MIDDLESBROUGH COUNCIL	Middlesbrough moving forward

CORPORATE AFFAIRS AND AUDIT COMMITTEE

Report title	Annual Report of the Senior Information Risk Owner
Director	Strategic Director of Finance, Governance and Support
Date	8 February 2018
Purpose of the report	To advise the Committee of arrangements in place to ensure the proper governance of information within the Council, progress made within the next past year, risks and issues arising, and priorities for the next 12 months.
Summary of the report	The Council continues to take steps to implement effective information governance arrangements across the organisation. In summary, current arrangements are largely satisfactory in relation to *current* legal requirements, but a significant amount of work is required within a short-time frame to ensure preparedness for the General Data Protection Regulation, which will override current data protection law from 28 May 2018. This work is now underway, and resources are available to support delivery.
If this is a confidential report, which exemption(s) from the Schedule 12a of the Local Government Act 1972 applies?	Not applicable.
Decision(s) asked for	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.
Impact of decision(s)	The decision will allow the Committee to fulfil its remit in relation to information governance. The activity outlined in the report will result in significant improvements in the Council's information governance arrangements.
Contact:	Paul Stephens, Head of Strategy, Information and Governance

What is the purpose of this report?

1. To advise Corporate Affairs and Audit Committee of arrangements in place to ensure the proper governance of information within the Council, progress made within the next past year, risks and issues arising, and priorities for the next 12 months.

Why is this report necessary?

2. This report aims to provide assurance to the Committee that information governance policy and practice within the Council is in line with legal obligations, and consistent with the principles of good governance.

What is Information Governance?

3. The Council holds a significant amount of information about Middlesbrough and its residents. In line with its forthcoming Information Strategy, it will continue to ensure that the right information is made available to the right users (including local communities and our partners) at the right time, to support the achievement of its aims and priorities.

4. Information Governance (IG) is the framework of law and best practice that regulates the manner in which information (including personal information) is managed, from creation to destruction.

Legal obligations

5. The Council is subject to a range of legal obligations in relation to IG, most notably under the Data Protection Act 1998 (DPA), Freedom of Information Act 2000 (FOI), and the Environmental Information Regulations 2004 (EIR).

6. Under the DPA, the Council must ensure that personal and sensitive personal data, in any format, is:

   - used fairly and lawfully;
   - used for limited, specifically stated purposes;
   - used in a way that is adequate, relevant and not excessive;
   - accurate;
   - kept for no longer than is absolutely necessary;
   - handled according to people's data protection rights;
   - kept safe and secure; and
   - not transferred outside the European Economic Area without adequate protection.

7. The Information Commissioner's Office (ICO) is the supervisory body for data protection, and can levy fines of up to £500,000 for infringement of the above principles.

8. The law provides for a range of information access rights. The DPA enables individuals to see a copy of the information an organisation holds about them, and be advised of how this used. These Subject Access Requests (SARs) must be responded to within 40 days. Requests for disclosure of information under the DPA can also be made from (for example) the police or the courts (Section 29, 31 and 35 requests).

9. Both the FOI and EIR provide public access to information held by public authorities. Requests under both must be responded to within 20 days. For all requests, a range of exemptions may be applied.

10. The 2008 O'Donnell Review of *Data Handling Procedures in Government* places a range of requirements the Council on to ensure the proper governance of information. It was this review that established the role of Senior Risk Information Owner (SIRO) for public bodies. The SIRO must provide written advice on information risk for inclusion within the organisation's Annual Governance Statement. It is common practice for the SIRO to prepare annual report to the Chief Executive and any other boards / bodies within an organisation with an interest in information governance and information risk.

11. In addition, as a partner to the NHS, the Council must comply with the Department of Health and Social Care's Information Governance Toolkit, which draws together the legal rules and central guidance set out by DH&SC policy and presents them in in a single standard as a set of information governance requirements.

12. The legal framework for data protection will be updated with the advent of the European Union's General Data Protection Regulation (GDPR), which will come into force on 25 May 2018, replacing existing EU directives and overriding the DPA. GDPR provides the following rights for individuals, which will bring significant impacts for all data 'controllers' and 'processors':

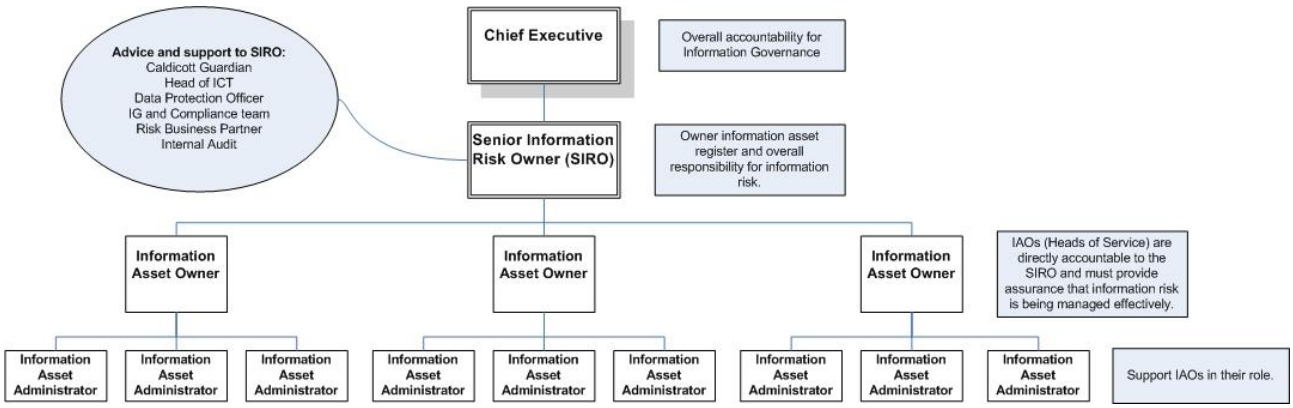
    - The right to be informed
    - The right of access
    - The right to rectification
    - The right to erase
    - The right to restrict processing
    - The right to data portability
    - The right to object
    - Rights in relation to automated decision making and profiling.

13. A controller determines the purposes and means of processing personal data. The work of the Council involves several discrete data controllers, all of whom have individual legal responsibilities under GDPR: the Council as a corporate body; elected members; the Local Safeguarding Children Board; the Local Safeguarding Adult Board; the Youth Offending Team; the Electoral Registration officer; and Registrars. A processor is responsible for processing personal data on behalf of a controller – this can be either in-house or contracted to third parties. It is anticipated that all services will take a common approach to GDPR requirements.

14. Under GDPR the potential size of potential fines increases significantly, from £500,000 up to €20m for serious breaches. The Council needs to redouble efforts to avoid breaches in future wherever possible. Like all applicable organisations, the Council will need to take steps to build on its existing processes if it is to ensure continued compliance with data protection law as reflected in GDPR.

Information Governance Framework

15. *Data Handling Procedures in Government* is the basis of the Council's IG Framework, under which all corporate information assets are managed under the following structure, incorporating key information roles within the organisation.



16. The Council has in place a range of policies and procedures to promote compliance with the law and best practice in relation to IG. These are published on the Council's intranet, and will be reviewed in line with GDPR. All staff with access to a device are required to undertake mandatory IG training as part of their induction process. This training was recently refreshed, and has been completed by 2,070 employees and partners. While further work is required to confirm this, it is understood that this numbers covers the majority of device users in the Council. In addition to this, managers are supported to train those staff without access to a device.

Compliance, risks and issues in 2017

17. The Council submitted its self-assessment against v.14 of the IG Toolkit to NHS Digital in March 2017. On review, arrangements were assessed as 'satisfactory, with improvement plan' at 67%. Half of North East councils have achieved a reviewed overall 'satisfactory' rating to date. The key area for improvement for the Council relates to the use of NHS numbers in all applicable systems. Work is now ongoing, particularly in Adult Social Care to ensure that at least 90% of care records include the client's NHS number. The Council will make its 14.1 IG Toolkit submission by the end of March 2018. The Data Security and Protection Toolkit will replace the current IG toolkit from April 2018.

18. Work such as this is driven by the Council's Information Governance and Compliance team. During 2017, the team has focused on updating policy, practice and communication tools in anticipation of GDPR.

19. In September 2017, LMT agreed the development of a new 'asset based' Information Strategy, supported by digital solutions, to allow the Council to fully exploit its data in pursuit of its strategic objectives. In support of the development and implementation of this strategy, all IG functions were transferred to the then Head of Performance and Partnerships (now Head of Strategy, Information and Governance) who was also designated as SIRO. Both the SIRO and a designated deputy have now been trained to the level required by the IG Toolkit.

20. Following transfer, TVAAS was commissioned to undertake a review of GDPR preparedness by the new SIRO, with findings to be reported to a future meeting of this Committee. Since this review was commissioned, a project plan for GDPR has been put in place, supported by a multi-disciplinary team. The majority of the remaining recommendations from the review will be addressed in the delivery of this project. In addition, a dedicated Data Protection Officer was appointed in December 2017, with the postholder to lead on this issue, and commencing work from mid-March 2018 onwards.

21. In May 2017, parts of the NHS experienced the 'WannaCry' ransomware attack. The attack exploited a weakness in operating systems that had been previously identified by the supplier and a patch issued, however some organisations had failed to apply the patch or had applied it incorrectly. During the attack, the Council's ICT team assessed the risk to the Council and took steps to further mitigate the likelihood of a successful attack on the Council's network, which had the patch correctly applied. Significant work has also been undertaken in the year to improve the Council's disaster recovery capability. In addition, work has been undertaken in 2017 to embed the approach to privacy impact assessment required under GDPR for all new systems, with nine completed in the year. The Head of ICT Services has provided assurance of the Council's compliance with the National Cyber Security Centre's '10 Steps to Cyber Security' guidance. Further work will be undertaken in 2018 to assess cyber security risks in relation to infrastructure and current and planned applications.

22. During 2017 calendar year, 48 data protection incidents were reported to the Information Governance and Compliance team for investigation, compared with 52 in 2016. Of these, four were reported to the ICO because it was judged that they met the reporting threshold, compared with one in 2016. Those incidents comprised two instances of data posted to the incorrect recipient, one theft of paperwork from a third party provider to the Council, and one cyber security misconfiguration. None of these were acted upon by the ICO. The total incidents break down as follows:

Incident type	Total	Reported to ICO
Data posted / faxed to incorrect recipient	13	2
Data sent by email to incorrect recipient	13	0
Loss / theft of paperwork	6	1
Other principle 7 failure	6	0
Verbal disclosure	5	0
Cyber security misconfiguration	2	1
Cryptographic flaws	1	0
Loss / theft of only copy of encrypted data	1	0
Failure to redact data	1	0
Total	**48**	**4**

23. To put the above into context, during 2016/17 around 2,400 incidents were reported to the ICO across all sectors, a 26.5% increase on the previous year, with nine incidents resulting in a financial penalty. 10.3% of incidents were received from local government, a slight rise from the previous year. This, and the Council's understanding of the position within neighbouring local authorities, suggests that the Council is disproportionately represented in the ICO's data, and this issue will be reviewed further in 2018.

24. The great majority of all reported incidents are due to human error, rather than cyber attack or common theft – over 50% of incidents within the Council were the result of data being incorrectly sent to the wrong recipient. Information on common breach causes has been used to create the 'Information Governance is ACE' campaign to all staff. To date, this video has been viewed 700 times.

25. Implementation of the Council's forthcoming Digital Strategy will provide opportunities to reduce such human error considerably, not least through the reduction in paper records. The Council currently has over 20m sheets of paper archived at several different locations. Though there is limited concern while this material is at rest, the

ongoing reconfiguration of the Council's operational estate means that much of the material is likely to be in transit over the next year. This will need to be carefully managed. Retention schedules and the forthcoming scanning strategy will see this volume of records diminish over time.

26. The following table summarises information requests received by the Council in 2017.

Request	2016	2017	% change	% in time
Data Protection Act 1998				
SARs	53	42	-20%	69%
S.29 requests	65	56	-14%	N/A
S.31 requests	0	2	N/A	N/A
S.35 requests	10	10	0%	N/A
Freedom of Information Act 2000				
FOI requests	1,229	1,266	+3%	96%
Requests to review initial responses	21	10	-52%	60%
Appeals	2	2	0%	100%
Appeals upheld	0	TBC	TBC	N/A
Environmental Information Regulations 2004				
EIR requests	75	197	+162%	100%
Total	**1,455**	**1,585**	**+9%**	

27. There is no national benchmarking data on numbers of information requests received by local authorities, but as many are sent to all or groups of local authorities, it is reasonable to assume that the numbers received by the Council is not uncommon. Overall, the number received by the Council rose by 9% in 2017, largely attributable to the significant increase in EIRs relating to certain land and property transactions involving the Council.

28. The volume of information requests places a considerable burden on all of those involved in responding to them. Despite this, the timeliness of responses to FOI and EIR requests exceeded the current UK Government average. SARs and FOI reviews are historically less timely due to the level of complexity involved. The focus going forward will be to reduce the number of requests by proactively publishing commonly requested information on the 'Open Data' section of the Council's website.

29. In view of the above-stated position, a short-form version of the current IG risk register is set out below.

Category	Risk	Current score[1]	Target score
Internal	Breach caused by third party processor	15	10
Internal	Insecure disposal of records	15	10
Internal	Internal misuse of data	15	10
Communication	Loss of sensitive data by human error	15	6
External	Cyber attack	15	5
Internal	Non-compliance with IG law	14	7
Internal	Non-compliance with Baseline Personnel Security Standard	14	7
Technical	Disaster recovery	14	6

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

Category	Risk	Current score	Target score
Technical	Vulnerabilities in third party applications	10	10
Technical	Unsupported infrastructure / applications	10	10
Internal	Non-compliance with Payment Card Industry standard	10	10
Internal	Lack of employee golden record	9	6
Internal	Ineffective staff training	9	6
Internal	Non-compliance with IG Toolkit	5	5
Technical	Unauthorised access due to incorrect security settings	5	5
Technical	Patching failure	5	5
Technical	Insecure disposal of hardware	5	5
Internal	Non-compliance with Public Services Network standard	5	5
Technical	Encryption failure	2	2

30. In summary, current arrangements are largely satisfactory in relation to *current* requirements, but a significant amount of work is required within a short-time frame to ensure preparedness for GDPR. This work is now underway, and resources are available to support delivery.

Priorities for 2018

31. Over the coming 12 months, the clear priority from an IG perspective will be to ensure that plans to ensure compliance with GDPR are effectively implemented and communicated, focusing on updating policies and procedures, and staff training. The Member Development Committee will be asked to consider whether, given their status as data controllers, all elected members should be required to undertake mandatory information governance training.

32. Once in post, the Data Protection Officer will assume responsibility for this work, reporting to the SIRO. In the interim, work will be led directly by the SIRO. It is anticipated that the Council will need to report progress to the ICO and other regulators such as the Care Quality Commission during the year, and TVAAS will undertake a follow-up review as part of the 2018/19 Audit Plan.

33. This activity is key to addressing the principal information governance risk currently facing the Council. The information risk register will be fully updated in 2018 in line with the output from work on GDPR, and the review of cyber security arrangements outlined above.

34. Alongside this, work will continue to develop and implement a new Information Strategy for the Council, supported by a restructured Strategy, Information and Governance service.

35. A review of data protection breach investigations will be undertaken and lessons disseminated across the organisation. Plans within the Council's forthcoming Digital Strategy, including an upgrade of the Council's Electronic Document and Records Management System and the implementation of digital mail and the scanning strategy, will do much to eliminate incidents arising from human error.

36. Management information relating to information requests will be improved significantly, and used to inform the proactive publication of datasets to reduce the burden of response on the organisation.

What decision(s) are being asked for?

37. 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?

38. 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

39. Not applicable.

Impact(s) of recommended decision(s)

Legal

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

Financial

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

The Mayor's Vision for Middlesbrough

42. Information Governance is fundamentally integrated with service and financial performance. Effective IG therefore underpins the delivery of the Council's three core strategic aims, contributing to the delivery of the Vision for Middlesbrough.

Policy Framework

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

Wards

44. Not applicable.

Equality and Diversity

45. Not applicable.

Risk

46. 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)

47. Not applicable.

Appendices

Not applicable.

Background papers

No background papers were used in the preparation of this report.

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