Audit and Governance Committee

30th September 2024

**Information Governance and Security -
Review of 2023/24**

**Report of: Director of Governance and Compliance, Director of
Finance and Customer Services**

Report Reference No: AG/21/24-25

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 received under relevant legislation during 2023/24.

2.   This report is provided to the committee to provide 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.

Background

Information Management

4.   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.

5.   The report to the committee for 2022/23 provided the background to Information Management and the work of the Information Assurance and Data Management Programme. The detail in this report relates to activities and updates on progress.

6.   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.

7.   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 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.

8.   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 pertaining 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.

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

	Balance	Level	Overall Score	Vision	Strategy	Metrics	Governance	Org/Roles	Lifecycle	Infrastructure
2016/17 EOY	Somewhat Unbalanced	Proactive	2.72	3.07	3.63	3.25	2.69	1.9	2.33	2.2
2017/18 EOY	Somewhat Unbalanced	Proactive	2.52	3.03	3.64	2.13	2.43	1.9	2.34	2.2
2018/19 EOY	Somewhat Balanced	Proactive	3.01	3.29	3.61	2.82	2.95	2.97	2.74	2.67
2019/20 EOY	Somewhat Balanced	Proactive	3.18	3.25	3.65	3.26	2.96	3.06	3.05	3.05
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	3.4	3.88	3.89	3.23	3.35	3.72	3.4
2023/24 EOY	Somewhat Balanced	Managed	3.71	3.6	3.99	3.95	3.32	3.39	3.84	3.87

10.   At the end of the financial year 23/24, 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".

11.   The assessment shows a further tangible increase in maturity level, this lends itself to the programme having worked on resolving legacy

issue and having plans in place to continue to do so as well as building on this with innovative new ways of working through Master Data Management and Enterprise Content Management (ECM). Over the last year, the programme has again increased its score across all assessment areas.

12. The direction and delivery of IADM is focused on these themes through several different channels with the aim to increase the organisations maturity levels, by doing this, the authority can be assured that information is being protected and utilised in ways which benefit both service delivery and compliance.

13. The aim of programme is to increase the maturity and move the overall assessment to a level of Highly Balanced which will ensure that information is used efficiently and consistently across the organisation. IADM is not striving for best practice for best practice's sake, the programme is focussing on pain points so improvements in maturity don't only lend themselves to strategic success but improve and optimise delivery.

14. Over the last two phases of IADM, the programme has delivered extensive amounts of learning materials and events to assist the organisation mature in its use and understanding of Information. The ownership and accountability of information management at the business area level has significantly matured.

15. All projects under IADM with business stakeholders, have business representation at either project board or steering group level, and so this by default has and is continuing to grow knowledge of information management processes.

16. AI is increasingly becoming a technology used by many organisations to enhance and speed up processes, it provides users with a lot of power in analysing data and creating outputs. Fundamentally, for AI to benefit the organisation and for it to work well, information must be accurate and up to date, AI will only create quality outputs if the data it is crawling is current and relevant. The activities therefore being delivered under IADM, will directly enable this.

17. Enterprise Content Management is applying retentions to all data on SharePoint (SP) and Fileshares, ensuring information that has reached its retention period is destroyed automatically.

18. Master Data Management is a method used to define and manage critical business data as a single point of reference, creating an up to date, trusted, central dataset which can be leveraged across the

organisation to ensure information is consistent across business systems.

19. It has directly improved data quality, data processes and digital services. Currently, the domains include several data feeds, in some cases this includes the two-way movement of data from MDM to the source systems. The activities and resultant processes will support the on-going enrichment of the MDM domains, ensuring direct improvements are delivered.

20. MDM is being delivered across four domains – Resident, Employee, Location and Business, and this has directly improved data quality, data processes and digital services.

- Using the MDM Employee record to improve and enhance the starters, movers and leavers process, improve the licence management, access rights (both physical and digital), improving currency and consistency of data across systems and technologies.

- Using the Resident record to bring together data from across core systems and ensure the Resident core fields are consistent across all these systems, further to this, using the record to the generate intelligence by creating views across the data, whether this be for single view of debt, use of the single persons discount, relationships in households and so forth.

- Using the Location record to ensure all addresses across systems are fed by the LLPG and using references beyond the UPRN to enable a golden thread between addresses and locations.

- Using the Business record to identify correct use of business benefits and rates, and other business-related processes.

21. MDM will by its nature significantly improve the data quality of information across systems, by harmonising these four key areas irrespective of where a Resident or Employee engages the organisation, the information will be the same, in terms of accuracy, quality, format and currency. Initial phases of MDM have shown that when cross referencing the same Resident information in different areas of the organisation there are up to 40% levels of inaccuracy between the records.

22. Adopting the MDM strategy and delivering MDM will hook into benefits not only with Information Governance (IG) but with Digital working and across the wider organisation. MDM will enable the organisation to support the National Fraud Initiative by harmonising data across systems and so businesses will be able to identify inaccuracies and inconsistencies with the information held. It will support and enable the Data Quality strategy, and align to the strategic objective of making decisions based on accurate and consistent information, MDM will automate the corrections of data quality issues as far as it possibly can, rather than requiring the workforce to do so, this will provide efficiencies and benefit on several fronts, reduction in the time spent on correcting records, reduction in the time spent trying to find records which are incorrectly recorded, validation of services being given (correctly or incorrectly) and currency of data across several areas.

23. The ECM delivery will put controls in place for legacy and newly created data that does not belong in a case management system, it is a central part of realising the strategic intent and benefits of IADM as well as GDPR, records management and security compliance. The organisation will not be managing vast amounts of content throughout the information lifecycle if ECM is not embedded to some extent. The organisation processes large volumes of content which is saved across many systems and platforms. It is the objective of ECM to standardise, simplify and rationalise the ways in which this content is held, used, stored and destroyed. It is essential for information compliance that the organisation understands the information it has, where it is held and is assured that it's being held for the correct periods of time. Standardising the classification and retention of content is central to this compliance and there are two parts to this, legacy content and content management for the future. Completing the implementation of ECM will also directly benefit technologies for the future, especially AI.

Information Security

24. There are a number of Information and Data Security policies which are published on the CEntranet and help to protect the Council from inappropriate and unauthorised access.

25. Progress on Information Risk and Information Security is monitored through the Information Security Steering Committee (ISSC), Strategic Information Governance Group (SIGG) and the IG Collaboration Group.

26. The Council complies with the Public Services Network (PSN) Code of Connection, NHS Data Security and Protection Toolkit, DWP's MOU

and NHS Digital controls, these controls and adherence to their standards provide assurance that the controls operated are consistent with central government and other peer authorities.

27.   There is further validation of controls through the assessment of third-party IT hardware and software vendors during the procurement phase, if any vulnerabilities are found then a mitigation plan is drawn up and actioned.

28.   Data Classification through protective marking has been rolled out to the organisation; this allows the categorisation of information so that appropriate controls can be employed to protect that information.

29.   The Council provides security and compliance on several e-learning modules (some of which are mandatory for all employees) on the Learning Lounge. This includes several modules of Data handling, Cyber Security, and Information Assurance. Work has begun on a new cyber e-learning package developed by NCSC and the content of data handling training is currently under review. There are also several best practice guides on the Councils Lighthouse on the best ways to use technology and to protect information. These modules and best practice guides are updated regularly to reflect changes in working practices and as a response to additional threats.

30.   Controls are in place to restrict access to the data centres and network equipment and risk assessments of existing systems and networks are on-going.

31.   The Council's ICT Services have a strategic direction to move to a "Cloud First" principle, whilst this enables an evergreen environment which is always up to date, additional controls are needed to prevent compromise or inappropriate use and access. This includes contract compliance and monitoring to ensure ongoing protection of information. To support the strategic direction and architecture principles all technical solutions are reviewed at the Technical Design Authority to ensure correct alignment.

32.   In addition, the Council is moving to Zero Trust architecture, this is a direct result of increased threats posed to the working infrastructure. This shift is in line with the latest thinking and guidelines issued by the NCSC.

33. A separate, focused briefing has been given to members of the Committee on Cyber threats and organisation mitigations and controls.

Information Requests

Individual Rights Requests

34. 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) which allows individuals to request copies of their own personal information, as well as other individual rights such as right of erasure or rectification. These are known as Individual Rights (IR) Requests.

35. 364 IR requests were received during 2023/24. This is an increase of 117 (47%) from 2022/23 and represents the largest number of requests received in a single financial year in the last five years.

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

37. Despite the increase in volume, 87% of requests were responded to within the statutory timescale, up 17% from 2022/23.

38. Of the 364 IRRs received, 268 requests (74%) related to information held by Children's Services, within requests typically originating from individuals, including care leavers and parents wishing to access social care records.

Year	IRR requests received	% Responded to on time
2019/2020	250	77%
2020/2021	191	72%
2021/2022	202	49%
2022/2023	247	70%
2023/2024	364	87%

Disclosure Requests

39. Requests for release of personal data from third-party agencies are referred to as Disclosure Requests.

40. Requests are received from various authorities such as the Police, Government departments including HMRC, solicitors, other Local Authorities or public bodies and regulatory bodies as well as

commercial organisations such as insurance companies requesting CCTV footage.

41. 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. We must assess the merits of requests and decide whether to apply the exemption; there is no obligation on the Council to disclose information if we have genuine concerns about releasing any personal information.

42. As disclosure requests are not a statutory obligation there is no statutory timescale for responding, however we aim to respond to all requests within one calendar month of receipt.

43. Disclosure requests are recorded and processed centrally by the Information Rights Team; however, the Council Tax Team also records and responds to requests specifically relating to Council Tax liability and verification of address details.

Year	Responded to by Information Rights team	Responded to by Council Tax	Total Disclosure Requests received
2020/2021	320	553	873
2021/2022	403	412	815
2022/2023	433	514	947
2023/2024	536	309	845

Data Protection Complaints

44. The table below shows the number of complaints received regarding alleged infringements of data protection legislation, some of which result in complaints to the Information Commissioner's Office (ICO). 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. These figures are included in the total number of complaints received by the Council which is presented to Committee separately under the relevant service area but not explicitly about data protection.

Source of complaint	2023/24	2022/23	2021/22	2020/21
Data Subject	34	29	31	20
ICO	3	2	5	1
Total	**37**	**31**	**36**	**21**

45.   The number of data protection complaints received is minimal when compared to the total number of complaints received by the Council. In 2023/24, data protection complaints represent 1.11% of the total number of complaints received, compared to 1.17% in 2022/23. Of the 37 complaints, 64.7% were not upheld, compared to 48.3% in 2022/23.

46.   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.

Reason for complaint	2023/24	2022/23	2021/22	2020/21
Alleged data breach	97%	94%	90%	100%
Handling of IR request	3%	3%	7%	0%
Other	0%	3%	3%	0%

Compliance

47.   Accountability is one of the key principles in data protection law and the Council must be able to demonstrate its compliance. An initial assessment of the Council's current data protection compliance was undertaken in 2023/24 using the ICO's accountability framework.

48.   The accountability framework is divided into 10 categories and each category can be measured in four different ways:

- Not meeting ICO expectations

- Partially meeting ICO expectations

- Fully meeting ICO expectations

- Not applicable

49.   The initial self-assessment shows that 63% of the Council's activities fully meets the ICO expectations; 28% partially meets the ICO expectations; and only 6% does not meet ICO expectations, which represents 18 instances out of a possible 324. This assessment shows a positive position for the Council's current data protection compliance.

50.   Work is now underway to identify recommendations and actions to improve data protection compliance across the organisation.

Freedom of Information/Environmental Information Requests

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

52.   1,943 FOIA and EIR requests were received in 2023/24. This is an increase of 19% from 2022/23 and represents the largest number of requests received in a single year since records began.

53.   The statutory timescale for responding to FOIA and EIR requests is within 20 working days. Despite the increase in volume, 90% of requests were responded to within the statutory timescale of 20 working days, up 1% from 2022/23.

54.   The requested information was released in full in 65% of requests, and partially provided in a further 10% of requests. The information was withheld in full in only 14% of requests. This demonstrates the Council's commitment to openness and transparency, with information being withheld or refused only when appropriate to do so.

55.   Requested information can only be refused if it falls under one of the specific 'exemptions' within the FOIA or 'exceptions' within the EIR.

56.   Of the 269 requests withheld in full or in part, 39 (14%) were withheld due to the cost of response exceeding the appropriate time limit, 5 (2%) were withheld as vexatious or repeated, and the remaining 209 (78%) fell under other exemptions.

57.   Of these other exemptions, Section 21 FOIA and Section 6(1)(b) EIR (covering information which is already publicly available) were by far the most commonly cited overall, making up 36% of all exemptions/exceptions applied. In these cases, the requester is directed to the location of the published information.

58.   The majority of FOIA and EIR responses are routinely published in the Council's FOI Disclosure Log, in an effort to reduce the burden of repeat requests and responses.

59.   FOIA and EIR requests can be made by any individual, company or a pre-existing and identifiable organisation or group. 46% of requests were made by individuals, 22% were made by commercial organisations and 10% of requests from the press or media, which is similar to previous years.

60.   Requesters are able to ask for an internal review if they are not satisfied with the Council's initial response. Internal reviews are

conducted by someone who was not involved in the initial response, usually by a senior officer in the Information Rights Team.

61. An internal review was initiated for 89 (5%) of the 1,872 requests (total requests received, less withdrawn/rejected requests), down by 1% from 2022/23. Of these, the Council's initial decision was overturned (either in full or part) in 55% of cases, up from 36% in 2022/23.

62. 93% of internal reviews were completed within the required timescales (usually 20 working days, subject to limited permitted extensions), up from 73% in 2022/23.

63. Requesters who remain dissatisfied with the outcome of a public authority's internal review can apply to the Information Commissioner (ICO) for a decision on whether or not a public authority has handled their request properly. There were only 4 known complaints to the ICO in 2023/24. Of these only 1 complaint was upheld by the ICO, 1 was informally resolved, and 2 were not upheld.

64. Further breakdowns for FOI and EIR requests are shown in the tables below.

Volume of FOI and EIR requests received

Type of Request	2023/24	2022/23	2021/22	2020/21
FOIA and EIR Requests	1,943	1,639	1,539	1,474
Property Search EIR Requests[1]	3,137	3,586	2,624	2,735
Total FOI/EIR Requests	5,080	5,225	4,163	4,209

Timeliness – FOI and EIR requests closed within the statutory deadline

Directorate	2023/24	2022/23	2021/22	2020/21
Corporate	94%	92%	95%	97%
Place	86%	86%	96%	95%
Adults Social Care	99%	90%	97%	98%
Childrens Services	90%	97%	99%	98%
Cheshire East Overall	**90%**	**89%**	**96%**	**97%**

---

[1] It should be noted that 'Property Search' search requests are also recorded and responded to under the EIR. These are enquiries made to local authorities by Personal Search companies, to make prospective buyers of properties aware of relevant issues before they complete their purchase. These requests are processed separately to a 'typical' EIR request and responded to directly by the Land Charges Team. All requests are completed within the statutory timescale and are not included in the information in this report, unless explicitly stated.

Outcome of FOI and EIR requests

Outcome	2023/24	2022/23	2021/22	2020/21
Information granted in full	1,213	1,027	829	856
Information not held	151	115	136	107
Information partially provided	192	159	214	191
Information withheld in full	269	251	286	257
Clarification was not provided	47	36	31	38
Request rejected (duplicate/not valid)	40	20	29	13
Request withdrawn by requester	31	31	14	11

Exemptions and Exceptions

FOIA Exemptions	2023/24	2022/23	2021/22	2020/21
Section 12: Exceeds appropriate time limit[2]	39	43	55	9
Section 14: Vexatious or repeated requests	5	5	2	0
Section 21: Info accessible by other means	98	75	90	79
Section 22: Intended for future publication	8	7	7	6
Section 24: Safeguarding national security	0	3	1	0
Section 30: Investigations and proceedings	3	0	1	15
Section 31: Law enforcement	18	26	40	68
Section 32: Court or inquiry records	0	0	0	0
Section 33: Public audit functions	0	0	0	0
Section 36: Conduct of public affairs	0	2	0	1
Section 40: Personal information	34	25	44	43
Section 41: Info. Provided in confidence	32	37	19	10
Section 42: Legal professional privilege	1	0	2	1
Section 43: Commercial interest	10	13	12	7
Section 44: Prohibitions on disclosure	0	2	0	0
EIR Exceptions	**2023/24**	**2022/23**	**2021/22**	**2020/21**
Reg 6(1)(b) Publicly Accessible	46	52	57	52
Reg 12(3) Personal Information	29	18	8	2
Reg12(4)(a) Information Not Held	3	3	11	4
Reg12(4)(b) Manifestly unreasonable	24	21	21	1
Reg 12(4)(c) Too general	0	1	1	0
Reg 12(4)(d) Draft Information	4	5	4	0
Reg12(4)(e) Internal Communications	1	2	1	0
Reg 12(5)(b) Course of Justice	29	13	5	0
Reg 12(5)(c) Intellectual Property Rights	0	0	0	0
Reg 12(5)(d) Confidential Proceedings	1	6	1	0
Reg 12(5)(e) Commercial Interests	10	3	2	0
Reg 12(5)(f) Information in Confidence	0	0	2	0
Reg 12(5)(g) Protection of Environment	0	1	2	0

---

[2] The 'appropriate limit' is 18 hours. If answering the request would exceed this limit, the request can be refused. Advice and assistance is provided to the requester as to how they could submit a revised, reduced request

Total exemptions/exceptions	395	363	388	298

* Please note that the totals for exemptions in the above table may sum to more than the number of requests refused, as multiple exemptions may be applied to an individual request.

Source of FOI and EIR Requests

Source	2023/24	2022/23	2021/22	2020/21
CEC Councillor	0%	1%	<1%	1%
Charity	3%	3%	<1%	Not recorded
Commercial	22%	23%	32%	32%
Individual	46%	42%	39%	40%
MP	0%	<1%	<1%	1%
Other	0%	1%	1%	<1%
Press or media	10%	9%	9%	9%
Pressure Groups	1%	2%	3%	4%
Public Sector	1%	1%	1%	1%
Researchers	3%	3%	2%	2%
Solicitor	1%	<1%	Not recorded	Not recorded
Student	0%	<1%	Not recorded	Not recorded
Town or Parish Councillor	1%	2%	Not recorded	Not recorded
whatdotheyknow.com[3]	10%	11%	11%	9%

Internal reviews

	2023/24	2022/23	2021/22	2020/21
Internal reviews received	89	94	93	73
Original decision upheld in full	40	58	56	40
Original decision overturned	30	18	17	13
Original decision partially upheld	19	15	14	19
Internal Review Withdrawn	0	3	6	1
Internal reviews closed within timescale	93%	73%	94%	93%

Complaints to the ICO

Outcome	2023/24	2022/23	2021/22	2020/21
Informally resolved	1	0	1	1
Complaint not upheld	2	5	2	4
Complaint Upheld	1	2	3	1
Complaint Withdrawn	0	2	3	0
Total complaints received	4	9	9	6

Consultation and Engagement

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

---

[3] 'whatdotheyknow.com' is a website used to make FOI and EIR requests

Reasons for Recommendations

66.   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 2023/24. The report supports the corporate objective of being an open and enabling organisation.

Other Options Considered

67.   Not applicable as report is for information and assurance.

Implications and Comments

Monitoring Officer/Legal

68.   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.

69.   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

70.   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.

Policy

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

Equality, Diversity and Inclusion

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

Human Resources

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

Risk Management

74.   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.

Rural Communities

75.   There are no implications affecting rural communities arising from this report.

Children and Young People including Cared for Children, care leavers and Children with special educational needs and disabilities (SEND)

76.   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.

Public Health

77.   There are no public health implications arising from this report.

Climate Change

78.   There are no climate implications arising from this report.

Access to Information	
Contact Officer:	Gareth Pawlett, Chief Information Officer gareth.pawlett@cheshireeast.gov.uk Julie Gibbs, Information Rights Manager (DPO) julie.gibbs@cheshireeast.gov.uk
Appendices:	None
Background Papers:	Information Governance Update 22/23 - July 2023 Audit and Governance Committee