MIDDLESBROUGH COUNCIL	Middlesbrough moving forward

Report of:	Head of Governance, Policy and Information
Submitted to:	Audit Committee
Date:	25 July 2024
Title:	Annual Report of the Senior Information Risk Owner (SIRO)
Report for:	Information
Status:	Public
Council Plan priority:	Delivering Value for Money
Key decision:	Not applicable
Why:	Not applicable
Subject to call in?:	Not applicable
Why:	Not applicable

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 and 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 2023 calendar year, risks and issues arising, and priorities for 2024. 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.

1. Purpose

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 2023 calendar year, risks and issues arising, and priorities for 2024/5.

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 and 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. Rationale for the recommended decision(s)

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

4. Background and relevant information

The Information Governance Framework

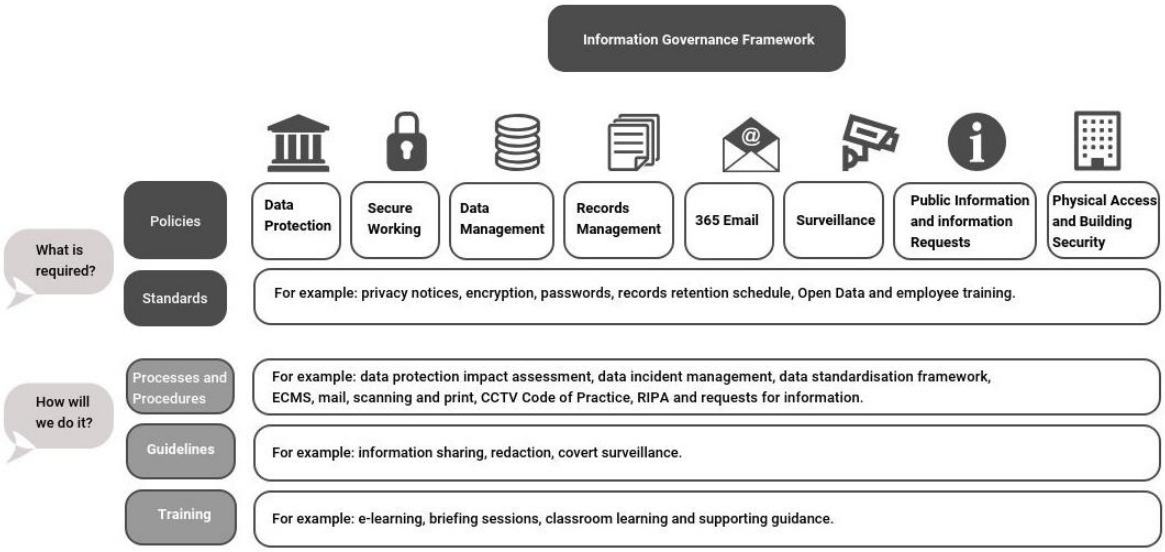
4.1 The Council must create, protect, manage, share and disclose information in line with a complex legal framework. This report deals principally with information governance arrangements relating to the following, and the risks arising from:

- 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); and
- Protection of Freedoms Act 2012 (PoFA).

4.2 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.

4.3 The Head of Governance, Policy and Information acts as the Council's Senior Information Risk Owner (SIRO) / 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.

4.4 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. The diagram below, sets out the current content of the Council's Information Governance policy framework.



The Information Strategy

4.5 In 2023 the Leadership Management Team requested an options appraisal on the potential to combine a number of Council business strategies into a single Operations Strategy. One outcome of that assessment was a decision that the Information Strategy should remain separate and be refreshed in 2024. Action is underway to refresh this strategy in 2024 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.

4.6 The 2024 refresh will focus on refreshing the assessment of the health of Council data, identifying improvement transformation required to enable the Council's delivery of transformation activity, refreshing the information governance policy framework to reflect emerging opportunities and risk, for example, opportunities around use of artificial intelligence and policy safeguards that will need to be put in place.

Data Protection

4.7 A focus for data protection work continues to be around incidents and rights requests. Other data protection activity over 2023 has involved cyclical reviews and updates to information sharing agreements and privacy notices.

4.8 Mandatory training compliance has declined to 91% with areas for improvement identified in Children's Services, partly due to staff turn-over, and Regeneration Services, where plans for alternative training approaches for large groups of casual staff in cultural and creative services are being developed.

4.9 The final 2 out of 63 recommendations from the 2020 Information Commissioner's Officer (ICO) consensual audit of the Council were implemented. Analysis of ICO published statistics for receipt of *any* complaints and concerns up to June 2023, showed Middlesbrough Council ranked 115th equal out of 118. Within 2023 there were no complaints or breaches referred to the Council by the ICO and of the 4 reports made to the ICO about the Council, all were closed with no further action.

Information Security

4.10 The UK Government cyber breaches survey reported in early 2023 found that 32% of businesses and 24% of charities overall reported breaches or attacks from the last 12 months with that figure increasing to 69% for large businesses. 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 our supply chain.

4.11 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
2021	100	8
2022	80	19
2023	94	20

4.12 Reported personal data breaches have increased slightly on the previous year, while ICT/other security incidents have remained in line with the number reported in the previous year but have changed in nature with the addition of lost/stolen identity badges and access fobs as a reportable category. 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.

4.13 Six personal data breaches were reported to the ICO in 2023 for the following reasons:

- Unauthorised access to records by staff member
- Prosecution legal bundle sent to wrong address
- Disclosure of identity of person who reported a safeguarding concern
- Manager disclosed health data about an employee to their colleague
- Sub-contractor of a supplier suffered a cyber-attack
- Disclosure of identity of service user to another family

4.14 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.

4.15 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, 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

4.16 Ransomware and state-sponsored attacks continue to dominate the threat landscape and in response, all services that the Council hosts internally i.e. within its data centres, for either residents or staff have now been restricted to only be accessible from the United Kingdom. There are however a small number of public facing services (such as the Council's website) that are exempt, where access is allowed from anywhere, other than 16 countries that are classed as high-risk, from which all internet traffic is blocked.

4.17 Within the context of rising threat levels globally, the Council continues to maintain a strong cyber security stance. No systems, services, or information (whether on premises or in the Cloud) were compromised during the year and all hardware and software continues to be supported, updated, and patched, in-line with the Council's policies.

4.18 All Council staff that have access to corporate devices have now been onboarded into the Microsoft 365 platform and enrolled for Multi-Factor Authentication, which enhances Microsoft's 'Conditional Access' service to require additional authentication when staff are using an unmanaged (personal) device. This is now enabling staff to realise the benefits and convenience of BYOD (Bring Your Own Device) to access cloud services, as these security enhancements have also allowed us to externally publish our new intranet site (hosted on SharePoint) and E-mail for all staff, without any fear of compromise or data leakage.

4.19 In November 2023, the annual test of the ICT Disaster Recovery Plan for its data centres was successfully completed. No additional technical recommendations were noted as a result of the test and the annual maintenance schedule for critical infrastructure components was completed without issue.

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

4.21 A Cyber Security Training Strategy is in development which will ensure that staff are educated appropriately regarding modern cyber threats and their associated risks and options for mitigation.

4.22 The Council successfully retained its annual Public Services Network (PSN) compliance, confirmed in May 2024.

4.23 After further exploration of the ISO27001 accreditation, which is a set of standards for organisations that host services and store data for other organisations, which Middlesbrough Council does not, it would not be appropriate. ICT Services will however undertake the government's new self-assessment programme, CAF (Cyber Assessment Framework) towards the end of 2024, which aims to compare our cyber security against industry standards.

4.24 The Local Government Association (LGA) has been invited to conduct a cyber security exercise in June 2024 to test our business continuity and disaster recovery plans. The aim of this work is to provide assurance about the reported risk controls that are in

place to safeguard the Council's ICT infrastructure, systems, applications, data and will assess our response. The exercise will involve a phishing campaign and a theoretical scenario locking staff out of business functions for service user payments. The LGA provide a report to the Council on areas of weaknesses and strengths together with recommendations for business continuity and ICT functional improvements.

Records Management

4.25 The Council continues to actively review its physical records and the storage and management options for them. The relocation of Council services to Fountain Court provided an opportunity in 2022 to further digitise records. The Council continues to assess records for digitising where there is a business case to do so. The advantage of digitised records is that their accessibility is increased and there is a reduced amount of physical storage space required. This is assessed against the costs of digitising.

4.26 Officers from ICT and Information Governance are working collaboratively to ensure good records management practice is embedded within the project to move to Microsoft SharePoint.

4.27 The team continue to complete ad hoc data audits where necessary to improve practice. One audit was completed during 2022 and all actions have been implemented as a result.

4.28 From time to time the Council will receive a direction to hold documentation for longer than the planned retention schedule, to support a national inquiry. Since this was last reported to the Committee, the requirement to retain documentation in relation to the Independent Inquiry Child Sexual Abuse (IICSA) has been ceased. During 2022 all councils received a direction to retain certain documentation in relation to Covid-19 by the UK Covid-19 inquiry.

Surveillance Policy

4.29 The Council continues to operate an integrated Surveillance Policy which sets out how and when surveillance would be authorised, conducted, reviewed and reported. During 2023 a priority for the team was to further develop training in relation to surveillance to ensure that key staff understand when they are likely to undertake an action which should be assessed using this policy and the differences between RIPA and non-RIPA processes. In line with best practice, the policy was reviewed in December 2023 by the Executive Member for Finance and Governance. The next review will be undertaken in December 2024.

Public Information and Information Requests

Subject Access Requests

4.30 In 2023, 102 individuals made subject access requests for the data held about them by the Council. 17 of those requests were for data held in more than one service area, meaning the number of actual responses provided totalled 128 and of those two thirds involved service areas in Children's Services.

4.31 Only 12 service area responses were overdue and only 2 of those were greater than 7 calendar days overdue. The reasons for those delays included problems with engagement from the requestor to enable provision of the response in an appropriate and safe manner and delays due to the legal requirement to consult the external "appropriate health professional" prior to disclosure of medical information held by the Council.

4.32 Overall, this represents a sustained improvement in the Council's compliance with data protection laws around transparency and access to data in 2023, compared to performance in 2019 where only 42% of SAR responses were "in time".

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	**2022**	**2023**	**% in time 2023**	**Volume trend**
Freedom of Information Act 2000 (FOIA)				
FOIA requests	1266	1295	88.6%	⇧
Environmental Information Regulations 2004 (EIR)				
EIR requests	94	70	85.7%	⇩
Appeals (FOIA and EIR)				
Requests to review initial responses	25	20	100%	⇧
Appeals to the ICO	3	0	100%	⇩
% Appeals upheld in MBC's favour	60%	60%	N/A	N/A

Requests under the Freedom of Information Act 2000 increased in volume by 2.29% during the 2023, compared to 2022. Performance reporting shows an increase in FOI/EIR compliance with timescales. The Council received a number of complex information requests regarding key programmes and projects and associated political decisions. 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.

Physical Access and Building Security

4.33 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. Following a spate of incidents, recommendations have been made about changes to building security measures and practices. Subject to the outcomes of any wider building asset portfolio decisions, further recommendations may be forthcoming. The Council's Health and Safety and Data Protection Teams continue to undertake audits of other buildings which includes testing of physical access policies and controls.

Priorities Risks and Opportunities for 2024

4.34 The key priority during 2024 will be to review the Information Strategy to ensure that the operational aims of the Council align with the Strategic vision set by Members and the organisations direction of travel, in particular in relation to the work on-going around budget and governance.

4.35 That work has already started, and the Information Strategy is in the process of being re-built around the public sector 'Information Principles' – that information is a valued asset, managed, fit for purpose, standardised and linkable, reused, published, and that citizens and businesses can access information about themselves.

4.36 The second priority of the organisation will be the successful delivery of transition to SharePoint. As set out above, SharePoint will transform how the Council stores, shares and uses data on a day-to-day basis. Information governance considerations are 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.

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

5.1 Not applicable – this report is for information only.

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

6.1 Financial (including procurement and Social Value)

There are no new direct financial considerations in relation to the topics covered in this report.

6.2 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.

6.1 *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.

6.2 *Human Rights, Public Sector Equality Duty and Community Cohesion*

Not applicable – this report is for information only.

6.3 *Climate Change / Environmental*

Not applicable – this report is for information only.

6.6 Children and Young People Cared for by the Authority and Care Leavers

Good information governance has a direct impact on the quality of services provided by the Council and the safety and security of vulnerable children.

6.7 Data Protection

There are no data protection implications about this specific report for information.

Actions to be taken to implement the recommended decision(s)

Not applicable, as the report advises the Committee and seeks comment. The activity outlined in the main body of the report will ensure good governance relation to information governance.

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

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