MIDDLESBROUGH COUNCIL	Middlesbrough moving forward

Report of:	Head of Governance, Policy and Information and Senior Information Risk Owner (SIRO), Ann-Marie Johnstone
Submitted to:	Audit Committee
Date:	25 September 2025
Title:	Annual Report of the Senior Information Risk Owner (SIRO)
Report for:	Discussion
Status:	Public
Council Plan priority:	Delivering Value for Money

Proposed decision(s)

That the Audit Committee:

- **NOTES** the position in respect of information governance as set out in the report and the arrangements in place to manage them
- **CONSIDERS** whether the information provided is sufficient to provide them with assurance that information governance arrangements that are in place are sufficient. If the committee is dissatisfied, it is asked to give direction on the additional information it requires in order to be assured about the Council's Information Governance arrangements.

Executive summary

This report sets out arrangements in place to ensure the proper governance of information within the Council, progress made within the 2024 calendar year, risks and issues arising, and priorities for 2025.

This report provides assurance to the Committee that Information Governance (IG) policy and practice within the Council is in line with legal obligations, and consistent with the principles of good governance.

It provides an update on activities and planned actions across the policy framework, the refresh of the Information Strategy, data protection, information security, cyber security, records management, surveillance, information requests and physical access controls.

1. Purpose of this report and its contribution to the achievement of the Council Plan ambitions

1.1 To advise the Audit Committee of arrangements in place to ensure the proper governance of information within the Council, progress made within the 2024 calendar year, risks and issues arising, and priorities for 2025/26.

Our ambitions	Summary of how this report will support delivery of these ambitions and the underpinning aims
A successful and ambitious town	This report sets out the measures the Council has in place to ensure an appropriate approach to information governance and plans to strengthen it over the next 12 months. Delivery of this activity will support delivery of these ambitions by ensuring that the Council has systems, processes and policies in place to manage, retain, use and dispose of data in line with legislative requirements.
A healthy Place	
Safe and resilient communities	
Delivering best value	Delivering activity within an approach to information governance that ensures the Council complies with its legislative requirements.

2. Recommendations

2.1 That the Audit Committee:

- **NOTES** the position in respect of information governance as set out in the report and the arrangements in place to manage them
- **CONSIDERS** whether the information provided is sufficient to provide them with assurance that information governance arrangements that are in place are sufficient. If the committee is dissatisfied, it is asked to give direction on the additional information it requires in order to be assured about the Council's Information Governance arrangements.

3. Background and relevant information

The Information Governance Framework

3.1 The Council must create, protect, manage, share and disclose information in line with a complex legal framework. This report deals principally with information governance arrangements relating to the following, and the risks arising from:

- Data Protection Act 2018 (DPA)
- UK General Data Protection Regulation 2016 (UK GDPR)
- Privacy and Electronic Communications Regulations 2003 (as amended)
- Environmental Information Regulations 2004 (EIR)
- Freedom of Information Act 2000 (FOI)
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Protection of Freedoms Act 2012 (PoFA)
- Data (Access and Use) Act 2025.

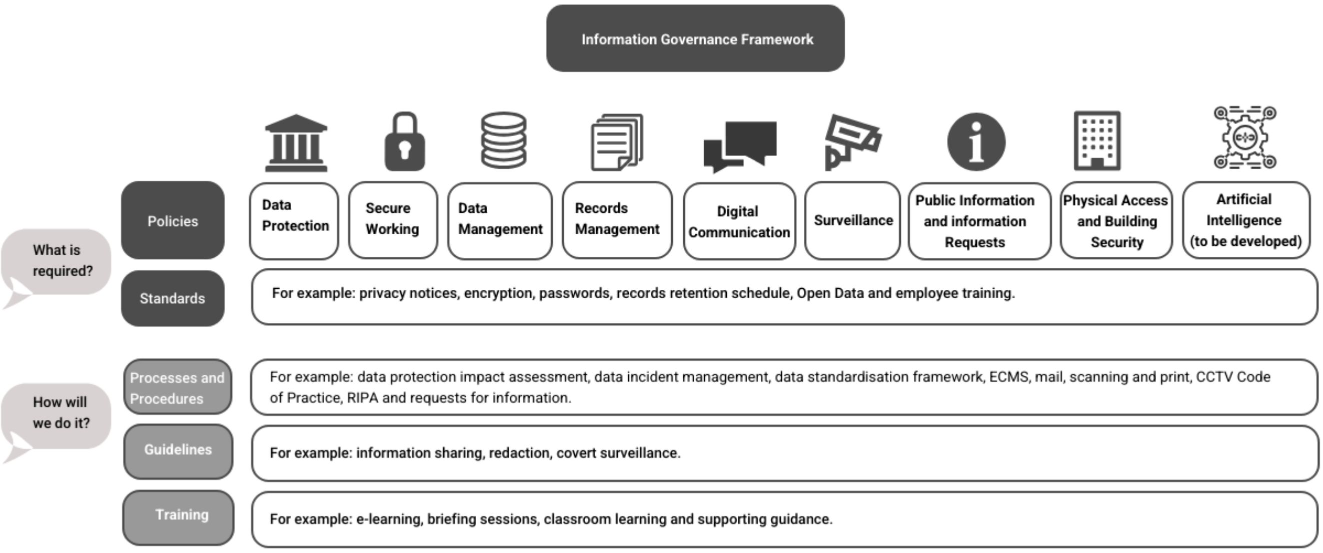
3.2 The Council's activity in this area is largely regulated by the Information Commissioner's Office (ICO), with the Investigatory Powers Commissioner's Office (IPCO) acting as the regulatory body for RIPA and compliance with the Surveillance Camera Code of Practice and the relevant provisions of PoFA encouraged by the Biometrics and Surveillance Camera Commissioner.

3.3 The Head of Governance, Policy and Information acts as the Council's Senior Information Risk Owner (SIRO) and as Senior Responsible Officer (SRO) for Biometrics and Surveillance and RIPA, and is the owner of the Council's Information Strategy. The SIRO advises the Chief Executive and the Council's management team on information risk, reporting quarterly to the internal risk management group and annually to the Leadership Management Team and to this Committee.

3.4 The Council has in place an Information Governance Framework (IGF) to ensure appropriate governance arrangements are in place and policies have been regularly refreshed prior to their set expiry dates. Since the last SIRO report to this committee the following policies were refreshed:

- Surveillance Policy
- 365 Policy
- Public Information and Information Requests Policy
- Records Management Policy.

3.5 Over the next 12 months the Council will adopt an Artificial Intelligence Policy to ensure it has appropriate governance in place for its lawful use. The diagram below, sets out the Council's Information Governance policy framework.



Information Governance Framework

What is required?

Policies: Data Protection; Secure Working; Data Management; Records Management; Digital Communication; Surveillance; Public Information and information Requests; Physical Access and Building Security; Artificial Intelligence (to be developed)

Standards: For example: privacy notices, encryption, passwords, records retention schedule, Open Data and employee training.

How will we do it?

Processes and Procedures: For example: data protection impact assessment, data incident management, data standardisation framework, ECMS, mail, scanning and print, CCTV Code of Practice, RIPA and requests for information.

Guidelines: For example: information sharing, redaction, covert surveillance.

Training: For example: e-learning, briefing sessions, classroom learning and supporting guidance.

The Information Strategy

3.6 In 2025 the Council refreshed its Information Strategy. The purpose of the Strategy is to ensure that the Council continues to adhere to good practice in relation to information governance and ensures that its approach to information governance adapts and reflects to a moving policy and technical landscape.

3.7 The Strategy has refreshed the assessment of the health of Council data, identifying priorities and key actions grouped around three themes to ensure:

- Good data management
- Ethical use and reuse of data
- Data can be used to transform services.

3.8 The Strategy sets out a vision for information which is that:

> ‘the right information will be available to the right users, at any time, accessible and used ethically to support achievement of the Council Plan’.

3.9 The Strategy will enhance transparency and accountability, allowing the Council to make informed decisions and build trust with the public. Furthermore, it will support economic development, optimise resource allocation, and promote innovation, driving sustainable growth and improving the quality of life for all residents.

3.10 The Information Strategy group will oversee deliver of the plan. The group is chaired by the SIRO and includes the Deputy SIRO, Data Protection Officer, Data and Analytics Manager, the Head of ICT and Digital, a HR Business Partner, the Single Point Of Contact (SPOC) for CCTV and will also include the strategic lead for Transformation once they are appointed.

Data Protection

3.11 The bulk of data protection work continues to be around data breaches/incidents and rights requests complaints, in line with the priorities of the Data Protection Officer and as set out in UK GDPR. Other data protection activity during 2024 has involved supporting the Council’s transformation programme, input to the Information Strategy, compliance audits in CCTV and surveillance, heavy involvement in procurement checks and contracts, and development of data protection impact assessment approaches to govern safe and lawful use of Artificial Intelligence applications.

3.12 By the end of 2024, mandatory training compliance had increased to 92% and there is an ongoing upward trend in compliance with this. The only Council directorate that met the 95% target was Adult Social Care and Health Integration (ASCHI). It should be noted that completion rates as of July 2025 have increased further. However, individual directorates, except ASCHI, have not yet met the challenging 95% target. Steps to ensure staff members understand their individual responsibilities for training completions are being taken in 2025.

Information Security

3.13 The UK Government regularly conducts cyber breaches surveys. The 2025 survey identified that there continues to be a high level of attempted or actual cyber security breaches, with 43% of companies and 30% of charities responding to the survey to say they had had an attack or a breach. Medium and large business continue to be a significant target with 67% and 74% reporting that they had had cyber security attacks.

3.14 As well as safeguarding systems the Council directly owns, it takes steps to ensure its suppliers are also safeguarding their data with appropriate measures. The robust approach to legally required compliance checks and contracts with suppliers and others continues to protect the Council from potential significant financial, regulatory, and other legal risks within its supply chain.

3.15 The table below summarises the number of personal data breaches and ICT/other security incidents (those involved lost or stolen ICT hardware or physical building security incidents).

Reporting by Year	Personal data breaches	ICT/other security incidents
2022	80	19
2023	94	20
2024	93	38

3.16 Reported personal data breaches have decreased slightly on the previous year, while ICT/other security incidents have increased as a result of cyberattacks and improved reporting of lost identity badges and access fobs. Investigations are undertaken into every report to identify any areas of concern and appropriate actions taken, up to and including disciplinary action if appropriate, to mitigate any unacceptable levels of risk.

3.17 Three personal data breaches were reported to the ICO in 2024 for the following reasons:

- Disclosure of the address of a vulnerable client
- Disclosure of contact details of businesses by a supplier
- Unauthorised access and disclosure information to a 3rd party.

3.18 Key measures that the ICO considered when assessing these breaches were the existence, and completion, of training relevant to the breach and the existing of processes that, if they had been followed, would have avoided the breach occurring.

3.19 Following investigation, the ICO took no further action on these incidents having been satisfied that the breaches were contained and the risk to individuals mitigated appropriately and that the actions were attributable to human error or deliberate action by an individual, due to the existence of robust controls already in place, or due to unauthorised actions of specific staff members which were addressed with disciplinary investigation/action.

Cyber Security

3.20 In early November 2024, the Council's website experienced two separate Distributed Denial of Service (DDoS) attacks. These incidents overwhelmed the server, making the website temporarily unavailable. Following these attacks, internal discussions were conducted to explore options for enhancing protection against future threats.

After a third attack in early December 2024, a decision was made to implement a mitigation solution, which was deployed in late December 2024. Since then, there have been no further outages, and the solution has consistently identified and blocked potentially harmful traffic.

3.21 In January, the Council entered into a Cyber Incident Response (CIR) retainer agreement. This agreement provides expert support for any cyber incident. If an incident occurs, the CIR can be activated for immediate assistance with investigation, containment, and resolution.

3.22 In light of increasing global threat levels, the Council remains committed to a robust cyber security strategy. Throughout the year, no systems, services, or information, whether stored on-site or in the Cloud were compromised. Furthermore, all hardware and software continue to receive the necessary support, updates, and patches in accordance with the Council’s policies.

3.23 In late May 2025, the Council implemented a policy that restricted staff access to browser-based artificial intelligence (AI) websites. This decision was made to minimise the risk of sensitive Middlesbrough Council data being inadvertently shared with large language models (LLMs), which could potentially expose that information to external parties.

3.24 To ensure data security while still promoting productivity with AI, the Council approved access only to Microsoft Copilot Chat. This platform operates within a secure environment, ensuring that organisational data remains protected.

3.25 An annual test of the ICT Disaster Recovery Plan for the data centres was successfully completed. No additional technical recommendations emerged from the test, and the annual maintenance schedule for critical infrastructure components was carried out without any issues.

3.26 The Council maintains the highest possible email domain security rating, which is assessed by the Northeast WARP (Warning Advice and Reporting Point) group.

3.27 In early April 2025, the Council approved a three-year strategy focused on Cyber Security Training. This initiative is designed to enhance staff understanding and skills to effectively identify and respond to current cyber threats. The primary goal is to inform and educate Middlesbrough Council staff who use its ICT systems about potential malicious activities that could threaten the Council’s ability to provide essential services. The progress of this strategy will be tracked on a monthly basis by the ICT team, with comprehensive updates provided annually to both the Audit Committee and the Leadership Management Team (LMT) as part of future SIRO reports.

3.28 The Council successfully retained its annual Public Services Network (PSN) compliance, confirmed in May 2025.

3.29 In December 2024, ICT Services successfully completed the Get Cyber Assessment Framework (CAF) readiness programme. This voluntary government initiative allowed the Council to evaluate its cyber security posture against recognised industry standards. The completion of this programme resulted in a grant award of £15,000. Additional phases of the optional CAF program are expected to be introduced as the government aims to broaden its reach and impact.

3.30 The Local Government Association (LGA) hosted an exercise in Fountain Court to assess ICT's response to a cyber incident. Their feedback was that "The team's response to the ransomware scenario was thoughtful, engaged and positive across the board. As is not unusual, the exercise identified areas for improvement in terms of preparedness and planning". Most of those improvements have now been put in place, with one outstanding, which is still being considered.

3.31 In June 2025, ICT suffered a network outage as a result of a failure of one of the core switches in the data centre. Usually, this on its own wouldn't have caused an outage, but unfortunately, it highlighted another problem, which ICT was previously unaware of, of a break in the fibre connection between the data centres. The faulty part in the switch was replaced under warranty however, the switches are nearing the end of life and are due to be replaced with new hardware by the end of September 2025. The fault with the fibre was identified as being malicious and is currently being repaired, which will be completed by mid-September.

3.32 Early in 2025 Veritau carried out an audit looking at Server Administration and Security. The audit gained the highest mark of Substantial assurance. The following was the conclusion from the audit - "*A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance."*

Records Management

3.33 There is ongoing activity to review and remove physical records in line with the corporate retention schedule, something that is in place to ensure the Council retains records for the legally permissible time. The Council continues to assess records for digitising where there is a business case to do so. Physical storage has been significantly reduced with further annual disposals and utilising off site storage for Council Planning records. These are now held in secure storage and scanned on demand should the service need to retrieve them, this enables further digitisation which improves accessibility.

3.34 A major focus of record management in the last year has been the ongoing implementation of SharePoint and transition of data from legacy systems and shared drives. This is ongoing with more services onboarding, reducing the overall volume of shared drives and redundant data held, further roll out of good practice guidance continues to further embed records management across the Council. Implementation of SharePoint will provide the council with a platform that has access and version controls while also providing opportunities for collaborative working.

3.35 The Covid-19 inquiry is still ongoing, and the Council continue to hold information in relation to practice at that time. Some of the information held has gone beyond its retention as stated in the Council retention schedule, however in line with the inquiry requirements, this information will be retained until we are advised otherwise.

Surveillance Policy

3.36 The Council continues to operate a Surveillance Policy which sets out how and when surveillance will be authorised, conducted, reviewed and reported. There is a training module in place to ensure compliance with this process. In 2025 this was made mandatory training for all Heads of Service. This step supports action to ensure key staff understand their responsibilities have awareness of the policy and the differences between the RIPA and non-RIPA process. The Surveillance policy was reviewed in December 2024 by the Mayor and Executive Member for Governance. The next review will be undertaken in December 2025.

3.37 A central log for all RIPA and non-RIPA requests is maintained and the detail is reported annually in the Surveillance Policy as listed in the background papers. This data is regularly scrutinised by the Council's Place scrutiny panel. The Panel last scrutinised this data at a meeting on 27 January 2025.

Public Information and Information Requests

Subject Access Requests

3.38 In 2024, 182 individuals made subject access requests for the data held about them by the Council. 20 of those requests were for data held in more than one service area, meaning the number of actual responses provided totalled 201 and of those 115 involved service areas in Children's Services.

3.39 Only 51 service area responses were overdue and 13 of those were greater than 7 calendar days overdue. The reasons for those delays were due to the complexity of the requests, which required reviewing handwritten data involving multiple third parties, combined with staff shortages.

3.40 The Council's compliance rate for 2024/2025 is 72%. Requests have increased for Children's Services by 35% for 2024-2025 which has placed significant pressure of the team completing these requests, as a result the capacity of the team has been expanded and recruitment to an additional post is underway. This will enable improved compliance in this area.

Freedom of Information and Environmental Information Regulations (FOI and EIR)

The following table summarises statutory information requests received by the Council over the previous two years.

Request Type	**2023**	**2024**	**% answered in time 2023**	**% answered in time 2024**	**Volume trend**
FOIA requests	1295	1469	88.6%	76%	⇧
EIR requests	70	77	85.7%	73%	⇧
Appeals (FOIA and EIR)					
Requests to review initial responses	20	30	100%	67%	⇧
Appeals to the ICO	0	3	100%	100%	⇧
% Appeals upheld in MBC's favour	60%	100%	N/A	N/A	⇧

3.41 Requests under the Freedom of Information Act 2000 increased in volume by 13.4% during the 2024 and Environmental Information Requests have increased by 10%, compared to 2023.

3.42 Performance reporting shows an increase in volume trend for FOI/EIR requests, Internal Reviews and ICO Complaints. The Council received several complex information requests regarding projects and associated political decisions. The delay in responding to information requests and requests to review initial responses is due to the increase in volume trend, the complexity of many of the requests and capacity of services to provide a response. Where there are trends in data requests, the Council continues to look to publish popular datasets in order to manage demand and reduce the need for the public to use the FOI/ EIR process. The Council publishes a range of datasets on its open data website. Information on compliance with these statutory processes is shared with Departmental Management Teams on a monthly basis and with Leadership Management Team on a quarterly basis.

Physical Access and Building Security

3.43 The Council has a range of policies and procedures in place which manage building security and access to Council sites, along with a building manager model. Responsibility for physical access and building security sits with the Head of Growth and Assets within the Regeneration Directorate.

3.44 There is a Physical Access and Building Security Policy in place which sets out roles and responsibilities.

3.45 The Council's Health and Safety and Data Protection Teams continue to undertake audits of Council buildings which includes testing of physical access policies and controls. In 2024 the team completed assessments of key building access risks which have been provided to Property Services to reflect within their access arrangements.

Priorities, Risks and Opportunities for 2025

3.46 The key priority during 2025 was to review the Information Strategy to ensure that the operational aims of it align with the Council Plan. Work is now underway to finalise a detailed delivery plan for the Strategy.

3.47 The second priority of the organisation will be the completion of the transition to SharePoint which has continued into 2025. SharePoint will transform how the Council stores, shares and uses data on a day-to-day basis. Information governance considerations were embedded within the scope of the project to ensure that the benefits of SharePoint are maximised while ensuring a robust approach to information governance and security.

3.48 Following Royal Assent on 19 June 2025 to the Data (Access and Use) Act 2025, work will continue to assess the impact and opportunities this new legislation presents and make the necessary adjustments to the Information Governance Framework. Features of the new Act include minor amendments to UK GDPR and PECR, creation of Digital Identity Verification provider frameworks, updates to digital records in Registrars services, and creation of a National Underground Assets Register.

4. Other potential alternative(s) and why these have not been recommended

4.1 Consideration of this report supports the Committee in discharging its responsibilities in relation to corporate governance, which includes information governance.

5. Impact(s) of the recommended decision(s)

Topic	Impact
Financial (including procurement and Social Value)	There are no new direct financial considerations in relation to the topics covered in this report.
Legal	Information Governance is governed by UK legislation, regulation, statutory guidance and case law. This report sets out, at a high level, measures that the Council is taking and plans to take in order to ensure ongoing compliance with this legal framework.
Risk	Improved information governance will ensure good risk management. Continued action in this area will positively impact on the risk within the Strategic Risk Register: • SR-09 - If the Council's **Corporate Governance arrangements are not fit for purpose and appropriate action is not taken to rectify this at pace**, this could result, censure from the Council's auditors within a public interest report that would damage the Council's reputation and/or in government formal intervention including removal of powers from officers and members and direction of council spend.
Human Rights, Public Sector Equality Duty and Community Cohesion	Not applicable – this report is for information only, however good data management will have a positive impact on the Council's ability to understand the potential impact of its decision making on these areas.
Reducing Poverty	
Climate Change / Environmental	

Children and Young People Cared for by the Authority and Care Leavers	
Data Protection	There are no data protection implications about this specific report for information.

Appendices

None.

Background papers

Body	Report title	Date
Corporate Audit and Affairs Committee	Annual Report of the SIRO	08/02/2018 07/02/2019 06/02/2020 21/04/2021 17/03/2022 16/03/2023
Audit committee	Annual Report of the SIRO	25 July 2025
Individual Executive Member – The Mayor	Surveillance Policy	17 December 2024

Contact: Ann-Marie Johnstone, Head of Governance, Policy and Information
Email: ann-marie_johnstone@middlesbrough.gov.uk