OPEN

Audit and Governance Committee

29 September 2025

Information Governance and Security - Review of 2024/25

Report of: Executive Director of Resources (S151 Officer) and Interim Director of Law and Governance (Monitoring Officer)

Report Reference No: AG/01/25-26

Ward(s) Affected: All wards

Purpose of Report

1 This report provides an update on the Council's arrangements for information management, information security, and requests for information during 2024/25.

2 The report provides assurance on the adequacy of governance, risk and control arrangements in these areas, informing the Committee's oversight and understanding, and supporting the Committee in their overall assessment of arrangements.

Executive Summary

3 Information is a critical asset for local authorities, where information is held in trust for its residents and the types of information processed are diverse, varying in levels of sensitivity and risk. Secure and appropriate creation, storage and use of information, and efficient and effective responses to requests for information are essential to ensuring that the organisation can meet its strategic objectives and ethical and legal responsibilities. This report provides the Committee with a summary of the organisation's arrangements to achieve this over the last year.

RECOMMENDATIONS

The Audit and Governance Committee is recommended to:

1. Receive the update paper.
2. Identify any further briefings which may support the Committee's understanding of the assurance provided.

Background

4 Information Management

4.1. Information is a critical asset to many organisations, particularly so for local authorities where information is held in trust for its residents and the types of information processed are so diverse, varying in levels of sensitivity and risk. Handling of information and its assurance is essential to ensuring that the organisation can meet its strategic objectives and ethical responsibilities.

4.2. The report to the committee for 2023/24 provided the background to Information Management and the work of the Information Assurance and Data Management (IADM) Programme. The detail in this report relates to activities and updates on progress.

4.3. The IADM programme is leading key projects which not only underpin the safeguarding of information but also enhance the use of information which will enable the organisation to use information to its full potential where it is appropriate to do so. The programme is focussed on improving ensuring that information is managed throughout the lifecycle, from creation to destruction. A key objective is also the quality of data and layering innovation across this to enable smart reporting, analytics, Artificial Intelligence and other emerging technologies.

4.4. The Programme has used the Gartner's Enterprise Information Management (EIM) Maturity assessment tool to monitor progress and to provide an assessment for future workloads to increase the organisations maturity. The Programme has conducted the self-assessment of its maturity and has also sought external assurance. However, the maturity assessment tool has been updated, so we are now collaborating with them to carry out the new assessment and plan for the review in the coming year.

4.5. This enables the programme to commission projects and stimulate strategic thinking in areas that require focus. The programme uses this assessment tool at the end of every delivery year, so comparisons can be made, reprioritisation and focus can take place where appropriate and the programme business case can be aligned accordingly.

4.6. The tool assesses maturity over seven themes:

- Vision – clear definition of business goals with the vision and initiatives in place to deliver against them.

- Strategy - the level of clarity, outline and communication related to the organisations attitude and approach to information and how this generates benefit.

- Metrics - demonstration of value beyond ICT teams, level of EIM alignment and support of enterprise performance improvements.

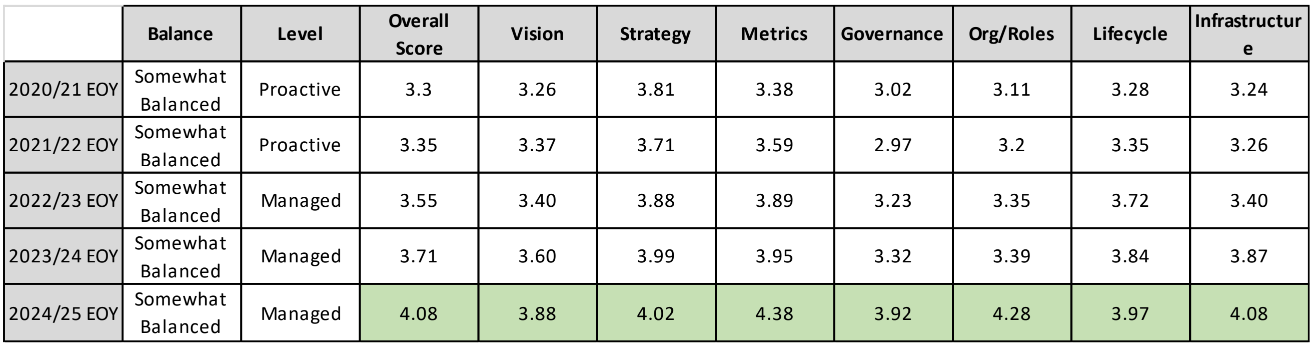
- Governance - frameworks and accountability for the processing of information.

- Organisation and Roles - an established organisation and structure which is accountable for EIM, a cross section of expertise focused on attaining enterprise goals.

- Lifecycle - the proper flow and management of information from creation to deletion.

- Infrastructure - components, information architecture and application needs.

4.7 IADM has self-assessed with the following outcomes, all scores are out of 5, and the assessment is made by aligning back to strategy, commissioning, delivery, business engagement and the effectiveness of business change.



	Balance	Level	Overall Score	Vision	Strategy	Metrics	Governance	Org/Roles	Lifecycle	Infrastructure
2020/21 EOY	Somewhat Balanced	Proactive	3.3	3.26	3.81	3.38	3.02	3.11	3.28	3.24
2021/22 EOY	Somewhat Balanced	Proactive	3.35	3.37	3.71	3.59	2.97	3.2	3.35	3.26
2022/23 EOY	Somewhat Balanced	Managed	3.55	3.40	3.88	3.89	3.23	3.35	3.72	3.40
2023/24 EOY	Somewhat Balanced	Managed	3.71	3.60	3.99	3.95	3.32	3.39	3.84	3.87
2024/25 EOY	Somewhat Balanced	Managed	4.08	3.88	4.02	4.38	3.92	4.28	3.97	4.08

4.8 At the end of the financial year 24/25, using this tool the Council has achieved a maturity rating of “Managed”.

> *“Your organization is among the 15% of those that are clear leaders in their industry with respect to managing and leveraging information across more than two programs. These organizations take a decidedly managed approach to information management, comprising enterprise-level coordination throughout the organization, with effective people, processes, and technologies”.*

4.9 The assessment shows an increase in maturity across all seven categories resulting in a marked improvement in the overall maturity score. This can be attributed to enhanced centralisation of information and the on-going standardisation of information lifecycle management through the on-going implementations of Master Data Management, Enterprise Content Management (ECM), Organisational Reporting, on-going investment in the IADM programme which continues to provide the strategic and cohesive delivery of IM across the organisation. This is dovetailed by the essential engagement and participation of business areas, the business design authority and the wider Digital Portfolio. Further detail on progress can be found in Appendix A – Information Management.

5 Cyber Security

5.1 There is an established robust framework to manage and mitigate information risk, underpinned by a combination of governance, policy, technical, and procedural controls. The following key assurances are in place:

Comprehensive Control Environment

A layered set of controls, including governance, policies, technical safeguards, and staff awareness which ensures effective management of information risk.

Strategic Oversight and Direction

Dedicated governance groups (ISSC, SIGG, IG Collaboration) provide strategic leadership and alignment with organisational priorities.

Policy Framework and Staff Guidance

Staff are supported by regularly updated security policies on CEntranet, promoting secure practices and clear incident response guidance.

Incident Management Assurance

A formal reporting process enables prompt incident handling, reducing recurrence and strengthening future resilience.

Compliance with External Standards

There are key external standards, and regular third-party assessments which are conducted to maintain a strong security posture.

5.2 These assurances reflect a mature and proactive approach to information governance and security. The Council’s commitment to continuous improvement, strategic oversight, and compliance with external standards provides strong confidence in its ability to manage information risk effectively. The assurances are described in detail in Appendix B – Cyber Security.

6 Information Requests

Freedom of Information/Environmental Information Requests

6.1 The Freedom of Information Act (FOIA) 2000 provides public access to recorded information held by the Council. The Environmental Information Regulations (EIR) 2004 provide the same right of access for 'environmental' information.

6.2 The Council received 1,867 FOIA and EIR requests in 2024/25. This is a reduction of 4% (76 requests) from 2023/24. Although there has been a small drop in numbers, it is still a 18% increase on 2022/23.

6.3 The statutory timescale for responding to FOIA and EIR requests is 20 working days. The Council has remained consistent with compliance of 90% of requests being responded to within the statutory timescale, which is the same as 2023/24.

6.4 The requested information was released in full in 56% of requests and partially provided in a further 16% of requests. The information was withheld in full in only 15% of requests. This demonstrates the Council's commitment to openness and transparency, with information being withheld or refused only when appropriate to do so.

6.5 Requested information can only be refused if it falls under one of the specific 'exemptions' within the FOIA or 'exceptions' within the EIR. Of the 282 requests withheld in full or in part, 28 (14%) were withheld due to the cost of responding exceeding the appropriate time limit, 10 (4%) were withheld as vexatious or repeated requests, and the remaining 244 (87%) fell under other exemptions.

6.6 Of those other exemptions, Section 21 FOIA and Section 6(1)(b) EIR (covering information which is already publicly available) were the most cited, making up 40% of all exemptions/exceptions applied. In these cases, the requester is directed to the location of the published information. The majority of FOIA and EIR responses are routinely published in the Council's FOI Disclosure Log, to help reduce the burden of repeat requests and responses.

6.7 FOIA and EIR requests can be made by any individual, company or a pre-existing and identifiable organisation or group if there is a valid name and address for correspondence. 46% of requests were made by individuals, 17% were made by commercial organisations and 10% of requests were from the press or media, which is similar to previous years.

6.8 Requesters can ask for an internal review within two months of the date of the response if they are not satisfied with the Council's initial response. Internal reviews are conducted by a senior officer in the Information Rights Team who was not involved in the initial response. The timescale for responding to internal reviews is 20 working days although this can be extended by up to an additional 20 working days in limited cases.

6.9 An internal review was initiated for 71 (4%) of the 1,806 requests (total requests received, less withdrawn/rejected requests), which is 27% less than 2023/24. Of these, the Council's initial decision was overturned (either in full or part) in 55% of cases, which is the same as the previous year 2023/24. 94% of internal reviews were completed within the required timescale, up from 92% in 2023/24.

6.10 Requesters who remain dissatisfied with the outcome of a public authority's internal review can apply to the Information Commissioner's Office (ICO) for a decision on whether a public authority has handled their request properly. There were nine known complaints to the ICO in 2024/25, which is an increase of five from the previous year. Of these only two complaints were upheld by the ICO, one was informally resolved, and five were not upheld. One complaint is ongoing.

Individual Rights Requests

6.11 The UK General Data Protection Regulation (UK GDPR) provides individuals with several rights relating to their personal data, including the Right of Access (also known as a Subject Access Request (SAR)). This allows individuals to request copies of their own personal information, as well as providing other individual rights such as right of erasure or rectification. These are known as Individual Rights (IR) Requests.

6.12 The statutory timescale for responding to IRRs is one calendar month although the UK GDPR allows the deadline to be extended by up to an additional two months in certain cases, for example where requests are complex.

6.13 The Council received 357 IR requests during 2024/25. This is a reduction of 12 (3%) from 2023/24. As well as a slight decrease in volume, there has also been a reduction in compliance. This is due mainly to the complexity and size of some requests, which can run into the tens of thousands of pages. 81% of requests were responded to within the statutory timescale, down 6% from 2023/24.

6.14 Of the 357 IR requests received, 248 requests (69%) related to information held by Children's Services, with requests typically originating from care leavers and parents wishing to access social care and SEND records for their children.

Disclosure Requests

6.15 Requests for release of personal data from third-party agencies are referred to as Disclosure Requests. Requests are received from various authorities such as the Police, Government Departments including HMRC and DWP, solicitors, other Local Authorities or regulatory bodies as well as commercial organisations such as insurance companies requesting CCTV footage.

6.16 Disclosure requests are made citing one or more of the discretionary exemptions detailed in the Data Protection Act 2018 (DPA). However, it is important to note that this does not give an automatic right of access to information. The merits of requests are carefully assessed by the Information Rights Team before deciding whether to apply an exemption. There is no obligation on the Council to disclose if there are genuine concerns about releasing any personal information, although the Council aims to co-operate with our partner agencies where it is necessary and proportionate to do so.

6.17 As disclosure requests are not a legal obligation there is no statutory timescale for responding, however we aim to respond to all requests within one calendar month of receipt in line with other data protection requests.

Data Protection Complaints

6.18 Complaints are sometimes received regarding alleged infringements of data protection legislation, some of which result in complaints to the Information Commissioner's Office (ICO). Data protection complaints fall outside the scope of the corporate complaints policy because there is a statutory process for data protection compliance and recourse is to the ICO rather than the Local Government and Social Care Ombudsman (LGSCO). Some complaints come directly from the data subject, and some originate from the ICO where the data subject has made a complaint directly to them without going through the Council's complaints process.

6.19 In 2024/25, data protection complaints represented 0.59% of the total number of complaints received by the Council, compared to 1.11% in 2023/24. Of the 23 data protection complaints, 30% were not upheld, compared to 64.7% in 2023/24.

6.20 Reasons for data protection complaints primarily relate to an alleged data breach and some are regarding the handling of IR requests, either exceeding the statutory deadline or not providing all the information the subject was expecting.

6.21 Detailed statistics can be found in Appendix C – Information Requests.

6.22 Data Protection Compliance

6.23 Accountability is a fundamental principle of the UK GDPR, and the Council must be able to demonstrate its compliance with the legislation. An initial assessment of the Council's data protection compliance was undertaken in 2023/24 using the ICO's accountability framework.

6.24 The initial self-assessment showed that 63% of the Council's activities fully meets the ICO expectations and 28% partially meets the ICO expectations. The assessment showed a positive position for the Council's data protection compliance at that time.

6.25 The ICO has launched a more extensive data protection audit framework, which will be used to re-assess and audit current data protection practices against the ICO's expectations. The new accountability framework is divided into nine toolkits, each addressing a core area of data protection compliance with individual trackers to assess procedures and the risks to personal information. The Data Protection Officer and Deputy Data Protection Officer will engage with relevant stakeholders to support the audit and assessment process.

Consultation and Engagement

7 It has not been necessary to consult on the contents of this report.

Reasons for Recommendations

8 In line with Committee's responsibility for receiving assurances on the effectiveness of arrangements for governance, risk and internal control, this report provides assurance to Committee on the adequacy of the Council's arrangements for information management, information security, and requests for information received under relevant legislation during 2024/25. The report supports the corporate objective of being an open and enabling organisation.

Other Options Considered

9 Not applicable as report is for information and assurance.

Implications and Comments

Monitoring Officer/Legal/Governance

10 The Council must comply with relevant legislation relating to information management and security, including the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, Computer Misuse Act 1990, Freedom of Information Act 2000 and Environmental Information Regulations 2004.

11 The Council needs to understand what data they are responsible for and what information is processed on their behalf by third party providers, building data protection into its day-to-day activities to ensure a privacy by design approach.

Section 151 Officer/Finance

12 There are no direct additional financial costs arising from this report other than in the event of non-compliance. Failure to comply with the UK GDPR, Data Protection Act and information rights legislation can attract enforcement action by the Information Commissioner's Office (ICO). This could include financial penalties of up to £17.5m for public authorities, public reprimands, enforcement notices or decision notices, all of which would cause financial and reputational damage.

Human Resources

13 There are no human resources implications arising from this report.

Risk Management

14 Inappropriate actions, improper use, storage and deletion of information by employees or third parties can present challenges which could affect the level of inefficiency and security or cause financial or reputational damage to the organisation. The measures and mitigations set out in this report describe how these risks are managed across the organisation.

Impact on other Committees

15 There are no implications affecting other Committees arising from this report.

Policy

16 There are no policy implications directly arising from this report.

Equality, Diversity and Inclusion

17 There are no equality, diversity or inclusion implications arising from this report.

Other Implications

18 Management and protection of information is essential to ensure the right levels of care are given to those residents that require it, and to ensure that accurate records are maintained and supplied in a timely manner when requests for that information are made.

Consultation

Name of Consultee	**Post held**	**Date sent**	**Date returned**
Statutory Officer (or deputy) :			
Ashley Hughes	S151 Officer	11/09/25	12/09/25
Kevin O'Keefe	Interim Monitoring Officer	11/09/25	12/09/25
Legal and Finance			
Julie Gregory	Acting Head of Legal Services	04/09/25	08/09/25
Chris Benham	Director of Finance	04/09/25	10/09/25
Other Consultees:			
Gareth Pawlett	Director of Digital	11/09/25	12/09/25
Josie Griffiths	Head of Audit Risk and Assurance	11/09/25	15/09/25

Access to Information	
Contact Officer:	Gareth Pawlett, Director of Digital (SIRO) Julie Gibbs, Information Rights Manager (DPO) gareth.pawlett@cheshireeast.gov.uk julie.gibbs@cheshireeast.gov.uk
Appendices:	Appendix A – Information Management Appendix B – Cyber Security Appendix C – Information Requests
Background Papers:	Information Governance – Review of 2023/24 Audit and Governance Committee, 30 September 2024