MIDDLESBROUGH COUNCIL	Middlesbrough moving forward

Report of:	Interim Head of Governance Policy and Information
Submitted to:	Corporate Affairs and Audit Committee
Date:	16 March 2023
Title:	Annual Report of the Senior Information Risk Owner (SIRO)
Report for:	Information
Status:	Public
Strategic priority:	All
Key decision:	Not applicable
Why:	Report is for information only
Urgent:	No
Why:	N/A

Executive summary

This report sets out arrangements in place to ensure the proper governance of information within the Council, progress made within the 2022 calendar year, risks and issues arising, and priorities for 2023.

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.

Purpose

1. To advise the Corporate Affairs and Audit Committee of arrangements in place to ensure the proper governance of information within the Council, progress made within the 2022 calendar year, risks and issues arising, and priorities for 2023.

Background and relevant information

Report background

2. 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).

3. 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. The Interim 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 Leadership Team and to this Committee.

Compliance, issues and risks in 2022

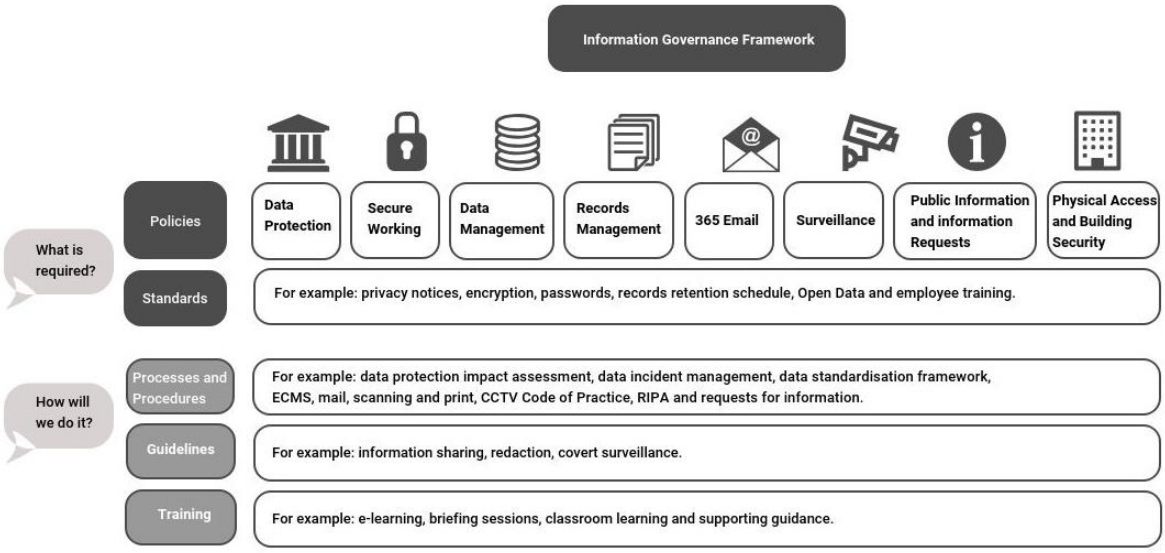
ICO consensual audit

5. In 2019 and 2020 the Council invited the Information Commissioner's Office (ICO) to undertake a consensual audit of its data protection arrangements which provided a 'reasonable' level of assurance (the second highest of the ICO's ratings, behind 'high').

6. Only 2 of the original 63 recommendations remain open which relate to standard user profiles and access rights audits across the 150 electronic systems identified in the Council's applications portfolio. Following a period of procedural development, these actions will be implemented in 2023/24 via the Council's new Information Asset Owner (Heads of Service) Handbook approach.

Information Governance Framework

7. The Council has in place an Information Governance Framework (IGF) to ensure appropriate governance arrangements are in place.



Statutory information requests

8. To improve effectiveness and timeliness against our statutory responsibilities for information requests the Council have increased the capacity of the corporate team and enhanced support to services, to enable a greater focus on compliance with requests in time. The team also use the new capabilities available to them to gather information pre-emptively available to speed up requests, including within the Microsoft 365-environment using the e-discovery capabilities.

9. Children's Services subject access requests (SARs) performance has significantly improved. Investment, including use of external resources has been used to significantly improve compliance. Overall, with 50 out of 59 requests in the last 12 months being completed within time. While 9 exceeded the statutory timescales, the number of days by which they exceeded these timescales was significantly reduced compared to previous years. The Children's Services directorate has mainstreamed a post that has proven will ensure the long-term efficacy of SAR responses.

10. Performance reporting also shows an increase in FOI/EIR compliance:

Reporting	No of FOI requests	% in time
Q2 2022	173	84%
Q3 2022	215	86%

Physical access

11. 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. During 2022 the Council's main office space was moved from the Civic Centre to Fountain Court. One of the key aspects of this move was ensuring that physical access security was embedded within the design and that the supporting model also

reflected the changes to the way most office-based staff are now working. During 2023 work is ongoing to refine this approach.

Surveillance policy

12. 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 will be 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. In line with best practice, the policy was reviewed in December 2022 by the Executive Member for Finance and Governance. The next review will be undertaken in December 2023.

Information Strategy

13. In November 2018, LMT agreed an Information Strategy for the Council for the period 2018-2022. The strategy vision is that the right information will be available to the right users, at any time, accessible from anywhere, underpinning the achievement of the Council's strategic objectives. That strategy has now lapsed. During 2023 a refreshed approach to Information Strategy will be developed alongside the refresh of the Strategic Plan to ensure the operational aims of the Council align with the Strategic vision set by Members.

Information asset registers

14. The Council's information asset registers were significantly developed in previous years and reviewed/consolidated with UK GDPR 'Records of Processing Activity' in 2019/20. Various in-year updates by individual Information Asset Owners will need to be merged with changes as a result of the Council's accommodation strategy, bulk transfer of records to digital formats, procurement of electronic systems – including the SharePoint Online migration (see below) and decommissioning of others.

Information security

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 incident).

16. Reported personal data breaches have decreased by 20% on the previous year, while ICT/other security incidents have increased, largely owing to more reports of lost or stolen ICT hardware devices. Investigations were undertaken into every report to identify any areas of concern. It was clear from those investigations that blended working is not a factor in these incidents. The risk of data loss, because of loss or theft is significantly reduced by ICT safety measures in place. All devices are encrypted by default, the Council has the capacity to remotely delete content and bar devices. The Council also has strong password or PIN protections in place and voluntary facial recognition on newer laptops has further improved device security and access.

17. Only two personal data breaches were reported to the ICO in 2022. One incident involved the theft of ICT hardware and paperwork from a staff member's home and a second was for the disclosure of a child's care placement address. The ICO reviewed

both incidents and was satisfied with the Council's proactive containment and response and decided to take no further action.

Reporting by Year	Personal data breaches	ICT/other security incidents
2021	100	8
2022	80	19

Cyber security

18. Ransomware and state-sponsored attacks continue to dominate the threat landscape and in response, the Council now has a list of 16 countries from which internet traffic is blocked. Over the next year the Council's geo-location posture will be further enhanced through an exercise which will define connections with countries, aligned to provision of a specific service.

19. 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.

20. As part of the Council's adoption of Microsoft 365 services, 'Conditional Access' has been implemented, which enables the Council to dictate how, when, where and from what device, a user can connect to resources, alongside the conditions to be met when using email, Teams, OneDrive and soon, SharePoint.

21. Between July and August 2022, 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.

22. In May 2022, ICT Services implemented MTA-STS; a new email standard to improve trust and enforce the use of Transport Layer Security (TLS) for email, enabling the Council to maintain the highest possible email domain security rating, which is assessed by the North East WARP (Warning Advice and Reporting Point) group.

23. During 2022, the Council's internal auditor Veritau assessed controls in relation to firewall change control processes, determining a 'strong assurance' rating on the measures in place.

24. The Council successfully retained its annual Public Services Network (PSN) compliance, confirmed in November 2022.

25. Discussions with a qualified assessor from Northumberland Police are underway as to whether Middlesbrough Council would benefit from retaining Cyber Essentials accreditation in 2023. Such accreditation tends to be more suitable for smaller organisations, with reduced portfolio of applications and associated security requirements. As an alternative, consideration of the international standard for information security management, ISO 27001 is being explored.

Records management

26. 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.

27. 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.

28. 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.

29. 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.

Data protection

30. Other than the main focus around incidents and rights requests, the Council's data protection activity over 2022 has involved strengthening governance of mandatory training and internal guidance, transparency obligations, information sharing arrangements, compliance checks on contractors and others, and data protection impact assessments (DPIA).

31. Mandatory training compliance has improved with more directorates achieving and maintaining a rolling 95% of staff completions. The Council's suite of privacy notices has become more granular in line with ICO guidance and over 70 operational notices are now being maintained for individual services and thematic local authority functions.

32. A number of detailed agreements with a wide variety of partner organisations across various sectors, have been reviewed and updated or put in place to support lawful and ethical information sharing as part of normal service delivery.

33. Changes to streamline the DPIA process have ensured a balance is maintained between the efficiency of business management and the efficacy of risk controls. Similarly, the approach to legally required compliance checks and contracts with suppliers and others has been streamlined and diversified to make sure that checks are proportional and targeted where needed.

Priorities for 2023

34. The key priority during 2023 will be to refresh the Information Strategy of the Council. As referenced within the body of this report, the refresh is being timed to ensure that the new strategy reflects the refreshed strategic plan vision of the Council which will be delivered in 2023 to ensure the strategy aligns with that.

35. 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.

What decision(s) are being recommended?

36. That the Corporate Affairs and Audit Committee notes the position in respect of information risk set out in the report.

Rationale for the recommended decision(s)

37. To support the Committee in discharging its responsibilities in relation to corporate governance, which includes information governance.

Other potential decision(s) and why these have not been recommended

38. Not applicable.

Impact(s) of the recommended decision(s)

Legal

39. IG 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.

Strategic priorities and risks

40. Improved information governance will underpin the delivery of all strategic priorities and ensure good risk management.

Human Rights, Equality and Data Protection

41. Not applicable.

Financial

42. It is anticipated that all activity set out in this report is achievable within existing and planned budgets.

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

43. 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

No appendices.

Background papers

Body	Report title	Dates
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

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