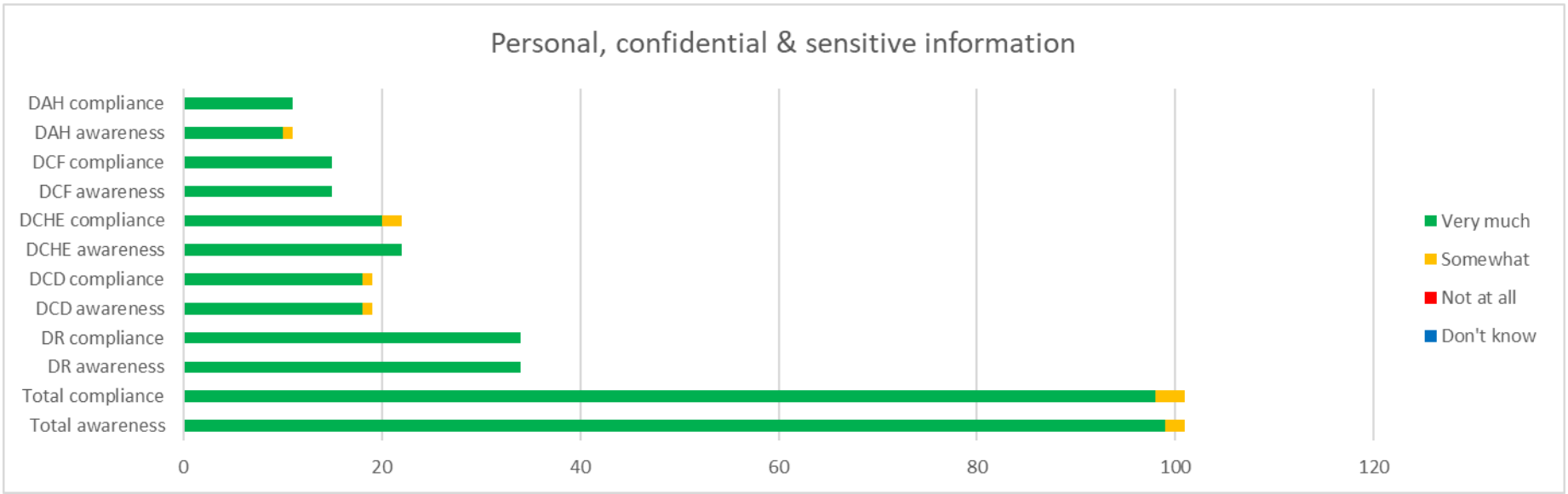
- The Council's arrangements for information governance
- Arrangements for records management and storage in accordance with document retention schedules
- Requirement to complete the information governance e-learning in accordance with corporate timescales
- Requirement to hold and transmit personal, confidential and sensitive information securely
- Requirement to report data breaches
- Requirement to complete a Data Protection Impact Assessment at the outset of any new project or initiative, and/or joint working with other organisations, where personal data is processed, to take into account any risks associated with the proposed project, and mitigate risks accordingly

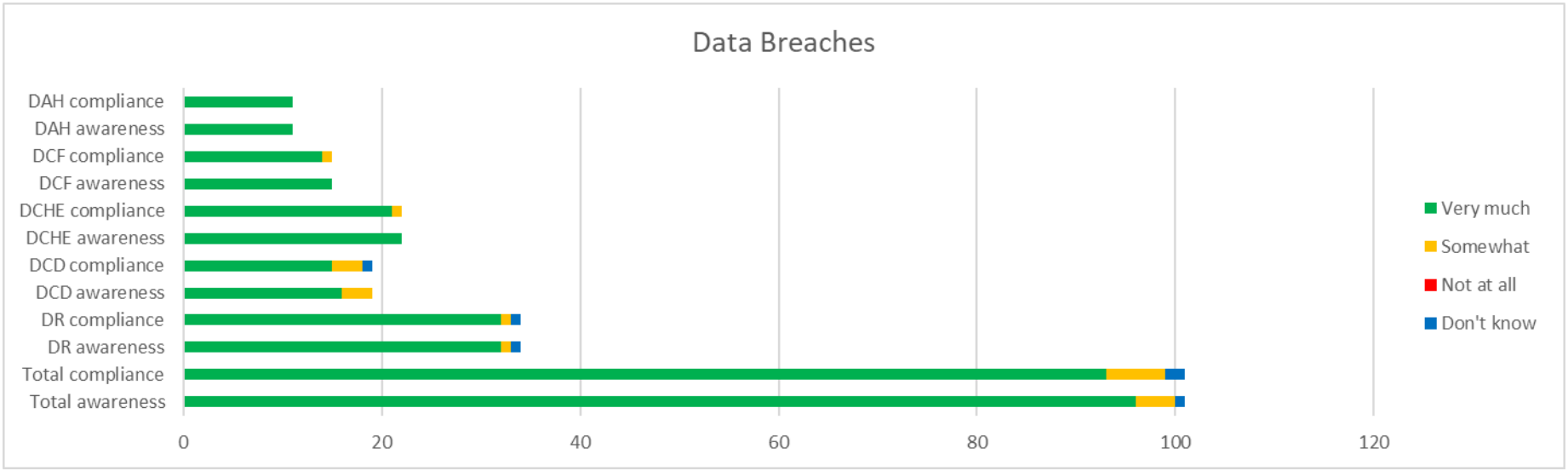
13.2 The charts below show responses in relation to awareness and how well officers work in accordance with controls (compliance) by directorate.

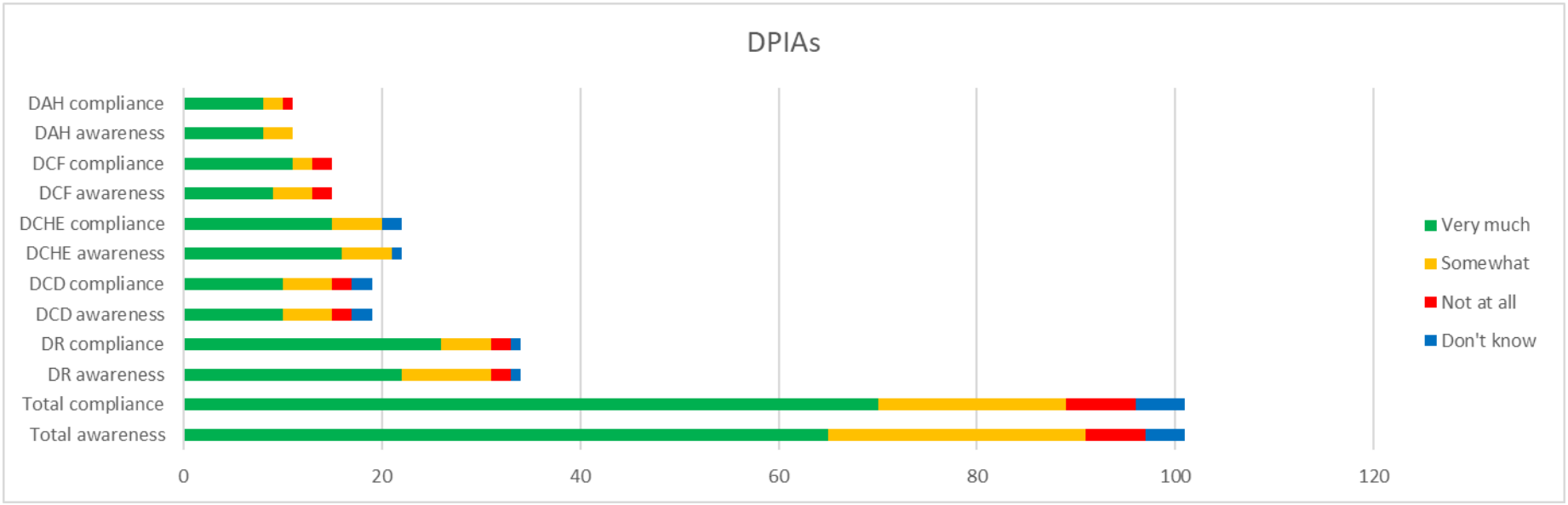

Arrangements for Information Governance
DAH compliance
DAH awareness
DCF compliance
DCF awareness
DCHE compliance
DCHE awareness
DCD compliance
DCD awareness
DR compliance
DR awareness
Total compliance
Total awareness
0
20
40
60
80
100
120
Very much
Somewhat
Not at all
Don't know


Records Management and Storage
DAH compliance
DAH awareness
DCF compliance
DCF awareness
DCHE compliance
DCHE awareness
DCD compliance
DCD awareness
DR compliance
DR awareness
Total compliance
Total awareness
0
20
40
60
80
100
120
Very much
Somewhat
Not at all
Don't know


Elearning
DAH compliance
DAH awareness
DCF compliance
DCF awareness
DCHE compliance
DCHE awareness
DCD compliance
DCD awareness
DR compliance
DR awareness
Total compliance
Total awareness
0
20
40
60
80
100
120
Very much
Somewhat
Not at all
Don't know


Personal, confidential & sensitive information
DAH compliance
DAH awareness
DCF compliance
DCF awareness
DCHE compliance
DCHE awareness
DCD compliance
DCD awareness
DR compliance
DR awareness
Total compliance
Total awareness
0
20
40
60
80
100
120
Very much
Somewhat
Not at all
Don't know





13.3 The results were generally positive. However, across the areas of Records Management and DPIA's the percentage of 'somewhat', 'not at all' and 'don't know' responses indicate that more needs to be done to promote these aspects of information governance. Plans to address this are given in the Effectively Embed section of this Appendix.