

**Report of:** Head of Strategy, Information and Governance**Submitted to:** Corporate Audit and Affairs Committee, 29 April 2021**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.

<b>Report for:</b>	<b>Key decision:</b>	<b>Confidential:</b>	<b>Is the report urgent?</b>
Information	No	No	No

**Contribution to delivery of the 2021-24 Strategic Plan**

<b>People</b>	<b>Place</b>	<b>Business</b>
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 2020 calendar year, risks and issues arising, and priorities for 2021.

## **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 (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 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 2020**

### **Implementation of 2020 priorities**

6. The last annual report to this Committee (6 February 2020) set out six key priorities to reduce information risk for the 2020 calendar year and beyond.
7. Shortly after this, the UK was locked down in response to the COVID-19 pandemic, and at the time of writing significant restrictions remain in place. As with all business areas, these restrictions resulted in 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 2020 and set out within this report, will complete during 2021. Nevertheless, good progress was made in many areas during the year, as summarised below.

### ***ICO consensual audit***

9. The first priority for 2020 was to implement all actions arising from the ICO's consensual audit of the Council's data protection arrangements, which took place in late 2019.
10. This audit looked specifically at three crosscutting domains:
- governance and accountability;
  - security of personal data; and
  - requests for personal data and data portability.
11. 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. The ICO made sixty-three recommendations to reduce the Council's risk of non-compliance.
12. In December 2020, the ICO undertook a follow-up audit and its report is at Appendix 1. Overall, the ICO concluded that despite some recommendations still awaiting completion, the Council had made meaningful progress to mitigate the risk of non-compliance with:
- 40 recommendations implemented;
  - 20 in progress; and
  - three yet to start.
13. The ICO noted improvements in risk management and monitoring, specialised training in subject access request handling, and development and implementation of a revised secure working policy.
14. The main areas of outstanding risk identified by the ICO were:
- expansion of detailed procedures for completing subject access requests to all directorates;
  - completion of the project on the physical security environment and access control procedures; and
  - implementation of a policy acceptance approach for all staff for information governance policies.
15. The outstanding actions from this audit will be implemented during 2021, with timescales aligned to the reoccupation of office space as COVID-19 restrictions ease, where appropriate.

### ***Subject access requests (SARs)***

16. The second priority for 2020 was to clear the Council's backlog of subject access requests (which fall largely within Children's Services) and put in place arrangements

to ensure compliance for all information requests within statutory timescales in at least 90% of cases. Three of the four urgent recommendations made by the ICO in the 2019 audit related to SARs, and this matter was the joint highest risk in the information risk register at the end of 2019.

17. The data protection and information requests sections of this report provide detailed statistics on volumes of requests received during the year and compliance with statutory timescales. However, in brief, given the pandemic:
  - the volume of information requests received reduced in all of the main RFI categories, including subject access requests; and
  - timeliness of responses fell slightly for FOI and EIR requests, but increased for SARs, though remained some way from the 90% target.
18. This resulted in only minor reduction in the Council's backlog of SARs, which reduced from 32 at the end of 2019 to 26 at the end of 2020.
19. While legal requirements to respond to information requests did not change, the ICO relaxed its regulatory approach during the year in recognition that the pandemic response would impact on local authorities' ability to respond within timescales. However, the ICO has now resumed regulatory activity and local authorities are expected to have recovery plans in place to address responsiveness issues and / or backlogs.
20. In line with this the Council took action during the year to ensure that this issue is now fully addressed during 2021:
  - a new post was put in place from January 2020 to process historic SARs and has had a significant impact in reducing these;
  - a procedure for handling SARs within Children's Services was created and implemented;
  - a temporary post was established within Children's Services was established to address the backlog of requests; and
  - ongoing monitoring of progress continued, with senior management and requesters regularly updated.
21. While, given the above position, this therefore remains the greatest information risk to the Council at present, there can be some confidence that the matter will be resolved during 2021.

### ***Physical access***

22. The third priority was to review physical controls into and within the Council's buildings and make recommendations to improve information security within the current and future estate. This matter was an urgent recommendation from the ICO and the joint highest risk in the information risk register at the end of 2019.
23. Complying with the ICO's recommendation, the Council launched a project to review physical security in early 2020 and a security audit of premises was undertaken prior to the first national lockdown in March 2020. The outcomes of this audit were then used to develop a draft corporate physical security policy, setting out a number of proposed procedural improvements.

24. While completion of this work was again delayed by the pandemic, the risk of information from unauthorised access of buildings was also significantly reduced during this period, through the closure of most Council buildings to the public and the close monitoring of those who did attend, and the significant reduction in paper holdings through the enforcement of clear floor and desk policies (as outlined in the Information Security section of this report).
25. Work will be completed during 2021 and implemented in line with timescales for the reoccupation of office space, focusing in particular upon access rights (to and within buildings), how changes to these are efficiently notified and aligned with digital permissions, visitor procedure and standardisation of the access 'bundles' (co-tag, ID etc.). This will be coordinated with work to relocate the Council's headquarters to Fountain Court to ensure a 'data protection by design approach' is adopted within that project.

### ***Information Governance Framework***

26. The fourth priority was to launch the revised Information Governance Framework (IGF) to staff utilising the Council's new business change framework, achieving a level of 95% acceptance and trained.
27. The revised IGF has now been completed (as set out in the Information Strategy section of this report), however in view of the pandemic, completion of this priority was deferred to 2021, with training to be incorporated within the 'reinduction' package that employees will be required to complete before returning to the workplace following the relaxation of COVID-19 restrictions.

### ***Email***

28. The fifth priority was, in agreeing the revised email policy, to seek CMT approval for greater controls within email to reduce the risk of data breach and duplicate records (e.g. auto-deletion after agreed time period).
29. This matter was discussed in year and CMT is comfortable for controls to be applied to email in order to ensure proper records management. These will be implemented and communicated to @middlesbrough.gov.uk email users during 2021 in line with Council's transition to Microsoft Office 365.

### ***CCTV***

30. The sixth and final priority was to apply the Council's CCTV Code of Practice to all uses of CCTV and review adherence to the code across the Council's various CCTV schemes.
31. The Code of Practice was revised during the year, and significant operational changes have been made to the Council's community safety teams, including the appointment of a new Single Point of Contact (SPoC) for CCTV.
32. An internal audit of the Council's CCTV arrangements is underway at the time of writing and it is expected that the forthcoming Surveillance Policy (see the Surveillance section of this report) will recommend a number of significant changes the Council's arrangements that will be taken forward by the new SPoC.

## Information strategy progress

33. 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.
34. 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.
35. In the first two years of the strategy, the Council has focussed largely on the 'Organise' theme, updating and joining up its information governance framework (IGF). The IGF now comprises the following policies:

Policy	Last revision	Next revision
Data Protection Policy	2019	2022
Public Information and Requests Policy	2019	2021
Records Management Policy	2019	2021
Email Policy	2019	2021
Data Management Policy	2019	2022
RIPA Policy	2020	2021
CCTV Code of Practice	2020	2021
Secure Working Policy	2020	2023

36. As indicated above, the following policies were reviewed and updated during 2020:
- the RIPA Policy and CCTV Code of Practice were reviewed and updated in year as required (see the Surveillance section of this report for further detail); and
  - the Information Security Policy (now Secure Working Policy) was refreshed, integrating policies and procedures issued over recent years relating to agile working and the use of personal devices for work.
37. The following policies will be reviewed and updated where required during 2021:
- Public Information and Requests, Records Management and Email Policies (in line with the Council's transition to Office 365);
  - RIPA Policy (subsumed within a new Surveillance Policy (see Surveillance section of this report for further detail); and
  - CCTV Code of Practice (to align with the new Surveillance Policy).

## Changes to information asset registers

38. 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).
39. 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
40. This information map was reviewed at the end of 2020, with the overall RAG as set out below.

RAG	Definition	%	Change from 2019
Red	Does not meet basic requirements	5.8%	-14%
Amber	Meets basic requirements but requires improvement	42.7%	+5%
Green	Fit for purpose	51.5%	-2%

41. 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).
42. A data quality audit of Children's Services was undertaken by the Council's internal auditor during the year and yielded substantial assurance, illustrating the progress made in this area as part of the department's post-Ofsted improvement journey.
43. A significant amount of data sharing was undertaken during the year, particularly in relation to the pandemic response. This was swiftly and securely handled by all services, and should build confidence in data sharing going forward. The Council also signed the Great North Care Record - Information Sharing Agreement for Health Information Exchange: Clinical and Social Care data sets in January 2021.
44. IARs have been reconfigured into the revised management structure implemented in June 2020, and as part of the revised IGF, IAOs will be required to formally provide the SIRO with assurance on information assets and risks on an annual basis using a standard template.

## Information security

45. COVID-19 has proved 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***

46. The Committee should note that 2020 represented a significant escalation in global cyber security risk and the long-term implications of this for organisations worldwide remain unclear at this time.
47. Phishing, leading to a user's inadvertent downloading of malware and / or the exploitation of application vulnerabilities, is estimated to be responsible for 80%+ of cyber security breaches worldwide.
48. On 8 February 2020, Redcar and Cleveland Borough Council (RCBC) fell victim to a ransomware attack, resulting from a successful email phishing attempt. The ransomware used in this attack (RYUK) is sophisticated and the impact on RCBC, both in terms of the reduced ability to deliver public services for an extended period and financially, have been well-publicised.
49. The Council had a real stake in this matter as it shares a number of services with RCBC, some of which involve sharing ICT network connections. The Council's ICT Services therefore took immediate steps to remove any possible risk of infection from RCBC and to ensure that all preventative measures for RYUK were in place across the Council's estate.
50. In short, this review determined that it is almost certain that an attack of this nature on this Council would not have succeeded, due to precautions that the Council already had in place, and should it or a similar attack have succeeded, then the Council would have recovered much more rapidly due to its back-up arrangements. However, a number of improvements were implemented as a result of the review to further enhance the Council's security posture.
51. In the subsequent weeks, the Council assisted RCBC in several ways, notably by swiftly assuming responsibility for the joint Multi-Agency Children's Hub (MACH), and relocating it to Middlesbrough. During the course of the year the Council resumed responsibility for its own 'front door' into Children's Services, in line with its post-Ofsted improvement journey.
52. Senior management and services were kept fully-informed throughout this incident and a full lessons learned report was completed, with business continuity plans updated where appropriate.
53. Nevertheless, the Council must however remain vigilant. 2020 saw a step change in sophistication and targeting of phishing, including the use of fake histories, individuals' names in context, and so on, with several elected members and senior officers of this Council unsuccessfully targeted.
54. In addition to this, cyber attackers sought to take advantage of the disruption caused by the pandemic, instigating targeted hacks against organisations worldwide.
55. In December 2020, a major, likely state-sponsored, attack on the US federal government was discovered. From March 2020, attackers had exploited software from at least three US companies (Microsoft, SolarWinds and VMWare) to attack those companies' supply chains, affecting tens of thousands of organisations worldwide, including US federal departments and local governments. This was the



first time an attack of this nature had been successful, and given the sophistication of the attack it has been reported that it may take years for hackers to be completely evicted from some networks.

56. UK Government departments, many UK police forces and many organisations in the UK health sector are also known to be users of SolarWinds' compromised Orion platform, though no UK breaches have been confirmed to date.
57. In March 2021, Microsoft reported additional targeted attacks that took advantage of four 'zero-day' vulnerabilities in its Exchange Server to gain full access to email on customer systems, with tens of thousands of servers hacked worldwide as a result. This was also considered by the US Government to be a state-sponsored attack.
58. The above serves to demonstrate an increasing cyber security threat globally, and also that attacks can be equally effective on premises or in the Cloud.
59. Within that context, the Council continued to maintain a strong cyber security posture during 2020. No 'on premises' systems, 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. No new threats requiring immediate intervention were identified during the year.
60. A number of the Council's websites are managed outside of ICT Services and the technical management of these will transfer to ICT during 2021 in order to ensure cyber security as part of an overall review of the Council's websites.
61. Almost 800 mobile devices have been rolled out to former desktop users during the pandemic to enable them to work from home, with new ways of communicating and collaborating with colleagues, partners and clients rapidly introduced e.g. video conferencing.
62. 1,176 access control changes were processed during 2020/21:
  - 592 new starters (employees and agency staff) had access rights established;
  - 72 movers had access rights updated; and
  - 512 leavers had access rights removed.
63. No end-of-life devices were destroyed by the Council's contractor during 2020 due to COVID-19 restrictions. All end-of-life devices are securely stored and will be destroyed during 2021, with appropriate destruction certificates supplied.
64. Following the decommissioning of the GCSX secure email system in 2019, unencrypted traffic had reduced to 2.33% and is expected to reach zero during 2021.
65. A number of important technical improvements were delivered during the year to enhance the Council's cyber security, including:
  - the Council's firewall cluster was refreshed one year ahead of schedule to support increased home working and to enable the deployment of enhanced cyber security measures;

- Domain Name Service (DNS) traffic has been separated from the corporate and guest Wi-Fi networks to ensure any threats quickly attributed to the correct source and addressed;
- the corporate anti-virus solution was upgraded to provide improved protection, including against ransomware;
- an intrusion prevention system has now been configured and enabled to allow the Council to better detect and prevent cyber attacks;
- geo-location blocking will also be enabled during 2021, automatically blocking all traffic from territories known to be a cyber threat;
- the Council's corporate password standard moved to a minimum length of 15 characters, in line with the latest guidance from the National Cyber Security Centre;
- externals emails are now clearly marked as such to Council account users in order to promote vigilance around content and attachments;
- threat emulation has been introduced to automatically detect and block malware from email content or downloaded files;
- additional controls have been applied to end user devices to reduce the risk around the use of some applications;
- use of Microsoft Edge browser was mandated to reduce patching vulnerabilities; and
- end-of-life applications such as Adobe Flash Player have been removed from devices to reduce the risk of vulnerabilities from unsupported applications.

66. In September 2020, 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.
67. 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 2020.
68. The Council continues to subscribe to all appropriate international, national and regional cyber security networks and alert services.
69. The Council continues to participate in the Local Government Association's (LGA's) Cyber Security Stocktake (now bi-annual), and received an overall rating of 'Green' in 2018 with all recommendations from that stocktake now implemented. The LGA did not run the Stocktake in 2020 due to the pandemic but it is anticipated that this will resume in 2021.
70. The Council is seeking accreditation from the Government-backed Cyber Essentials scheme before June 2021 to provide further, external, assurance of the Council's preparedness for cyber-attacks.
71. ICT Services has implemented staffing changes during the year to improve oversight of and focus on cyber security, with monthly reviews in place. The resourcing of cyber security will be kept under regular review in line with the heightened risk in this area.

## ***Records management***

72. The closure due to the pandemic of Council buildings to the public and the majority of employees, with logging of those attending, reduced the risk to information from unauthorised access, albeit on a temporary basis.
73. At the same time the Council continued to reduce its use of paper and paper holdings through mandating clear floor and desk policies. 1,215,000 pieces of paper were removed from the Civic Centre during 2020, and a business case for archiving / digitising physical records was completed for consideration as part of the forthcoming move to new HQ accommodation.
74. Significant improvements were made to the Council's mail and print operation during the year, with controls around printing implemented and a 'mail from desktop' solution now in place.
75. A review of the Council's enterprise content management system was launched in line with the planned move to Microsoft Office 365 during 2021.

## **Data protection**

76. 2020 represented the third year of the EU GDPR, which first came into force, together with the new DPA, at the end of May 2018. At the end of the EU transition period (31 December 2020), GDPR was transferred into UK law, with jurisdiction for enforcement of the UK regulatory regime now solely invested in the ICO.
77. While there have been some changes to rules protecting the international transfer of personal data outside of the UK, the Government has largely endorsed the EU's existing security measures, such as adequacy decisions of selected data protection regimes in overseas territories such as Canada.
78. When the UK left the European Economic Area it became a 'third country' for the purposes of EU data protection. During 2020, the Council completed an assessment of EU-based ICT suppliers that cloud-host its data and sought assurances that data flows would continue after the transition period.
79. The Trade and Security Agreement with the EU has provided for a six-month grace period to allow data flows to continue back to the UK. This position will be kept under review and it is still envisaged that the UK will receive its own adequacy decision from the European Commission.
80. Work in 2020 has focussed on continuing to meet the requirements of the Council's Data Protection Policy, which was set in 2018 and mandated the approach to compliance with statutory requirements.
81. This included strengthening staff training, assisting with development of procedures for subject access requests, the development of bespoke guidance, and significant improvements and additions to the Council's suite of privacy notices.
82. A number of data protection impact assessments have been undertaken to support decisions on new, high-risk data processing and no residual high risks were accepted by the SIRO through the Council's data privacy impact assessment process.

83. The Council was notified of a number of third party data processor issues during 2020 involving cyber security breaches suffered by suppliers, including one local authority. The UK GDPR places responsibility for such incidents on suppliers, an approach that was rebalanced after the previous Data Protection Act 1998 was repealed. The Council's Data Protection Officer was kept informed about these incidents by the suppliers and monitored these situation with the Council's procurement team. No significant impacts were reported on any Council's service users.
84. Poor compliance with the rights of the data subject, such as subject access requests, in some service areas has been stabilised. Although this has been documented in the Council's strategic risk register, new effective mitigations have been implemented to reverse trend, and the situation remains under close monitoring.
85. The immediate future focus of activities will include the next phase of training and development refresh for whole scale parts of the workforce and the commencement of dashboard performance reporting on training completions. This training is considered to be critical to ensure that the improvements realised in the decreased severity of personal data breaches (outlined below) are maintained.
86. 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 £17.5million, and significant reputational damage.
87. The Council is also in the third 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, focussing efforts on the National Data Guardian Standards.
88. Incident statistics for 2020 show an increase overall and changes in the type of some incidents that are being reported. Incidents that resulted from disclosures in error increased (including those attributable to lack of 'golden records') and there was a slight increase in lost or stolen paperwork. Some of this is likely to be attributable to the very significant amount of new work required as part of the emergency response, involving personal data and multiple partners, increasing the risk of data breach through sheer volume and rapid turnaround.

Incident type	2018	Reported to ICO	2019	Reported to ICO	2020	% change in past year	Reported to ICO	% change in past year
Disclosed in error	40	3	52	2	84	+62%	0	-100%
Lost or stolen hardware	0	0	3	0	3	0%	0	0%
Lost or stolen paperwork	3	2	1	0	2	+100%	0	0%
Unauthorised access / disclosure	4	2	9	0	9	0%	0	0%
Corruption / inability to recover data	0	0	1	0	0	-100%	0	0%
Other – Breach of confidentiality	1	0	0	0	0	0%	0	0%
Other – Data quality leading to disclosure	1	0	0	0	0	0%	0	0%
Other – Building security	1	0	0	0	1	+100%	0	0%
Other – email sent to personal account	0	0	0	0	1	+100%	0	0%
Other – inappropriate use of staff portal	0	0	0	0	1	+100%	0	0%
<b>Total</b>	<b>50</b>	<b>7</b>	<b>66</b>	<b>2</b>	<b>101</b>	<b>+53%</b>	<b>0</b>	<b>-100%</b>

89. However, 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 zero incidents were reported to the Information Commissioner's Office in 2020, which is a significant achievement.

### Information Requests

90. The following table summarises statutory information requests received by the Council in 2020 and trends over the previous four years.

Request type	2016	2017	2018	2019	2020	% change in past year	% in time in 2020	% in time trend
<b>Data Protection Act 2018</b>								
Subject Access Requests	53	42	72	140	81	-42%	58%	Up
Disclosure – Crime or taxation	65	56	91	121	71	-70%	N/A	N/A
Disclosure – Immigration	0	0	0	8	20	+60%	N/A	N/A
Disclosure – Legal proceedings	10	10	12	55	6	-817%	N/A	N/A
Disclosure – Public protection	0	0	0	2	0	-100%	N/A	N/A
Disclosure – Regulatory	0	2	0	0	0	N/A	N/A	N/A
Disclosure CCTV – Crime	-	-	-	-	1,045	-	-	-
Disclosure CCTV – Legal proceedings	-	-	-	-	11	-	-	-
<b>Freedom of Information Act 2000</b>								
FOIA requests	1,229	1,266	1,343	1,360	1,032	-24%	73%	Down
<b>Environmental Information Regulations 2004</b>								
EIR requests	75	197	206	214	142	-34%	75%	Down
<b>Appeals (FOIA and EIR)</b>								
Requests to review initial responses	21	10	23	26	26	0%	77%	Up
Appeals to ICO	2	2	5	2	2	0%	50%	Down
% Appeals upheld in MBC's favour	0%	100%	50%	0%	50%	N/A	N/A	N/A
<b>Total</b>	<b>1,455</b>	<b>1,585</b>	<b>1,752</b>	<b>1,928</b>	<b>2,436</b>	<b>+26.5%</b>		

91. In summary, the number of information requests received by the Council grew by 26.5% per annum.
92. Growth during 2020 was however driven by CCTV disclosure requests, which have been added to the above statistics as a separate line following the transfer of the management of such requests from the corporate team to the CCTV unit.

93. In this and future reports, disclosures made under the 'CCTV – Crime' category will include footage that has been shared with law enforcement agencies, with those made under 'CCTV – Legal Proceedings' relating to requests from solicitors and claims handlers, largely for road traffic collisions. The significant increase in the former disclosures reflects increased joint working on crime and anti-social behaviour in line with the Mayor's strategic priority on this matter.
94. Numbers of SARs, FOI and EIR requests and fell during the year due to the pandemic, with timeliness also affected (as set out in the Implementation of 2020 priorities section of this report) but it is highly likely that these will begin to increase again during 2021.
95. During Quarter Two the Council launched the open data site, creating a single hub for all data published by the Council and accessible via the Council's website. Almost 1,000 datasets are currently available, and the Council will build on this significantly over time, looking at demand from members, customers, regulators and others.
96. The Council continues to receive a number of complex information requests regarding key programmes and projects and associated political decisions. Many requests also seek information for which elected members themselves are the data controller. During 2021, further training and guidance will be provided to members on these issues.

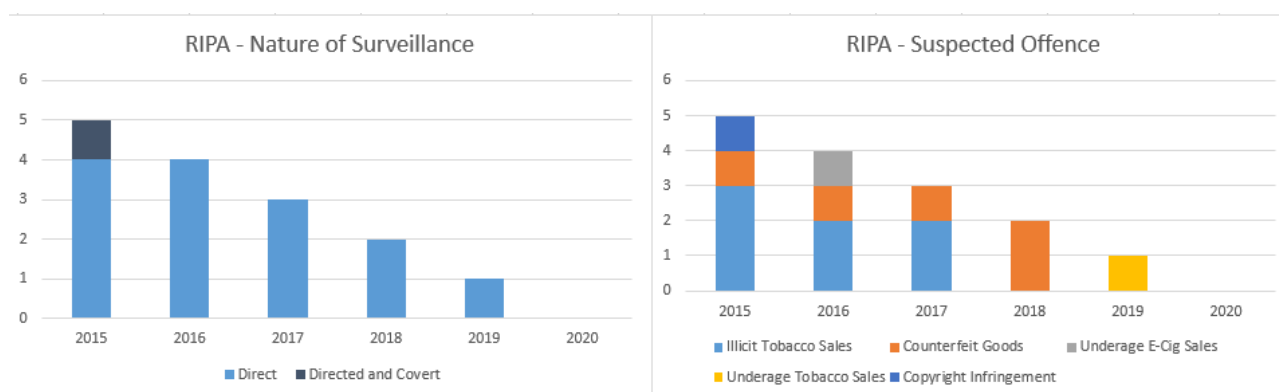
## **Surveillance**

### ***CCTV***

97. The Implementation of 2020 priorities section of this report provides an update on the governance of CCTV.

### ***RIPA***

98. 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.
99. 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.
100. The Council's use of RIPA has reduced annually since 2015, with no applications made in 2020. The charts below set out the number of applications made the Council in the past six years, the nature of the surveillance and the reasons why it was undertaken.



101. The RIPA policy is updated annually and was last approved by the Executive Member for Finance and Governance in February 2020. In late 2020 the Council was subject to a (periodic) inspection by the IPCO regarding its use of RIPA powers. The IPCO's conclusions are at Appendix 3.
102. The Council has agreed with the IPCO that from now on it will maintain an overarching Surveillance Policy, which will cover CCTV, RIPA, non-RIPA covert surveillance and the surveillance of employees. The first iteration of this policy will be presented to the Executive in June 2021 and from next year a separate annual report on surveillance will be presented to this Committee.

### Assessment of information risk

103. During 2020, taking into account the impact of the COVID-19 pandemic, the Council continued to take positive steps to enhance information governance and minimise information risk across the organisation.
104. Taking into account progress in the past year and issues and risks emerging from the global and national situation and the ongoing monitoring of the Council's information governance practice
105. The revised short-form version of the Council's information risk register is attached at Appendix 3, with the risk RAG-rating amended where appropriate to reflect the revised Risk and Opportunity Management Policy approved by the Executive in February 2020.
106. In overall terms, the Council's risk profile is broadly stable, but (as set out within the report) the Council needs to maintain vigilance in relation to cyber security, as well completing activity to permanently mitigate risks relating to breach of data rights and unauthorised access, and compliance with surveillance law.
107. Deferred from 2020, 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 2021**

108. Key priorities for 2021 to address the issues and risks outlined in this report are therefore as follows:

- continue monthly monitoring of the Council's cyber security posture and improvements and undertake a staff phishing exercise;
- implement the outstanding recommendations from the ICO Consensual Data Protection Audit;
- launch the Council's revised Information Governance Framework to staff as part of the post-pandemic reinduction process, and enhance elected member training on information governance;
- continue to improve the Council's responsiveness to information requests through the provision of real-time dashboards for senior managers;
- agree physical security policy and procedures for the Council's office estate, implementing changes for reinduction and advising on design of the Council's new HQ;
- agree a position in respect of digitising or rehousing the Council's historic papers records as part of the new HQ project;
- complete and implement the revised Surveillance Policy and actions from forthcoming audit of CCTV; and
- ensure that key ICT projects for 2021 including the migration to Microsoft Office 365 and the review of the Council's website are aligned with the Information Governance Framework and progress the aims of the Council's Information Strategy.

## **Key messages for staff**

109. 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 photocopyers.



- 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) 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?**

110. 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?**

111. 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**

112. Not applicable.

#### **Impact(s) of recommended decision(s)**

##### **Legal**

113. 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**

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

## **Policy Framework**

115. 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**

116. Not applicable.

## **Risk**

117. 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)**

118. 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 ICO Follow-up data protection audit report
- Appendix 2 IPCO Inspection
- Appendix 3 Summary Information Risk Register at end 2020

## **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 |

**Contact:** Paul Stephens, Head of Strategy, Information and Governance  
**Email:** [paul\\_stephens@middlesbrough.gov.uk](mailto:paul_stephens@middlesbrough.gov.uk)

# Middlesbrough Council

## Follow-up data protection audit report

December 2020

# Executive summary



## Background

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 original audit took place at Middlesbrough Council's premises in December 2019 and covered the following scope 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.

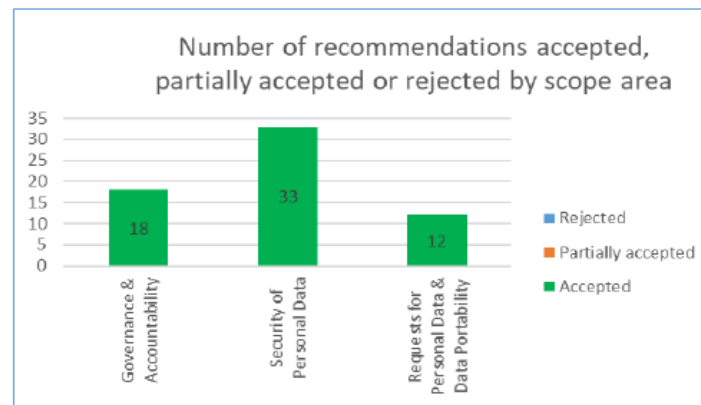
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this were a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

Where weaknesses were identified recommendations were made, primarily around enhancing existing processes to facilitate compliance with the DPA.

63 recommendations were made in the original audit report. In order to assist Middlesbrough Council in implementing the recommendations each was assigned a priority rating based upon the risks that they were intended to address. The ratings were assigned based upon the ICO's assessment of the risks involved.

Middlesbrough Council responded to these recommendations positively, agreeing to formally document procedures and implement further compliance measures.

The below chart summarises Middlesbrough Council's response to the recommendations made.



## Follow-up process

The objective of a follow-up audit assessment is to provide the ICO with a level of assurance that the agreed audit recommendations have been appropriately implemented to mitigate the identified risks and thereby support compliance with data protection legislation and implement good practice.

For all Urgent and High priority recommendations made in the original audit report, Middlesbrough Council are required to provide an update on the actions they have taken with supporting documentation to evidence progress.

For all Medium and Low priority recommendations made in the original audit report, Middlesbrough Council are required to provide an update on the actions they have taken.

The updated Action Plan should be signed off at Board Level.

## Follow-up audit summary

A desk based follow-up took place in December 2020 to provide the ICO and Middlesbrough Council with a measure of the extent to which Middlesbrough Council had implemented the agreed recommendations. The following charts show a summary of progress to date.



## Key follow-up audit findings

Main improvements include:

- Middlesbrough Council has increased its oversight of data protection matters by implementing new procedures such as standard risk management agenda items on meeting agendas, and increased monitoring and compliance checks on records management.
- Staff involved in responding to subject access requests have been provided with specialised training for their roles.
- A Secure Working Policy has been developed and implemented, and content from the historic Information Security Policy has been reviewed and captured within appropriate policies and procedures.

Main risk areas still outstanding:

- Procedures for the handling of Subject Access Requests (SARs) have only been created for Children's Services, which receives the majority of requests. Middlesbrough Council should continue to create procedures for its outstanding service areas to ensure that all staff have procedures to refer to in the event they receive a SAR.
- Middlesbrough Council have not completed its project to identify and manage risks associated with its current physical security environment and access control procedures. The Council should continue to work on this project as soon as possible so any physical security risks, particularly those relating to unauthorised access, are identified and controlled as appropriate.
- Action has not been taken to gather assurance from staff that they have read and understood the Council's data protection policies and procedures. Staff sign off processes should be implemented to gain assurance that policies and procedures have been read and understood.



## Follow-up audit conclusion

The follow-up is now complete. Some outstanding actions exist, but meaningful progress is being made with the remaining actions to mitigate the risk of non-compliance.

# Credits

---



### ICO Auditor

Eve Wright – Lead Auditor

### Thanks

The ICO would like to thank Michael Brearley (Data Protection Officer) for their help in the audit follow up engagement.

### Distribution List

This report is for the attention of Paul Stevens (Head of Strategy Information and Governance) and Michael Brearley (Data Protection Officer).

## Disclaimer

The matters arising in this report are only those that came to our attention during the course of the follow up 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 follow up 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 solely for the use of Middlesbrough Council. The scope areas and controls covered by the original audit were tailored to Middlesbrough Council and, as a result, this report is not intended to be used in comparison with other ICO follow up audit reports.

## Appendix 3: IPCO Inspection of MBC

OFFICIAL

# IPCO

Investigatory Powers  
Commissioner's Office

PO Box 29105, London  
SW1V 1ZU

Mr. Tony Parkinson  
Chief Executive  
Middlesbrough Borough Council  
PO Box 500  
Middlesbrough  
TS1 9FT  
[Claire\\_jones@middlesbrough.gov.uk](mailto:Claire_jones@middlesbrough.gov.uk)

6 January 2021

Dear Mr. Parkinson,

### Inspection of Middlesbrough Borough Council

*Please be aware that IPCO is not a "public authority" for the purpose of the Freedom of Information Act (FOIA) and therefore falls outside the reach of the FOIA. It is appreciated that local authorities are subject to the FOIA and that they may receive requests for disclosure of our reports. In the first instance the SRO should bring the matter to the attention of the IPCO Data Protection Officer (at: [info@ipco.org.uk](mailto:info@ipco.org.uk)), before making any disclosure. This is also the case if you wish to make the content of this letter publicly available.*


Your Council was recently the subject of a telephone and desktop-based inspection by one of my Inspectors, Mr. Graham McCrory MBE. This has been facilitated through your Senior Responsible Officer (SRO), Head of Strategy, Information and Governance – Mr Paul Stephens and Deputy SRO, Governance and Information Manager – Ms. Anne-Marie Johnstone, both of whom were interviewed on the telephone. My Inspector is most grateful to Ms Johnstone for providing the supporting information required, as well as her professional approach to the inspection.

The information provided has demonstrated a level of compliance that removes, for the present, the requirement for a physical inspection.

The last inspection was undertaken by IPCO Inspector, Mr Paul Donaldson, in January 2019. No recommendations were necessary on this occasion.

The authority has continued to develop strong compliance regimes under the leadership of Mr Stephens and Ms Johnstone.

Mandatory refresher training schedules have been created with 'E learning' modules completed by staff within enforcement and public protection roles. Units identified as requiring additional training or departments utilising social media, have received bespoke inputs and appropriate guidance.

 0207 389 8900

 [info@ipco.org.uk](mailto:info@ipco.org.uk)

OFFICIAL

 @IPCOOffice

 [www.ipco.org.uk](http://www.ipco.org.uk)

Only one authorisation, for directed surveillance, has been undertaken since the last inspection. Whilst the Council is not a frequent user of the covert powers available it is recognised that staff, normally deployed on enforcement duties, have been concerned in dealing with matters relating to the current Covid-19 pandemic rather than developing covert operations.

Your RIPA policy has been refreshed, as is the case on an annual basis, with my Inspector offering to review forthcoming additions which outline procedures for the use of covert tactics in investigations which do not attract RIPA authorisation. The processes, discussed during the inspection, should give clear guidance to your staff and have been formed 'in the spirit' of RIPA with checks and balances in place to document events and decisions made.

Oversight takes place in the form of regular Risk Management Group (RMG) meetings to assess ongoing issues, with this group's findings feeding into the quarterly meeting of the Corporate Governance Group (CGG), attended by various Directors, including the Director of Legal Services.

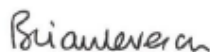
A specific focus for the inspection was the retention and destruction of data gathered whilst utilising the covert powers. I note that your SRO and his deputy are alive to this issue. Your Council has an Electronic Document Records Management System (EDRMS) which allows for the electronic audit of documents retained and the setting of review and destruction schedules. The application of this process, to review material gathered utilising covert powers, is an excellent advance and should allow your staff to comply with the safeguards as documented within the codes of practice for surveillance and CHIS. I trust you will find the details within my additional letter, sent to your SRO, of benefit. Ultimately, it will be for your SRO to ensure the requirements within the letter are addressed.

There is no doubt that your SRO and deputy SRO have been instrumental in developing a strong ethos of compliance within your Council. It is commendable that this has included regular training, oversight and updating of the relevant policies and procedures.

My Office is available to you should you have any queries following the recent inspection, or at any point in the future. Contact details are provided at the foot of this letter.

I shall be grateful if you would acknowledge receipt of this letter within two months.

Yours sincerely,



**The Rt. Hon. Sir Brian Leveson**  
The Investigatory Powers Commissioner

### Appendix 3: Summary Information Risk Register at end 2020

Category	Risk	Current score <sup>1</sup>	Trend	Target score
Internal	Breach of data rights due to untimely response to information requests	20	Same	10
Internal	<b>REVISED</b> Lack of employee and customer golden records	20	Up	6
Internal	Non-compliance with PoFA 2012 (CCTV provisions)	20	Up	5
Internal	<b>REVISED</b> Unauthorised access due to tailgating / break-in / inaccurate records	20	Same	3
Communication	Loss of sensitive data by human error	15	Same	6
External	Loss of personal data from cyber attack	14	Up	7
Internal	Non-compliance with information law, including GDPR	14	Same	7
Internal	Non-compliance with Baseline Personnel Security Standard	14	Same	7
Internal	Breach caused by third party processor	10	Down	10
Internal	Internal misuse of data	10	Down	10
Internal	Ineffective staff training	9	Same	6
Internal	<b>NEW</b> Misfiled historic records	9	-	3
Technical	Failure of disaster recovery	7	Same	6
Technical	Unauthorised access due to ICT not being notified of movers / leavers	6	Same	6
Internal	Non-compliance with Payment Card Industry standard	6	Same	3
External	<b>NEW</b> Interrupted data flows in to and from the European Union, post-Brexit	6	-	3
Internal	Non-compliance with NHS Data Security and Protection Toolkit	5	Same	5

<sup>1</sup> 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
Internal	Insecure disposal of records	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 PSN standard	5	Same	5
Internal	Non-compliance with RIPA 2000	5	Same	5
Technical	Encryption failure	2	Same	2
Technical	Insecure disposal of hardware	2	Same	2