MIDDLESBROUGH COUNCIL	Middlesbrough moving forward

Report of:	Head of Strategy, Information and Governance

Submitted to:	Corporate Audit and Affairs Committee, 31 March 2022

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

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 2021-24 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 2021 calendar year, risks and issues arising, and priorities for 2022.

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);
    - 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. 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.

5. The Head of Strategy, Information and Governance 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 2021

Implementation of 2021 priorities

6. The last annual report to this Committee (29 April 2021) set out eight key priorities to reduce information risk for the 2021 calendar year and beyond.

7. During this period the COVID-19 pandemic has persisted, and again associated restrictions resulted in some delays to planned activity, as relevant employees were either re-directed to emergency response or otherwise unable to progress work e.g. due to the unavailability of the workplace.

8. As such, work on these, and other priorities identified during 2021 and set out within this report, will complete during 2022. Nevertheless, good progress was made in many areas during the year, as summarised below.

Cyber security posture

9. The first priority for 2021 was to continue the monthly monitoring of the Council's cyber security posture and improvements and undertake a staff phishing exercise. While always critical, this assumed even greater importance during COVID-19, given the continued increase in cyber-attacks worldwide and potential increase of a successful attack exploiting the disruption caused by the pandemic. This priority was achieved and the *Cyber Security* section of this report outlines improvements delivered during the year in detail.

ICO consensual audit

10. The second priority was to complete the implementation of remaining actions arising from the ICO's consensual audit and follow-up of the Council's data protection arrangements, which took place in late 2019 and 2020 respectively.

11. This audit looked specifically at three crosscutting domains:

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

12. The Committee will recall that the audit rated the Council as providing a 'reasonable' level of assurance (the second highest of the ICO's ratings, behind 'high') that the Council's arrangements are delivering data protection compliance across the above three domains.

13. Of the original 63 recommendations made by the ICO, only eight are yet to completely implemented, in part due to the delays in reoccupation of buildings following 'work from home restrictions' in the pandemic. However, it should be noted that work is now ongoing to complete these actions during 2022, which are in the areas of information asset management and system access.

Information Governance Framework

14. The third priority was to launch the revised Information Governance Framework (IGF) as part of the post-pandemic reinduction process, and enhance elected member training on information governance.

15. This priority was again delayed due to COVID-19, but the opportunity was taken during the year to refresh the IGF, which now includes the Surveillance and Premises Security and Access Policies. A staff survey on the IGF has been issued and the results of this will inform the development of training and associated guidance, which will be launched in 2022.

16. Refreshed mandatory data protection training was launched during the year, Following development of an integrated, comprehensive dashboard for the reporting and management of data protection training completions, LMT and DMTs have

increased compliance to 82%. This means that of the 3,244 employees within the workforce, 2,659 have completed mandatory training within the required 12-month refresh period. The Council is aiming to increase this to and consistently maintain compliance at 95% in line with ICO guidance. Staff training is a key organisational measure required to ensure that the Council complies with data protection legislation and hence is one of the three key metrics monitored and reported to LMT and DMT level.

17. In December 2021, Constitution and Members' Development Committee agreed that the DPA training for elected members would be made mandatory. E-learning comparable to that undertaken by officers has been purchased and circulated to members for completion. Progress on completions will be reported to Constitution and Members' Development Committee and this Committee as appropriate.

Statutory information requests

18. The fourth priority was to continue to improve the Council's responsiveness to information requests through the provision of real-time dashboards for senior managers.

19. These dashboards are now in place and are monitored by departmental management teams and Leadership Team monthly. The Information Requests section of this report provide detailed statistics on volumes of requests received during the year and compliance with statutory timescales. In brief, while good progress has been made in addressing the backlog of Subject Access Requests – a key priority for the Council – the timeliness of responses to new information requests (though improving significantly during the last quarter of the year) remains too low, and the Council has allocated additional resources to the Information Requests team to improve performance significantly during 2022.

Physical access

20. The fifth priority was to agree a physical security policy and procedures for the Council's office estate, implementing changes for reinduction and advising on design of the Council's new headquarters, since confirmed to be Fountain Court.

21. A Premises Security and Access Policy has now been approved and is in the process of implementation across all premises. Aside from the obvious health and safety benefits, the policy will mitigate the potential for data breach through unauthorised access to premises.

Historic paper records

22. The sixth priority was to agree a position in respect of digitising or rehousing the Council's historic paper records as part of the new HQ project. This has been achieved and is detailed in the Records Management section of this report.

Surveillance policy

23. The seventh priority was to complete and implement the revised Surveillance Policy and actions from the then forthcoming internal audit of CCTV. The Council's first integrated Surveillance Policy was approved by the Executive Member for

Environment, Finance and Governance in August 2021. The Surveillance section of this report sets out the Council's response to the internal audit of its CCTV and planned actions for both overt and covert surveillance during 2022.

Alignment of major ICT projects and information governance requirements

24. The final priority was to ensure that key ICT projects for 2021 including the migration to Microsoft Office 365 and the review of the Council's website were aligned with the Information Governance Framework and progress the aims of the Council's Information Strategy. This has been achieved through close collaborative working between services during the year.

Information Strategy progress

25. 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.

26. 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.

27. Much work has been undertaken to date on the 'Organise' theme, updating and joining up the Council's IGF. The IGF can be found on the Council's intranet and now comprises the following policies:

Policy	Last revision	Next revision
Data Protection Policy	2021	2024
Secure Working Policy	2021	2024
Premises Security and Access	2022	2025
Data Management Policy	2021	2024
Records Management Policy	2019	2021
Microsoft 365 Policy	2021	2024
Direct Marketing and Cookies Policy	2021	2024
Surveillance Policy (subsumes RIPA Policy)	2021	2022
Public Information and Requests Policy	2021	2024

28. As indicated above, the majority of policies were reviewed during the year, mainly in line with the introduction of Microsoft 365. The review of the Records Management Policy was deferred so that the review of the Council's enterprise content management system (ECS) could be taken into account and will now be reviewed in 2022.

29. As set out in paragraph 15, the IGF will be relaunched during 2022, with additional training and guidance to be provided, particularly to Information Asset Owners.

30. During 2022 a new Operations Strategy will be developed for the Council, subsuming existing strategies such as the ICT and Information Strategies in order to create maximum alignment in future.

Changes to information asset registers

31. Information asset registers (IARs) list all the information owned by services, in any format, quantifies these and sets out how they are managed across the lifecycle. IARs are owned by Information Asset Owners (Heads of Service).

32. 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

33. This information map was reviewed at the end of 2021, with the overall RAG as set out below.

RAG	Definition	%	Change from 2020
Red	Does not meet basic requirements	5.3%	-9%
Amber	Meets basic requirements but requires improvement	42.4%	-1%
Green	Fit for purpose	52.3%	+2%

34. 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).

35. A significant amount of data sharing was again undertaken during the year, particularly in relation to the pandemic response and recovery. This was swiftly and securely handled by all services.

Information security

36. COVID-19 has continued to prove challenging for all of those working in information security, which is properly defined as activity designed to protect all appropriate data (print, electronic and other) from unauthorised persons, and rapidly changed the Council's information security risk profile.

Cyber security

37. The Committee should note that 2021 saw a continued escalation in global cyber security risk, which was exacerbated by continued remote or home working during the COVID-19 pandemic and the rapid implementation of video conferencing and other collaborative solutions. Ransomware and state-sponsored attacks will again dominate the threat landscape in the coming year, with successful data breaches fuelling the upward trend in attacks.

38. In response to the threat of state-sponsored attacks, during the year the Council strengthened geo-location blocking and blocked all internet traffic from China and Russia to mitigate the threat from persistent attacks emanating from those territories. The list of blocked territories is kept under continuous review.

39. The Head of ICT attended Leadership Team during the year to increase awareness of the increasing cyber security risk, including sharing lessons learned from the attack on Redcar and Cleveland Borough Council in February 2020 (the recovery from which cost an estimated £12m) and the approach being taken to securing the ICT estate.

40. Within this context of rising threats globally, the Council continued to maintain a strong cyber security posture during 2021. No systems (whether on premises or in the Cloud), services or information were compromised during the year, and all hardware and software continued to be supported, updated and patched in line with the Council's policies.

41. Several threats requiring immediate intervention were identified and mitigated during the year, the most significant being Log4j, a Java-based vulnerability found in the code of almost all websites and applications around the world. The Council remediated this vulnerability without data loss or disruption to business activities.

42. Following ongoing issues, several of the Council's websites currently hosted and managed by external parties will transfer to ICT Services during 2022/23 to ensure cyber security as part of an overall review of the Council's online presence, including its corporate website.

43. In line with the Council's device refresh programme, and in response to the evolving scale and impact of the pandemic, 700 laptops were rolled out to employees, enabling them to work flexibly, at home or in the office. The planned introduction of Microsoft 365 was also expedited by one year to ensure all users have access to online collaborative tools.

44. 1,126 access control changes were processed during 2021/22:

    - 474 new starters (115 of which were temporary or agency staff) had access rights established;
    - 103 employees moved role and had access rights updated as a result; and
    - 549 leavers had access rights removed.

45. No end-of-life devices were destroyed by the Council's contractor during 2021 due to COVID-19 restrictions. All end-of-life devices are securely stored, and it is anticipated

that the secure recycling of equipment will recommence in spring 2022 with appropriate data destruction certificates being supplied.

46. Following the decommissioning of the GCSX secure email system in 2019, unencrypted email traffic leaving the Council's network reduced to below 1% and will reduce further in future years as partners increase their own security postures.

47. Several important technical improvements were delivered during the year to enhance the Council's cyber security, including:

- the introduction of Microsoft 365 provided significant additional options for device security, including Windows Hello, PIN, Multi Factor Authentication, biometrics;
- in line with the introduction of 365, much of the corporate email infrastructure was migrated to Microsoft Azure Cloud to increase security, resilience and performance;
- the resilience offered by 365 was supplemented by an on premises daily back-up solution so that the Council can access its mailboxes in the event of the Microsoft Cloud being unavailable;
- additional controls were applied to devices to reduce the risk around the use of applications and to limit the use of USB peripherals; and
- a security information and event management was implemented, providing real-time analysis of security alerts generated by applications and network hardware.

48. Between September and November 2021, 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.

49. 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 2021.

50. The Council continues to subscribe to all appropriate national and regional cyber security networks and alert services.

51. The Council successfully retained accreditation from the Government-backed Cyber Essentials scheme during the year, and the Council's email domain security posture achieved the highest rating across all North East local authorities in the recent Cyber Health Care assessment conducted by the Northeast WARP (Warning Advice & Reporting Point).

52. The Councils internal auditor assessed the Council's controls in relation to Cyber Awareness during the year, an exercise which included a bi-annual phishing exercise on a sample of employees. The auditor provided an opinion of 'strong assurance' on the controls in place and the outcome from the phishing exercise will inform future training and communication with employees.

53. The approach to and resourcing of cyber security will be kept under regular review in line with the high level of risk in this area, which has increased further following

Russia's invasion of Ukraine in February 2022. The future approach will reflect changes to National Cyber Security Centre guidance as well as the Government's recently-published National Cyber Strategy for 2022-2030.

Records management

54. The continued closure due to the pandemic of Council buildings to the public and the majority of employees, with logging of those attending, continued to temporarily reduce the risk to information from unauthorised access. The Council now mandates clear floor and desk policies, and checks will be undertaken during 2021 to ensure employees are complying with this directive, post office reoccupation.

55. During 2020, a business case for archiving / digitising physical records was completed for consideration as part of the forthcoming move to the Council's new headquarters, since confirmed to be Fountain Court.

56. During 2021, the planning archive (1,959 boxes, dating back 26 years) housed in the Civic Centre was indexed and sent to an offsite facility which will provide a scan on demand service. If a request is received for the information via the Council's Planning Portal, the relevant file will be pull scanned and uploaded to the planning site for public viewing.

57. During 2022 a decision will be made on the preferred options for the remaining historic records, held in the Municipal Buildings, as part of decisions on the future use of this building following the Council's decampment from the Civic Centre. This will also address the long-term storage needs of historic records not held within the Central Campus.

58. A review of the Council's enterprise content management system (ECS) was undertaken during the year, in line with the move to Microsoft 365 during 2021.

59. The agreed option was to pursue Microsoft SharePoint as the Council's ECS going forward, integrating with 365. With appropriate licensing and supplementary applications, SharePoint can be configured to meet the Council's needs for a structured ECS, including document workflow, and its ambitions for improved document tagging, retention and deletion and search.

60. It is imperative that SharePoint is appropriately resourced so that it can be implemented and managed in line with the Council's Record Management Policy, and that the roll-out plan mandates the use of SharePoint over other potential options wherever possible so that the Council finally has a single solution for electronic document storage.

61. Both the move to Fountain Court and implementation of SharePoint involve the transit of very significant amounts of data, and as such the risk of data loss and hence large scale breaches of the DPA, FOIA and EIR will be heightened in 2022.

Data protection

62. 2021 was the first year post-Brexit in which the UK General Data Protection Regulation took effect having been transferred into domestic law with minor amendments. The UK Department for Culture Media and Sport (DCMS), as the

parent department for data protection, launched a consultation in September 2021 'Data: a new direction' with the following broad policy aims:

- support vibrant competition and innovation to drive economic growth;
- maintain high data protection standards without creating unnecessary barriers to responsible data use;
- keep pace with the rapid innovation of data-intensive technologies;
- help innovative businesses of all sizes to use data responsibly without undue uncertainty or risk, both in the UK and internationally; and
- ensure the Information Commissioner's Office (ICO) is equipped to regulate effectively in an increasingly data-driven world.

63. The consultation feedback will inform the Government's proposed 'Brexit Freedoms Bill' which will amend the existing data protection regime. As a public authority that handles high volumes of sensitive data, it is expected that the Council will still be required to meet high data protection standards. The Government's proposals may lead to some changes in how the Council administrates data protection matters and may derive other benefits such as the simplification of the appointment of overseas suppliers particularly in the areas of data hosting and processing. The expected legislative reforms will be a key area of work for the Data Protection Team in 2022/23.

64. The use of overseas suppliers is an area of work that continues to present significant challenges within the procurement process as the Council is required by law to assess the compliance of complex digital supply chains. This can involve the hosting and processing of data in countries with legal regimes that do not guarantee the same level of protection to personal data including the United States of America which is a major global hub for data storage services. Eight months after the European Union issued updated 'standard contractual clauses' (SCCs) for use in assuring the security of data transfers overseas, DCMS has laid draft 'International data transfer agreements' before Parliament. These are a UK version of the SCCs which will take some months for overseas suppliers to assess and offer to customers.

65. In addition to work on personal data breach management and audits of subject access request complaints, data protection work has focussed largely on the following items:

- developing LMT and DMT dashboards for information security incidents, information requests and employee training completion;
- procuring and implementing data protection training for elected members;
- developing more granular Privacy Notices – particularly in relation to local COVID-19 projects and grant schemes;
- implementing several important information sharing agreements with key partners – again particularly in relation to COVID-19 projects;
- improving the way in which suppliers that process personal data for the Council are assessed and appointed; and
- developing a Direct Marketing and Cookies Policy and implementing changes to ensure that the Council's websites and applications comply with the latest guidance from the ICO.

66. The Council is also in the fourth year of the refreshed NHS Data Security and Protection Toolkit, the health and social care information governance standard. This

self-assessment approach has largely reduced the evidential burden on the Council to prove compliance through large amounts of documentary evidence, focussing efforts on the National Data Guardian Standards. Completing the Toolkit is a key aspect of providing assurances to national and regional health partners and the Council's response to the COVID-19 pandemic, specifically access to test and trace and vaccination data, would have been limited without this being in place.

67. Incident statistics for 2021 show a slight increase overall and changes in the type of some incidents that are being reported, which are reflected in the information risk profile at Appendix 1. Incidents that resulted from disclosures in error increased and there was a slight increase in lost or stolen hardware, which may be explained by the changing nature of working from home as people movement restrictions have been relaxed over the year.

68. The severity of impact from incidents remains under control due to quicker and more effective containment from timely responses and action by officers and despite two incidents meeting the legal threshold for reporting to the ICO in 2021, following engagement and investigation the ICO took no further action having been satisfied with the Council's incident management and response.

Incident type	2019	Reported to ICO	2020	Reported to ICO	2021	% change in past year	Reported to ICO	% change in past year
Disclosed in error	52	2	84	0	88	4.8%	2	100%
Lost or stolen hardware	3	0	3	0	5	66.7%	0	0%
Lost or stolen paperwork	1	0	2	0	2	0%	0	0%
Unauthorised access / disclosure	9	0	9	0	7	-22.2%	0	0%
Corruption / inability to recover data	1	0	0	0	1	100%	0	0%
Uploaded to website in error	0	0	0	0	1	100%	0	0%
Other – breach of confidentiality	0	0	0	0	0	0%	0	0%
Other – building security	0	0	1	0	2	100%	0	0%
Other – damaged paper records	0	0	0	0	1	100%	0	0%
Other – data quality leading to disclosure	0	0	0	0	0	0%	0	0%
Other – email sent to personal account	0	0	1	0	0	-100%	0	0%
Other – inappropriate use of staff portal	0	0	1	0	0	-100%	0	0%
Cyber - Hacking	0	0	0	0	1	100%	0	0%
Total	**66**	**2**	**101**	**0**	**108**	**6.9%**	**2**	**100%**

Surveillance

69. As reported to the Committee last year, during 2020/21 the Council agreed with the IPCO that it would maintain an overarching Surveillance Policy, covering CCTV, RIPA, non-RIPA covert surveillance and the surveillance of employees. This policy was approved by the Executive Member for Environment, Finance and Governance in August 2021 and will be updated on an annual basis.

70. The Council's use of CCTV was subject to internal audit during 2021. The audit discovered a fundamental weakness in that the auditor was unable to demonstrate that all CCTV schemes were identified on a central register overseen by the Single Point of Contact (SPOC). As such, the risk of the Council not complying with the POFA 2012 across its various CCTV schemes was heightened. In addition, further

issues were identified relating to roles and responsibilities, compliance of disclosures with the DPA, performance management (including via service level agreements) and annual reporting.

71. While the audit yielded only Limited Assurance, the auditor had reviewed the then draft Surveillance Policy and confirmed in his report that all issues identified by the audit would be addressed when that policy was implemented. The agreed management actions in response to this audit (which form part of the Surveillance Policy implementation plan), with current deadlines, are set out below:

Action	Priority	Owner	Deadline
1.1) A central register of all public space surveillance camera equipment operated by the Council, including the location of each piece of equipment, its asset reference and the manager responsible, will be developed and maintained by the SPoC.	1	Operational Community Safety Manager (CCTV Single Point of Contact (SPOC))	28/02/22
2.1) Scheme managers and responsible officers will be identified for all schemes and maintain Code Assessment Packs, demonstrating compliance with the Councils local code of practice. The SPoC will produce an annual report based on a review of annual self-assessments for scheme managers.	1		28/02/22
3.1) CCTV Code of Practice and associated procedures to be supplied to all scheme managers and responsible officers, with appropriate briefings and / or training.	2		28/02/22
4.1) Define the role of SPoC within the Council's Surveillance Policy and brief SPoC on roles and responsibilities.	2	Head of Strategy Information and Governance	31/07/21
5.1) The SPoC will produce an annual report based on a review of annual self-assessments from scheme managers, which will include scheme performance against key measures and targets to be agreed with the Head of Strategy, Information and Governance (SRO).	2	Operational Community Safety Manager (CCTV Single Point of Contact (SPOC))	28/02/22
6.1) The Council's Data Protection Officer will schedule a more in depth data protection audit of the CCTV unit to review compliance with UK GDPR, DPA 2018, and ICO CCTV guidance.	2	Data Protection Officer	31/07/21
7.1) Contract owners to work with the NEPO and the CCTV provider to enforce current contract stipulations regarding performance and to update them where required in line with the Council's Code Assessment Pack and annual review process.	2	Operational Community Safety Manager (CCTV Single Point of Contact (SPOC))	31/03/22
8.1) To ensure formal approval of AIM Terms of Reference, CSP ISP and any existing tier 2 agreement are signed by relevant partners and any tier 2 agreements that need input / advice are forwarded to the Data Protection Officer.	3	Head of Stronger Communities	30/11/21

72. In brief, the following activity has been undertaken to date:

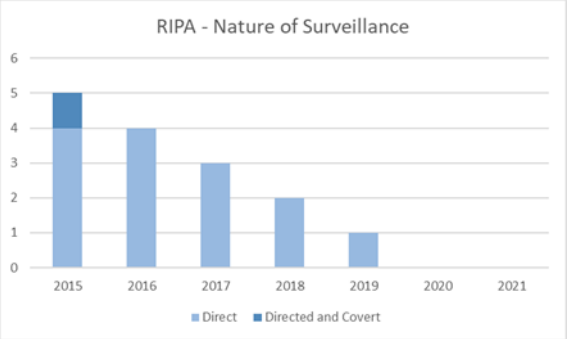
- the role of the SPOC was defined in the Surveillance Policy and the current role holder (the Operational Community Safety Manager) was briefed on role requirements;
- the SPOC has developed a central register of surveillance camera equipment, identifying schemes and scheme owners – the register needs to record asset numbers in order to be complete, and this work will be completed during 2022;
- the SPOC has revised the Council's CCTV Code of Practice and issued it to scheme owners, along with an associated Code Assessment Pack;
- scheme owners are in the process of completing their returns to the SPOC which will in turn allow him to complete the first CCTV annual report, which will be published on the Council's website;
- the SPOC has arranged monthly meetings with contract owners and quarterly meetings with scheme owners to discuss status and any compliance concerns; and
- the Data Protection Officer has confirmed that procedures in the CCTV unit are compliant with relevant legislation.

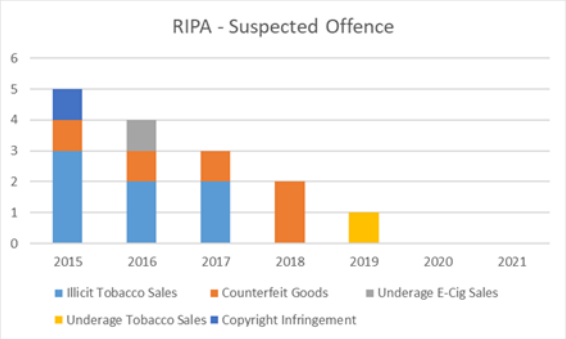
73. As such, while some actions from the audit will now complete in 2022, work to date has substantially reduced the risk of non-compliance with the POFA 2012 and this is reflected in the Council's revised information risk profile.

74. 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.

75. In such instances, covert surveillance can be undertaken, subject to magistrate approval, if it is not possible to gather sufficient evidence to secure a prosecution without this.

76. The Council's use of RIPA has reduced annually since 2015, with no applications made in 2020 or 2021, due in part to COVID-19. The charts below set out the number of applications made the Council in the past seven years, the nature of the surveillance and the reasons why it was undertaken.





77. The Council's revised Surveillance Policy commits the Council to establishing an authorisation process comparable to RIPA for covert surveillance undertaken during investigations that would not reach the RIPA threshold and this will be implemented during 2022. Also during the past year, the Council has taken steps to clarify under what circumstances employees may be surveilled (e.g. disciplinary investigations or for health and safety purposes) and how this would be authorised and undertaken.

78. As work on overt and covert surveillance procedures, the previous proposal to present a separate annual report on surveillance to the Committee will be deferred to next year.

Information Requests

79. The following table summarises statutory information requests received by the Council in 2021 and trends over the past three years.

80. In summary, caseload in respect of information requests grew by 2.9% in 2021, down significantly from the 26.5% growth seen in 2020, in which CCTV disclosure requests grew significantly following the transfer of the management of such requests from the corporate team to the CCTV unit, reflecting increasing joint working on crime and anti-social behaviour.

81. The Council carries out a vast amount of lawful information sharing daily with various partners and organisations. The number of requests for disclosure of information where the organisation has specifically sought the Council to 'exempt' the request from data protection laws has greatly increased. The main point to note regarding these exempted disclosures is that the Council would normally be required to inform the individuals about such disclosures and provide a copy of their data if it was requested by them. The 'exemptions' do not require notification or provision of data to a data subject if it would prejudice the purposes of the disclosure. The highest number of such requests remains in crime and taxation. However, immigration disclosure requests have increased, as have requests from regulatory bodies under the 'public protection' heading (mostly from the Disclosure and Barring Service and Social Work England).

Request type	2019	2020	2021	% change in past year	% in time in 2021	% in time trend
Data Protection Act 2018						
Subject Access Requests	140	81	142	75.3%	59.1%	Up
Disclosure – Crime or taxation	121	71	68	-4.2%	N/A	N/A
Disclosure – Immigration	8	20	31	55%	N/A	N/A
Disclosure – Legal proceedings	55	6	8	33.3%	N/A	N/A
Disclosure – Public protection	2	0	12	100%	N/A	N/A
Disclosure CCTV – Crime	-	1,045	1,096	4.9%	N/A	N/A
Disclosure CCTV – Legal proceedings	-	11	26	136.4%	N/A	N/A
Freedom of Information Act 2000 (FOIA)						
FOIA requests	1,360	1,032	919	-10.9%	69.6%	Down
Environmental Information Regulations 2004 (EIR)						
EIR requests	214	142	164	15.5%	64%	Down
Appeals (FOIA and EIR)						
Requests to review initial responses	26	26	39	50%	70%	Down
Appeals to the ICO	2	2	2	0%	100%	Up
% Appeals upheld in MBC's favour	0%	50%	100%*	N/A	N/A	N/A
Total	**1,928**	**2,436**	**2,507**	**2.9%**		

** One appeal pending at the time of writing.*

82. Growth in 2021 was mainly seen in Subject Access Requests and requests under the Environmental Information Regulations 2004, which returned to pre-pandemic levels, though requests under the Freedom of Information Act 2000 fell by 11% during the year. This is likely to be attributable to use of the Council's open data site, on which 1,500 datasets are now available, at 50% increase on 2020.

83. The Committee was provided with an interim update on work to address the Council's backlog of Subject Access Requests in September 2021. The number of SARs has returned to pre-pandemic levels and the number responded to on time has increased in 2021. The continued improvement work has reduced the Council's rolling number of overdue SARs from 26 at the end of 2020 to 17 as of February 2022. Of those 17, only 6 were originally received prior to 2021 – this is a marked improvement from the Committee's last update at which time there were 10 overdue requests still open that were received prior to 2021.

84. As a result of one complaint, the Council engaged with the ICO about its governance arrangements for SARs. It was able to provide detailed information regarding

overdue responses and the improvement plan in place to address these. Having been satisfied with the Council's responses (which included clearing the SAR backlog by August 2022), the ICO took no further action on this matter.

85. The Council continues to receive a number of complex information requests regarding key programmes and projects and associated political decisions, and the timeliness of responses did not approve as planned during the year. The Council has recognised this and agreed investment in two additional FTE posts within the Information Requests team. Coupled with the additional search capacity provided by Microsoft 365, this should see the timeliness of responses improve significantly during 2022.

86. During 2021, an internal audit of Direct Marketing and Freedom of Information requests was undertaken. This area of focus was agreed with the SIRO and Data Protection Officer to address priority issues not covered by the ICO Consensual Data Protection Audit.

87. The audit concluded that there is a generally sound system of governance, risk management and control in place, yielding an opinion of Reasonable Assurance and seven management actions (two Priority 2s and five 3s).

88. The two P2 actions related to revising the Council's Request for Information procedures to improve the robustness of the close down procedure, and implementing an FOI business intelligence dashboard so that LMT and Heads of Service will monitor responsiveness in real time to ensure compliance with timescales. These actions have now been completed. Four of the five P3 actions have also been implemented, with the outstanding action (relating to an online marketing consent platform) will be implemented as part of the Council's new website (due November 2022).

89. While the above 'green shoots' and additional investment provides some assurance the ongoing issues around timeliness of responses to information requests will be resolved during 2022, this issue remains a key information risk to the Council.

Assessment of information risk

90. During 2021, taking into account the continued impact of the COVID-19 pandemic, the Council continued to take positive steps to enhance information governance and minimise information risk across the organisation.

91. Considering progress in the past year, issues and risks emerging from the global and national situation and the ongoing monitoring of the Council's information governance practice, a revised short-form version of the Council's information risk register is attached at Appendix 1.

92. In overall terms, the Council's risk profile is broadly stable, but (as set out within the report) the Council needs to maintain extreme vigilance in relation to cyber security, as well completing activity to permanently mitigate risks relating to breach of data rights and unauthorised access. Loss of data (physical or electronic) while in transit or migration places as joint highest risk at the end of 2021 as the Council commences moving the vast majority of its records in the coming year.

93. Deferred from 2021, 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. As part of this, IAOs will be required to formally provide the SIRO with assurance on information assets and risks on an annual basis using a standard template.

Priorities for 2022

94. Key priorities for 2022 to address the issues and risks outlined in this report are therefore as follows:

- review the Council's approach to cyber security and continuity / recovery plans in line with changes to National Cyber Security Centre guidance and the Government's National Cyber Strategy for 2022-2030, focusing on zero-day, internet-facing application and supply chain attacks, particularly in view of the ongoing situation in Ukraine;
- continue to improve the Council's responsiveness to information requests through use of enhanced 365 tools and increased resourcing of the central team;
- continue to improve the Council's surveillance practice by implementing in full the provisions of the Surveillance Policy;
- develop an Integrated Operations Strategy for the Council, fully aligning all existing operational strategies including the Information and ICT strategies;
- launch the Council's revised Information Governance Framework to staff, focusing in particular on those with specific roles in the framework – IAOs, system owners and Information Asset Assistants;
- ensure that the move to and operation of Fountain Court is undertaken in line with the Council's Premises Security and Access policy to avoid loss of or unauthorised access to information;
- ensure that key ICT projects for 2022 including the migration from the Council's existing EDRMS to Microsoft SharePoint and the review of the Council's website are fully aligned with the Information Governance Framework and progress the aims of the Council's Information Strategy.

Key messages for staff

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

- Always ensure that you have completed the latest training on data protection, cyber security and related information governance matters.
- Power off your machine at the end of every day and restart it for updates when prompted.
- Always read and implement advice and guidance provided by ICT Services.
- Do not attempt to install any software without authorisation from ICT Services.
- Be vigilant to the threat from phishing – read emails carefully and report any suspect emails to the ICT Service Desk.
- 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.

- Be careful in your personal use of social media that you do not make yourself vulnerable to identity fraud.
- Never use personal devices (including printers), accounts (such as email or cloud storage) to store or work on Council documents and data.
- 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.
- 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, and drawers and filing cabinets should always be locked.
- Keep your 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) locked in the boot of your vehicle. However do not leave items unattended in your vehicle as these will not be deemed to be secured and you will be held responsible.
- 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.

What decision(s) are being asked for?

96. 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?

97. 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

98. Not applicable.

Impact(s) of recommended decision(s)

Legal

99. IG is governed by 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

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

Policy Framework

101. Current and planned activity outlined is consistent with the direction of travel set out in the 'Business' section of the Strategic Plan.

Equality and Diversity

102. Not applicable.

Risk

103. 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)

104. 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 Summary Information Risk Register at end 2021

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
06/02/20	Corporate Audit and Affairs Committee	Annual Report of the SIRO
21/04/21	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: Summary Information Risk Register at end 2021

Category	Risk	Current score[1]	Trend	Target score
Internal	Failure to comply with the FOIA 2000, EIR 2004 or DPA 2018 due to late response to information requests	20	Same	10
Internal	Loss of data (physical or electronic) while in transit / migration	20	New	5
Internal	Lack of employee and customer golden records / inaccurate records	20	Same	6
Internal	Unauthorised access to / loss of information due to tailgating, damage or theft	15	Down	3
Internal	Internal misuse of data	15	Up	10
Internal	Insecure disposal of records	15	Up	5
Communication	Breach of personal data by human error	15	Same	6
External	Breach of personal data from cyber attack	14	Same	7
Internal	Failure to comply with the UK GDPR 2016 / DPA 2018	14	Same	7
Internal	Failure to comply with the PoFA 2012 (CCTV provisions)	10	Down	5
Internal	Breach of personal data by third party processor	10	Same	10
Internal	Ineffective staff training on information governance	9	Same	6
Internal	Misfiled historic records	9	Same	3
Technical	Failure of disaster recovery	7	Same	6
Internal	Failure to comply with the Baseline Personnel Security Standard	7	Down	7
Technical	Unauthorised access due to ICT not being notified of movers / leavers	6	Same	6
Internal	Failure to comply with the Payment Card Industry standard	6	Same	3

[1] Scoring is in line with the Council's Risk Management Framework. Low risks = <5, Medium = 6-10, and High = >12.

Category	Risk	Current score	Trend	Target score
External	Reduced VFM in procurements due to international data transfer rules	6	Same	3
Internal	Non-compliance with the NHS Data Security and Protection Toolkit	5	Same	5
Technical	Vulnerabilities in third party applications	5	Same	5
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 Public Services Network standard	5	Same	5
Internal	Failure to comply with the RIPA 2000	5	Same	5
Internal	Failure to comply with the PECR 2003	5	New	5
Technical	Encryption failure	2	Same	2
Technical	Insecure disposal of hardware	2	Same	2