MIDDLESBROUGH COUNCIL	Middlesbrough moving forward

AGENDA ITEM 12

Report of:	Head of Strategy, Information and Governance

Submitted to:	Corporate Audit and Affairs Committee, 6 February 2020

Subject:	Annual Report of the Senior Information Risk Owner (SIRO) - PART A

Summary

Proposed decision(s)
That the Committee notes the position in respect of information risk set out in the report, and proposes for consideration any further steps it may wish to see taken to promote good practice in information governance within the Council.

Report for:	**Key decision:**	**Confidential:**	**Is the report urgent?**
Information	No	No	No

Contribution to delivery of the 2020-23 Strategic Plan		
People	**Place**	**Business**
Improved information governance will underpin the delivery of all strategic priorities.	Improved information governance will underpin the delivery of all strategic priorities.	The activity outlined in the main body of the report will result in significant improvements in the Council's information governance arrangements.

Ward(s) affected
None.

What is the purpose of this report?

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 2019 calendar year, risks and issues arising, and priorities for the next 12 months.

Why does this report require a member decision?

2. 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.

Report background

3. 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 therefrom:

    - Data Protection Act 2018 (DPA);
    - EU General Data Protection Regulation 2016 (GDPR);
    - 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. 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 CCTV Code of Practice and the relevant provisions of PoFA encouraged by the Surveillance Camera Commissioner.

5. The Head of Strategy, Information and Governance acts as the Council's Senior Information Risk Owner (SIRO) / Senior Responsible Officer (SRO) for these issues, 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 CMT and to this Committee.

Compliance, issues and risks in 2019

Implementation of 2019 priorities

6. The last annual report to this Committee (7 February 2019) set out eight key priorities to reduce information risk for the 2019 calendar year and beyond. Good progress was made on these priorities during the year, as summarised at Appendix 1, with 14 remaining or resulting actions to be completed during 2020 as part of the Council's overall Information Strategy delivery plan.

ICO Consensual Audit

7. In July 2019, the ICO was invited to undertake an audit of the Council's data protection arrangements, looking specifically at three crosscutting domains:

- governance and accountability;
- security of personal data; and
- requests for personal data and data portability.

8. The Executive Summary of the ICO's report on the audit (which took place during November and December 2019) is at Appendix 2 and is also published on the ICO's website.

9. The audit rated the Council as providing a 'reasonable' level of assurance (the second highest behind 'high') that the Council's arrangements are delivering data protection compliance across all three domains. Sixty recommendations were made by the ICO to reduce the Council's risk of non-compliance – four with urgent priority, 37 high and 19 medium.

10. The main areas of improvement identified by the ICO related to physical access control, subject access requests, email security, and enhancing the role and accountability of senior managers on data protection matters. These, and the majority of recommendations made, were already known to the Council and reflected in its information risk register and Information Strategy delivery plan.

11. The Council has responded to the ICO with proposed actions to address its recommendations, and these have been accepted by the ICO as effective controls for the risks identified. The ICO will undertake a desktop follow-up audit in 6-12 months' time to confirm the actions have been implemented. If the Council fails to implement a recommendation and then has to report a breach to the ICO pertaining to that recommendation, then there is a high likelihood of sanctions.

12. By the date of this meeting of the Committee, 15 of 72 actions should have been delivered, including all actions in response to the ICO's urgent recommendations.

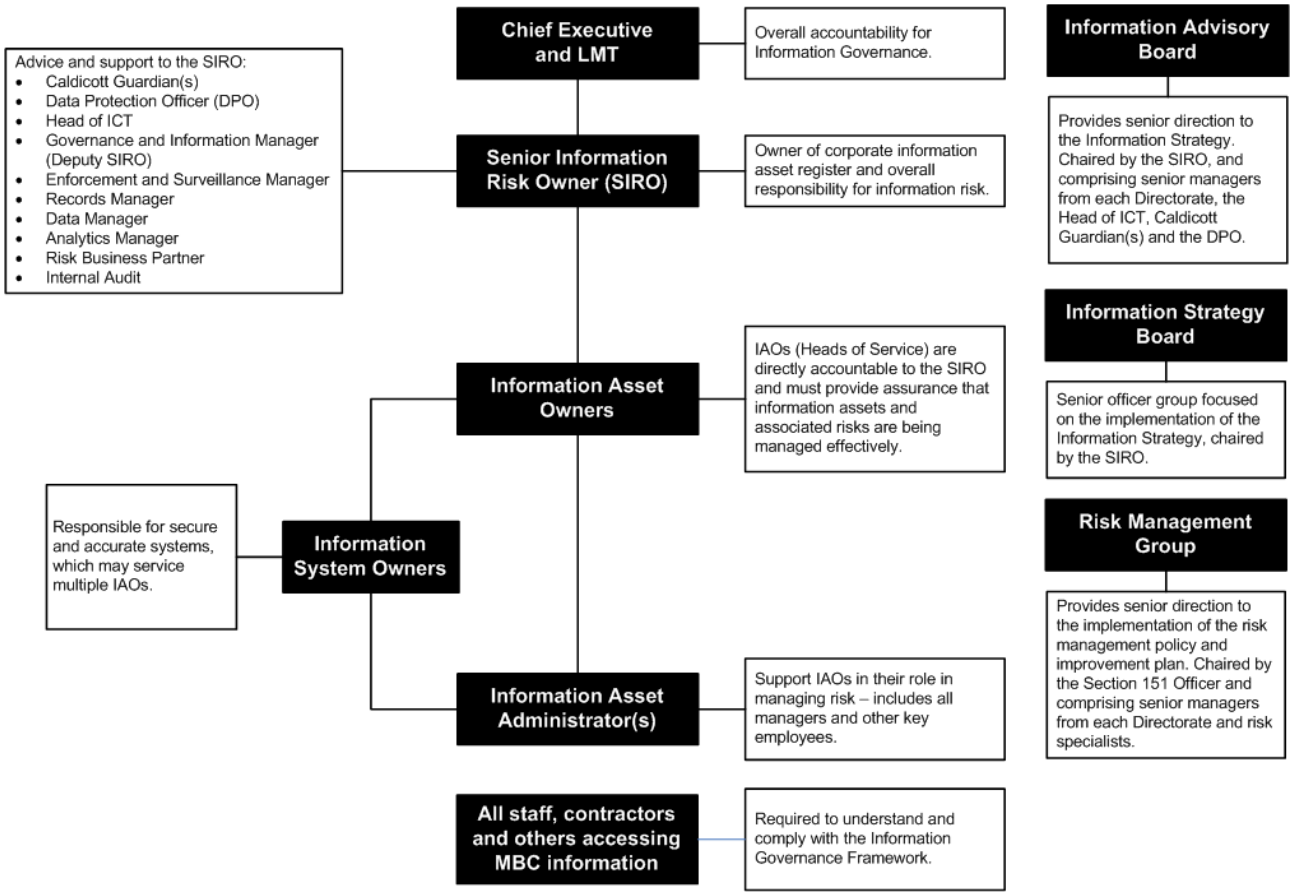
Information strategy progress

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*.

14. The strategy has three key themes:

- **Organise**: implement a streamlined and integrated information governance framework, responding to legislative changes, and providing a firm foundation for improvement;
- **Collaborate**: maximise the quality and the value of our information through joint-working, both internally, with our partners, and with our citizens and customers; and
- **Transform:** ensure that our information is improved in line with our strategic priorities, and used to support evidence-based approaches to strategy, policy and commissioning.

15. The strategy is implemented through governance arrangements consistent with the requirements of Data Handling Procedures in Government (2008) and the NHS Digital Data and Security Toolkit (with which the Council must comply to share data with the NHS):



16. In the first year of the strategy the Council focussed largely on the 'Organise' theme, updating and joining up its information governance framework (IGF). There are now eight policies within the IGF, with the following policies either created or reviewed and updated at the end of 2019:

- **Public Information and Requests Policy**: this sets out how the Council will proactively publish information, and will respond to statutory requests for recorded information, either held directly by the Council or by another organisation on behalf the Council. Its key focus is public awareness.
- **Data Protection Policy**: this sets out how the Council and its constituent data controllers will comply with data protection law and associated codes of practice and guidance. Its key focus is all staff compliance.
- **Records Management Policy**: this sets out how the Council will ensure good practice in records management across its operations, minimising paper records and shifting the majority of electronic records to its Enterprise Content Management System. Its key focus is all staff compliance.
- **Email Policy**: this sets out how the Council will ensure that its email system is operated in line with the principles of effective information governance. Its key focus is all staff compliance.
- **Data Management Policy**: this sets out how the Council will effectively standardise, manage, link and exploit data throughout its lifecycle, and ensure that it meets its obligations in respect of data integrity, statutory returns to Government, statutory information requests and data transparency. As such its key focus is specialist technical staff and all staff compliance.
- **RIPA Policy**: this sets out how the Council will use covert techniques to obtain private information about someone if they are suspected of criminal activity. Its key focus is all staff compliance.

17. The following policies will be reviewed and updated as required during 2020:

- **Information Security Policy**: this sets out how the Council will protect its data, hardware and software from accidental or deliberate misuse, damage or destruction. Its key focus is specialist technical staff and all staff compliance. The update will focus on integrating the policies and procedures issued in recent years relating to agile working and the use of personal devices for work.
- **CCTV Code of Practice**: this sets out how the Council will comply with the provision of PoFA 2012. The review will ensure a consistent approach is being operated across the Council's CCTV schemes.

18. The ICO audit made a number of recommendations relating to the IGF, relating largely to communications, training and monitoring. Once these are in implemented, the Council will relaunch the framework to managers and employees using its new business change framework. This will include enhanced communications and training and briefings more bespoke to specific roles within the framework, with a particular focus on Information Asset Owners. The Council's target is for 95% of all employees to have confirmed acceptance of the new framework and to have undertaken appropriate training.

Changes to information asset registers

19. Information asset registers (IARs) list all the information owned by services, digital and paper, quantifies these and sets out how they are managed across the lifecycle. In the Council, IARs are owned by Information Asset Owners (Heads of Service).

20. The Council's information strategy uses IARS to present an overall view of the fitness-for-purpose of information across service areas on a RAG basis, taking into account the following criteria:

- Security
- Confidentiality
- Accuracy
- Completeness
- Timeliness
- Relevance
- Reliability
- Validity
- Availability

21. This information map is reviewed on a quarterly basis by Information Strategy Board based on dialogue with Information Asset Owners. At the last review, the overall RAG was as set out below. There have been no major changes to IARs reported this year, and the position reflects ongoing improvements in the Council's information (movement from Red to Amber) and a greater understanding across services of what information is required for effective decision-making and delivery (movement from Green to Amber).

RAG	Definition	%	Change from last review
Red	Does not meet basic requirements	6.7%	-24%
Amber	Meets basic requirements but requires improvement	40.6%	+9%
Green	Fit for purpose	52.7%	-2%

22. IARs are currently being reconfigured into the management structure implemented in November 2019, and as part of the revised IGF, IAOs will be required to formally provide the SIRO with assurance on information assets and risks an annual basis using a standard template.

Information security

23. The Council continued to maintain a strong cyber security posture during 2019. No systems, services or information were compromised during the year, with all hardware and software continue to be updated and patched in line with the Council's policy, further reducing the risk of successful attack.

24. Work was undertaken during the year to ensure that ICT is notified in advance of starters / leavers / movers within the organisation, allowing them to amend access to systems in good time and reduce the risk of data breaches. Almost 1,000 access control changes were processed during 2019:

- 381 new starters (employees and agency staff) had access rights established;
- 68 movers had access rights updated; and
- 527 leavers had access rights removed.

25. A 100 user phishing exercise was conducted in March 2019 in which fake potentially malicious emails were sent to employees to test vulnerability to attack. No users exposed the Council to potential attack from this test, but it is important for employees to remain vigilant and aware of how they could be targeted in such scams.

26. Over 500 end-of-life devices were destroyed by the Council's contractor during 2019 with the appropriate destruction certificate supplied for all.

27. A number of important technical improvements were delivered during the year to enhance cyber security, including:

- GCSX mail was decommissioned in March 2019 following enhancements to the main Exchange email system. These improvements removed the need for multiple mailboxes, reduced costs and ensured that those receiving emails from middlesbrough.gov.uk can be confident that emails are genuine correspondence and not a third parties masking themselves as the Council;
- websites developed for the Council by third parties (e.g. LoveMiddlesbrough) were strengthened in line with recommendations derived from used of the NCSC Webcheck tool introduced in 2018;
- the Microsoft Windows 10 estate was upgraded from version 1803 to version 1909, and maintaining a best practice patching cycle for all applications; and
- the Council's firewalls were upgraded to the latest software version, enhancing both security and functionality.

28. In April 2019, the Council relocated one of its data centres from Melrose House to BOHO One. This allowed ICT to re-design some elements of the security infrastructure, improving network resilience and reducing operational costs. In September, the annual test of the ICT Disaster Recovery Plan for its data centres was successfully undertaken, and identified a number of improvements to be implemented to further enhance resilience.

29. During the year, the Council used an external CHECK-approved assessor as part of its annual Public Services Network (PSN) compliance audit. This highlighted some areas for improvement, which were addressed in-year and the Council retained its PSN compliance certificate in November 2019.

30. The Council continues to participate in the Local Government Association's (LGA's) Cyber Security Stocktake (now bi-annual), receiving an overall rating of 'Green' in 2018. The 2019 outcome and associated actions are awaited at the time of writing.

31. The ICO audit made a number of recommendations broadly relating to ICT, which will be implemented in 2020, including:

- establishing system access rights profiles to ensure consistency and proactively undertaking system access audits across the organisation;
- proactively undertaking retention audits to ensure that records are not held for longer than required by the Council's retention schedule (this also applies to physical records);
- changes to email to avoid breaches (e.g. removal of autocomplete, locking down access to group email) and to reduce duplication of records; and
- greater controls being applied to USB within the organisation to reduce the risk of breaches and the loss of unique records.

32. However, the most significant and urgent recommendation related to need to improve physical access controls within the Central Campus (though lessons need to be applied to all Council buildings). This relates primarily to improving controls at the front door, including a consistent approach to ID cards and lanyards for both employees and visitors and reception cover to reduce unauthorised access through tailgating, but also to such matters as clear desk policy and access granted to individuals to move around within buildings via the co-tag system. This risk score relating to this issue has therefore risen at the end of 2019, and a corporate project has now been launched to review this matter, which will report to CMT by the end of 2019/20.

Data protection

33. 2019 was the second year of the new GDPR which first came into force, together with the new DPA, at the end of May 2018.

34. During 2019 the Government legislated for the transfer of the GDPR into UK law and proposed amendments to existing legislation to effect changes from Brexit such as removal of the European Data Protection Board from the UK regulatory regime.

35. More immediate actions for the Council included taking account of changes in how the stringent EU rules protecting the international transfer of personal data will be applied after Brexit. When the UK leaves the EEA it will become a 'third country' for the purposes of EU data protection. In the year the Council completed an assessment of EU based ICT suppliers that cloud host its data. Based on advice from the Government and the ICO, this assessment found very low levels of risk to information flows back to the Council after Brexit.

36. One final matter relating to Brexit is the proposed EU ePrivacy Regulation which regulates issues including electronic direct marketing and certain website technical functions called 'cookies'. At present the new Regulation will not apply prior to the exit date. However, the Council will need to monitor the UK Government's response to the EU ePrivacy Regulation and may need to update its existing regulations to maintain any 'adequacy' and parity with EU law to avoid barriers, particularly to information flows.

37. Remaining data protection work has focussed on meeting the requirements of the Council's Data Protection Policy which was set in 2018 and mandated the approach to compliance with statutory requirements.

38. This has involved updating procedures and processes where existing requirements have been strengthened in law such as incident notification, transparency and, where applicable, consent requirements. Other new requirements have been well documented in detailed, accessible procedures and guidance issued to Council officers on matters including completion of the 'record of processing activity' which documents all personal data processing and the data protection impact assessment process which supports decisions on new, high-risk data processing.

39. No significant third party data processor issues were reported during 2019, and no residual high risks were accepted by the SIRO through the Council's data privacy impact assessment process.

40. Compliance with the rights of the data subject, such as subject access requests, remain a challenge in some service areas, which has been documented in the Council's strategic risk register, mitigations implemented, and the situation remains under close monitoring.

41. The immediate future focus of activities will include the next phase of training and development which will include a training refresh for all staff and specialist training for specific roles in areas of higher risk including subject access requests. Alongside this, communications work will be taken forward to ensure organisational and technical measures are understood and embedded. This work is considered to be critical to ensure that the downward trend in the severity of personal data breaches continues.

42. Members are reminded of the importance of balancing modest investment in these measures against the risk of legal non-compliance which, in the worst scenarios, can lead to significant harm to service users, regulatory action including fines of up to £17million, and significant reputational damage.

43. The Council is also in the second year of the refreshed NHS Data Security and Protection Toolkit, the health and social care information governance standard. This new self-assessment approach has largely reduced the evidential burden on the Council to prove compliance through large amounts of documentary evidence, it has focussed efforts on the National Data Guardian Standards.

Incident type	**2018**	**Reported to ICO**	**2019**	**% change in past year**	**Reported to ICO**	**% change in past year**
Disclosed in error	40	3	52	+40%	2	-33%
Lost or stolen hardware	0	0	3	N/A	0	0%
Lost or stolen paperwork	3	2	1	-66%	0	-100%
Unauthorised access / disclosure	4	2	9	+125%	0	-100%
Corruption or inability to recover electronic data	0	0	1	N/A	0	0%
Other - Breach of confidentiality	1	0	0	-100%	0	0%
Other - Data quality leading to disclosure	1	0	0	-100%	0	0%
Other - Building security	1	0	0	-100%	0	0%
Total	**50**	**7**	**66**	**+32%**	**2**	**-71%**

44. The incident statistics for 2019 show a slight increase in incidents overall and a change in the type of some incidents that are being reported. Incidents that resulted from disclosures in error have increased and there has been a slight increase in lost or stolen hardware which is due to better integration of reporting between ICT Services and the Data Protection Officer rather than an increase in incidents reported which have largely been due to thefts from vehicles.

45. The reclassification of some incidents to reduce reliance on the 'other' category has seen an increase in unauthorised/access disclosure reports which have largely related to allegations made against staff which are either unsubstantiated/unproven or where members of the public have gained unauthorised access to Council offices.

46. The key message within the incident statistics is the reduction in severity of impact from incidents due to quicker and more effective containment from timely responses and action by officers. This is also reflected in the fact that only 2 incidents were reported to the Information Commissioner this year, both of which resulted in no further action against the Council, in comparison to 7 in 2018.

47. Whilst further training and communications on Council policy requirements, better detection procedures for records access will address some of these rising trends, a review of physical security is needed to mitigate the access issues which have also been highlighted by the ICO as in need of urgent work.

Information Requests

48. The following table summarises statutory information requests received by the Council in 2019 and trends over the past four years.

Request	2016	2017	2018	2019	% change in past year	% in time in 2019	% in time trend
Data Protection Act 2018							
Subject Access Requests	53	42	72	140	+94%	42%	Down
Disclosure – Crime or taxation	65	56	91	121	+33%	N/A	N/A
Disclosure - Immigration	0	0	0	8	N/A	N/A	N/A
Disclosure – Legal proceedings	10	10	12	55	+358%	N/A	N/A
Disclosure – Public protection	0	0	0	2	N/A	N/A	N/A
Disclosure – Regulatory	0	2	0	0	N/A	N/A	N/A
Freedom of Information Act 2000							
FOIA requests	1,229	1,266	1,343	1,360	+1%	81%	Down
Environmental Information Regulations 2004							
EIR requests	75	197	206	214	+4%	79%	Down
Appeals (FOIA and EIR)							
Requests to review initial responses	21	10	23	26	+13%	65%	Down
FOIA appeals to ICO	2	2	5	2	-60%	100%	Same
% FOIA appeals upheld in MBC favour	0%	100%	40%*	0%	-40%	N/A	N/A
Total	**1,455**	**1,585**	**1,752**	**1,928**	**+10%**		

**2 appeals remain outstanding – dates for these are determined solely by the ICO.*

49. In summary, the number of information requests received by the Council continues to grow at around 10% per annum, though growth is now been driven by the DPA 2018, particularly Subject Access Requests (SARs), with the growth in FOIA and EIR requests relatively static in 2019.

50. Analysis undertaken during in the year however has suggested that the volume of FOIA and EIRs received by the Council significantly exceeds those received by other local authorities in the region. In 2018, the received 50% more requests than Redcar and Cleveland and 25% more than Newcastle councils. The difference is the volume of local requests, linked to largely to urban development.

51. This volume of requests places a considerable burden on all of those involved in responding to them. This is particularly the case within Children's Services, given its focus on Ofsted requirements and other pressures. The timeliness of responses continued to fall in 2019, with SARs (many of which fall to Children's Services to answer) a particular concern.

52. This matter was covered in the 2018 report to this Committee and discussions have been ongoing throughout the year to put in place a solution to allow requests to be responded to in line with statutory timescales. As a result, a new post was created to process historic SARs (the postholder started in January 2020) and work as part of temporary recovery arrangements until such a time as BAU arrangements within Children's Services are sufficiently robust to achieve statutory compliance.

53. Three of the four urgent recommendations made by the ICO relate to SARs, specifically relating to improving the monitoring of compliance and the provision of training for those responding to requests, which in future will be mandatory. These have been implemented and will be kept under review during 2020.

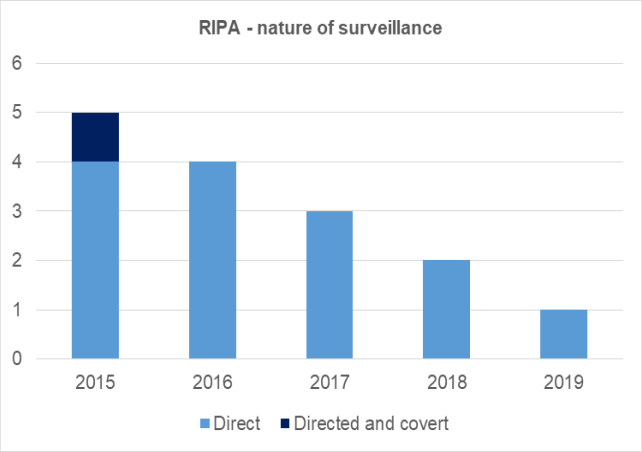
RIPA

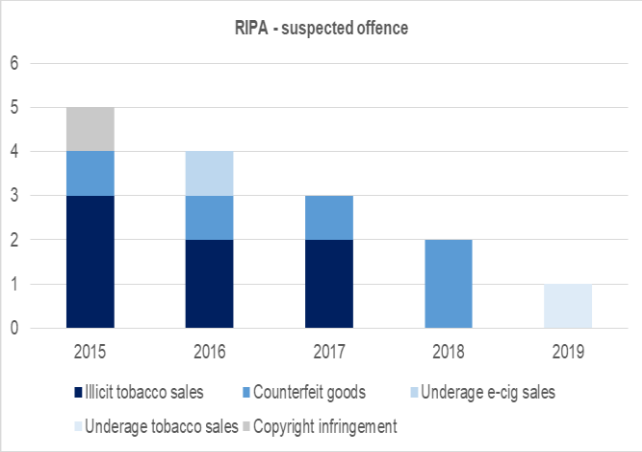
54. RIPA is the law governing the use of surveillance techniques by public authorities, including local authorities. RIPA requires that when public authorities need to use covert techniques to obtain private information about someone, they only do so if surveillance is necessary, proportionate, and compatible with human rights. Typically this relates to suspected criminal activity that is likely to result in a custodial sentence of six months or more.

55. In such instances, surveillance (either covert and / or directed) can be undertaken, subject to magistrate approval, if it is not possible to gather sufficient evidence to secure a prosecution without this.

56. As set out in the last annual report, the Council was in late 2018 subject to a (periodic) documentary inspection by the IPCO regarding its use of RIPA powers. This inspection demonstrated a level of compliance that removed the requirement for a full inspection at that time, and singled out the Council's training and (then draft) RIPA policy for praise. That RIPA policy has since been approved by the then Executive Member for Finance and Governance in February 2019), with the annual update of the policy to be considered by the current Executive Member in February 2020.

57. The Council's use of RIPA has reduced annually since 2015. The charts below set out the number of applications made the Council, the nature of the surveillance and the reasons why it was undertaken.





CCTV

58. The Surveillance Camera Commissioner wrote to SROs in December 2019 confirming that a survey of all local authorities will be undertaken in early 2020 to assess the compliance of systems operated by councils with the PoFA 2012 and the Surveillance Camera Code of Practice.

59. The Council's use of CCTV across different Directorates has grown in recent years and work will be undertaken during 2020 with the Council's Single Point of Contact (the Enforcement and Surveillance Manager) to ensure that a consistent corporate approach to demonstrating compliance is being maintained.

Assessment of information risk

60. During 2019, the Council continued to take steps to enhance information governance and minimise information risk across the organisation.

61. Taking into account progress in the past year and issues and risks emerging from the ongoing monitoring of the Council's information governance practice, the revised short-form version of the Council's information risk register is attached at Appendix 3.

62. In general terms the risk profile is reduced, but (as set out within the report) the Council needs to act urgently to resolve risks relating to:

- breach of data rights arising from untimely response to information requests, particularly Subject Access Requests; and
- compromised information security from unauthorised access due to tailgating / break-in.

63. A new approach to the monitoring and management of information risk will be introduced alongside the new IGF which will be reflected in the next annual report.

Priorities for 2020

64. Key priorities for 2020 to address the issues and risks outlined in this report are as follows:

- Implement all actions arising from the Council's ICO Consensual Audit.

- Clear the Council's backlog of Subject Access Requests and put in place arrangements that ensure compliance for all information requests within statutory timescales in at least 90% of cases.
- Review physical controls into and within the Council's buildings and make recommendations to improve information security within the current and future estate.
- Launch the Council's revised Information Governance Framework to staff utilising the new business change framework, achieving a level of 95% acceptance and trained.
- In agreeing the revised Email Policy, seek CMT approval from greater controls within email to reduce the risk of data breach and duplicate records (e.g. auto-deletion after agreed time period).
- Review the Council's CCTV Code of Practice and adherence to the code across the Council's various CCTV schemes.

65. Future activity relating to data protection in particular will be influenced by Brexit, and progress on this will be monitored closely to ensure that the Council remains compliant with the future legal framework for the UK.

Key messages for staff

66. The following key messages will be communicated to staff via induction, Information Asset Owners and other means in order to ensure improved information risk management:

- If you do not recognise someone who is trying to access employee only areas, and they are not wearing a Council ID / lanyard or appropriate visitor badge, do not simply hold the door open for them. If they appear lost, politely refer them to reception. If you are concerned, report the matter to reception or raise the matter with your manager straight away.
- Always leave your workspace clear of information and your computer screen locked when unattended – no documents or passwords should be left on desks or monitors, drawers and filing cabinets should always be locked.
- Never use your Council email address for personal reasons e.g. signing-up to a website not related to work.
- Never use the same password for different Council systems and do not use any work passwords on non-Council systems e.g. personal email or website accounts.
- Do not access records that you have no professional reason to view – this includes reading material that may have been accidentally left on desks or photocopiers.
- Keep the use of paper to an absolute minimum – diaries, notebooks or correspondence – and never leave these unattended.
- Be careful when sending emails and letters that you take the time to make sure that you are using the correct, up to date, and full addresses.
- If you are sending documents electronically to a recipient, consider using Objective Connect for extra security and audit trails.
- Always transport devices and any information on paper (where taking this off-site is unavoidable) in the boot of your car. If using paper to work at home, do not leave in a place where it can obviously be stolen (e.g. with your laptop in the hall) at night or when you are out of the house.
- Be careful in your personal use of social media that you do not make yourself vulnerable to identity fraud.

What decision(s) are being asked for?

67. That the Committee notes the position set out in the report, and proposes for consideration any further steps it may wish to see taken to promote good practice in information governance within the Council.

Why is this being recommended?

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

Other potential decisions and why these have not been recommended

69. Not applicable.

Impact(s) of recommended decision(s)

Legal

70. IG is governed by European and UK legislation, regulation, statutory guidance and case law. This report sets out, at a high level, the reasonable technical and organisational measures that the Council is taking and plans to take in order to ensure compliance with this legal framework and minimise information risk.

Financial

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

Policy Framework

72. Current and planned activity outlined is consistent with the direction of travel set out in the 'Business' section of the Strategic Plan, so this report does not vary the Council's Policy Framework.

Equality and Diversity

73. Not applicable.

Risk

74. This report sets out the Council's information risks and current arrangements and future plans for their management.

Actions to be taken to implement the decision(s)

75. Not applicable, as the report advises the Committee and seeks comment. The activity outlined in the main body of the report will result in significant improvements in the Council's information governance arrangements.

Appendices

Appendix 1	Progress on 2019 priorities
Appendix 2	ICO Consensual Audit – Executive Summary
Appendix 3	Summary Information Risk Register at end 2019

Background papers

08/02/18	Corporate Audit and Affairs Committee	Annual Report of the SIRO
07/02/19	Corporate Audit and Affairs Committee	Annual Report of the SIRO

Contact: Paul Stephens, Head of Strategy, Information and Governance
Email: paul_stephens@middlesbrough.gov.uk

Appendix 1: Progress on 2019 priorities

Priority	Status	Progress at end 2019	Remaining / resulting actions for 2020
Implementing actions from the 2018 LGA Cyber Security Stocktake, specifically providing specialist cyber security training for professionals in ICT, implementing an intrusion alert system, and nominating a council member with lead responsibility for cyber security.	Ongoing	The Executive Member for Finance and Governance is lead member for information security. Specialist training has been delivered to ICT teams, with a forward plan of training now in place. The intrusion alert system will be configured in early 2020/21.	1. Complete implementation of specialist training for ICT teams. 2. Complete implementation of intrusion alert system.
Implementing a revised process for starters / leavers / movers notifications, removing reliance on manager notification, and reducing the risk of data breach.	Ongoing	ICT now receives automatic notification of starters / leavers / movers once the Council's HR system has been updated, significantly reducing the risk of data breaches. Work will progress in 2020 to extend this approach to permissions around physical access.	3. Ensure that notifications of starters / leavers / movers are applied to physical access systems and that physical and digital access permissions are aligned.
Implementing the Information Strategy and revised policies for Secure Working, Data Protection, Records Management, Data Management, Access to Information and RIPA that will underpin it.	Ongoing	The Information Governance Framework has been fully reviewed during 2019, with a number of supporting policies either revised or created. During 2020, the Information Security Policy will be updated and CCTV practice reviewed, completing this work.	4. Complete revision of Information Security Policy and review CCTV Code of Practice.
Continuing to enhance the functionality and securing of email, improving integration with Objective to allow email records to be better captured, and ensuring that the Council's system is able to offer the same level of security as the Government's GCSX accounts, when these end in March 2019.	Ongoing	Following enhancements to the main Exchange email system, GCSX was decommissioned as planned. An upgrade of the Objective system was deferred until the functionality required by the Council is available. A revised email policy will be rolled out in 2020.	5. Complete discussions with Objective in respect of future functionality of the system and how this aligns with the Council's Information Strategy. 6. Launch revised Email Policy as part of the updated Information Governance Framework.

Priority	Status	Progress at end 2019	Remaining / resulting actions for 2020
Digitising and / or archiving historic paper records as appropriate, minimising the creation of new paper records through revised approaches to print and mail, and shifting the majority of electronic records to our Enterprise Content Management System (Objective), to improve their accessibility and usefulness.	Ongoing	Considerable work has been undertaken in recent years to quantify and secure the Council's physical records in line with future planning for the operational estate. Over 9,000 cabinets of paper records have been securely destroyed, and in 2019 the majority of the Children's Services archive was digitised (126 cabinets). In addition, 114 file shares have been closed (133,000 documents deleted). A new contract for digital mail and print was agreed with Xerox, with solutions now being rolled out.	7. Complete business case for archiving / digitising physical records for consideration as part of move to new HQ accommodation. 8. Develop and implement file share minimisation plan. 9. Fully implement digital mail and print solution.
Implementing a business change programme to ensure our managers and employees understand our IG framework and how to make it work for them. We will ensure that this integrates with other work being undertaken to modernise working practices in the run-up to our moving into our new headquarters in 2020.	Deferred	This was deferred due to changes in plans for the Council's future HQ following the May 2019 election. Discussions have been held internally regarding data protection by design so that the new accommodation is fir-for purpose from an information risk perspective.	10. Launch revised IGF using the Council's new business change model. 11. Develop DP by design approach for new accommodation using lessons from post-ICO audit project on Central Campus access.
Automating data sharing where practicable, and ensuring that employees, and where appropriate partners and contractors, are provided with the tools to share information securely and effectively.	Ongoing	Use of the secure transfer site Objective Connect has continued to grow, with 578 shares currently open sharing over 40,000 documents. Connect is now used for all new employees to receive new starter welcome packs with health, contract and pay information.	12. Map information sharing agreements and identify where digital solutions can further assist in data sharing.
Reducing the number of information requests reduce by proactively publishing commonly requested information via new Open Data portal, and establishing an arrangement within Children's Services to improve the responsiveness to SARs.	Ongoing	An early resolution approach to FOI was implemented in 2019, resulting in almost 500 requests being answered at first point of contact. The implementation of the new GIS system was delayed, resulting in a corresponding delay to the Open Data portal, which has now been developed. Following a number of discussions an arrangement has been established with Children's Services to improve responsiveness to SARs.	13. Launch Open Data portal. 14. Monitor revised approach to SARS to ensure that it is successful in clearing backlog and delivering knowledge transfer to Children's Services providing for timely response in future.

Appendix 2: ICO Consensual Audit – Executive Summary

Middlesbrough Council

Data protection audit report

December 2019

ico.
Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

Following a registration of interest made by Middlesbrough Council to the ICO in June 2019 to engage in a consensual audit, the ICO agreed to conduct an audit of its processing of personal data.

The purpose of the audit is to provide the Information Commissioner and Middlesbrough Council with an independent assurance of the extent to which Middlesbrough Council, within the scope of this agreed audit, is complying with data protection legislation.

It was agreed that the audit would focus on the following areas:

Scope Area	Description
Governance & Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the GDPR and national data protection legislation are in place and in operation throughout the organisation.
Security of Personal Data	There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.
Requests for Personal Data & Data Portability	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to or to transfer their personal data.

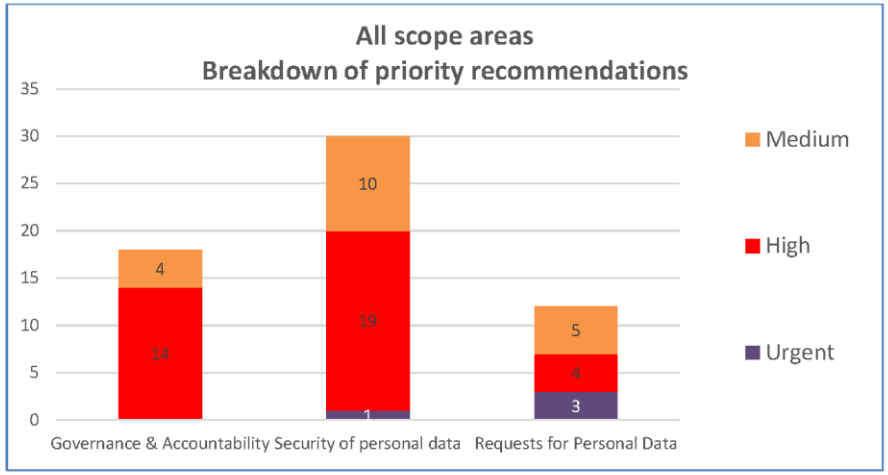
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist Middlesbrough Council in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. Middlesbrough Council's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

Audit Scope Area	Assurance Rating	Overall opinion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Security of Personal Data	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Requests for Personal Data & Data Portability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

Priority Recommendations



Areas for Improvement

The Council should continue to produce a completed Record of Processing of Activities for each of its service functions.

In public-facing areas where personal data is being provided, the Council should ensure that information about how it processes individuals' personal data (i.e. privacy notices) is made readily available and in an appropriate format. It should also ensure that whenever it is capturing special category personal data, details of individuals' rights in line with data protection legislation are transparent and clear.

The Council should provide specialised data protection training for operational staff teams who encounter higher risks in their practice and/or those with more specialised job functions.

The Council should review the policies and procedures around physical access control.

The Council should extend the practice of periodically reviewing access rights to all case management systems where personal data is being processed.

Periodic checks should be introduced of the access activity to all case management systems where personal data is being processed.

The Council should monitor its compliance with Subject Access Requests (SARs), including introducing Key Performance Indicators (KPIs) in relation to historical SARs, to identify if any additional resources or changes to procedures around SARs need to be considered.

The Council should assess the training requirements of staff responsible for handling SARs and introduce mandatory specialised training for all staff who have a responsibility for processing requests.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Middlesbrough Council.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of Middlesbrough Council. The scope areas and controls covered by the audit have been tailored to Middlesbrough Council and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.

Appendix 3: Summary Information Risk Register at end 2019

Category	Risk	Current score[1]	Trend	Target score
Internal	Breach of data rights due to untimely response to information requests	20	Same	10
Internal	Unauthorised access due to tailgating / break-in	20	Up	3
Internal	Breach caused by third party processor	15	Same	10
Internal	Internal misuse of data	15	Same	10
Communication	Loss of sensitive data by human error	15	Same	6
Internal	Non-compliance with information law, including GDPR	14	Same	7
Internal	Non-compliance with Baseline Personnel Security Standard	14	Same	7
Internal	**New** Non-compliance with PoFA 2012 (CCTV provisions)	10	-	5
Internal	Lack of employee golden record	9	Same	6
Internal	Ineffective staff training	9	Same	6
External	Loss of personal data from cyber attack	7	Down	7
Technical	Disaster recovery	7	Up	6
Technical	Unauthorised access due to ICT not being notified of movers / leavers	6	Down	6
Internal	Non-compliance with Payment Card Industry standard	6	Down	3
Internal	Non-compliance with NHS IG Toolkit	5	Same	5
Internal	Insecure disposal of records	5	Down	5
Technical	Vulnerabilities in third party applications	5	Same	5

[1] Scoring is in line with the Council's Risk Management Framework. Low risks = <8, Medium = 9-15, and High = >20.

Category	Risk	Current score	Trend	Target score
Technical	Unsupported infrastructure / applications	5	Same	5
Technical	Unauthorised access due to incorrect security settings	5	Same	5
Technical	Patching failure	5	Same	5
Internal	Non-compliance with PSN standard	5	Same	5
Internal	**New** Non-compliance with RIPA 2000	5	-	5
Technical	Encryption failure	2	Same	2
Technical	Insecure disposal of hardware	2	Down	2