Audit Committee – 13 March 2017

Information Governance Annual Report: Full Report

Recommendation

1. That the Audit and Standards Committee considers the Annual Information Governance Report and notes the work ongoing to manage the County Council's information assets with regard to legislative and regulatory requirements.

Report of the Director of Strategy, Governance and Change

Background

2. Information Governance is the term used to describe how the Council manages its information assets particularly with respect to legislative and regulatory requirements. This report seeks to provide assurance around the policies, processes and practices employed to ensure we meet those requirements.

3. There is a comprehensive and complex legal and regulatory information landscape within which the County Council must operate including compliance with the Data Protection Act 1998, Freedom of Information Act 2000, Environmental Information Regulations 2004 and other statutes. In addition to this, there are a number of further requirements contained within codes of practice and regulations dealing with a range of service provision. Compliance with this range of legislation is monitored and administered through various national commissioner roles including the Information Commissioner, Surveillance Commissioner and Interception of Communications Commissioner. These commissioners have powers to impose significant penalties, including monetary penalties and custodial sentences on organisations or individuals who breach these rules.

4. The County Council has adopted and promoted an Information Governance Framework which collates requirements, standards, policy and guidance on the Council intranet pages. This provides for a strategic direction in terms of managing information and provides detailed guidance and support for staff in using information, including sharing and working with partners. This is particularly important as we continue to share information with partners to provide better and more efficient services across Staffordshire.

Transparency

5. The County Council has statutory obligations to publish data as required by the Inspire Directive and the Local Government Transparency Code 2014. Publishing under this code will give's the public access to information about local authorities' assets, contracts and financial spend as well as providing detail on senior officers roles and salaries. In 2016 the County Council now also publishes data regarding tenders with a value of £25000 and over, in line with procurement regulations.

Freedom of Information

6. Published statistics have shown that nationally the number and complexity of Freedom of Information requests submitted to Local Authorities remains high and overall the amount of time consumed in administering the requests continues to increase. The Council continues to mirror the national picture with the volume of requests increasing. The Council has a robust system in place for dealing with FOI requests. However as request numbers remain in excess of 4000 a year, this places a greater challenge to remain compliant within the statutory deadline of twenty days. Failure to meet statutory requirements in this area is monitored by the Information Commissioners Office (the ombudsman for information legislation).

7. Performance in SCC is monitored on a quarterly basis and published on the internet. The benchmark set by the Information Commissioner for an acceptable service is 85% of requests answered with 20 days, for 2016 SCC maintained a 95% rate against the 20 day target. Freedom of Information statistics can be found at Appendix A.

8. We publish a selection of questions and answers under FOI, based on the nature of requests and to potentially negate the need for duplicate requests. In doing this, we can simply refer requestors to the website rather than responding to a request we have already published, therefore saving staff time and resources.

9. In 2015/16 the Freedom of Information Act was subject to a review by the Independent Commission on Freedom of Information ("the Commission") and it was their opinion that the Act is generally working well, and that it has been one of a number of measures that have helped to change the culture of the public sector. It has enhanced openness and transparency. The Commission considered that there is no evidence that the Act needs to be radically altered but made several recommendations including that the right of access should be increased and a reduction in the delays in the process. This has yet to be implemented by parliament but may lead to additional requirements in future years.

Data Protection

10. Data protection is primarily concerned with personal data about individuals rather than general information as covered by Freedom of Information legislation. As a public body with a diverse range of people services this relates to a significant volume of data. As service delivery and commissioning evolve the way in which SCC is delivering its services has an impact on information governance arrangements. The Information Governance Unit is working together with all partners on projects and initiatives which require sharing personal information on a large scale to ensure that it meets statutory obligations and is completed securely.

11. Central to information sharing is the on-going use of the One Staffordshire Information Sharing Protocol. Information sharing protocols are agreements that establish mutually binding rules for the safe and appropriate sharing of personal information between different agencies. The County Council took the lead on establishing this single agreement signed by over 173 public sector bodies across Staffordshire who are committed to effective

information sharing. The County Council lead on the management of the Protocol including a full review in March 2016 to ensure that the protocol is up to date and fit for purpose.

12. The authority is committed to partnership in terms of safe and strong communities. Under section 29 of the Data Protection Act 1998, the Police and other agencies, are able to request a data controller, to waive an individual's rights to have their personal data protected, for the purposes of prevention and detection of a crime and investigation of taxation. The County Council has signed up to a national protocol to expedite Police and CPS requests for information in child safeguarding investigations known as Annexe C requests. We have committed that an Annex C request under the protocol will be answered within fourteen days, in practice this is often done within seven days. Although at times this can place a strain on resources it evidence of our commitment to give the highest priority to such matters.

13. The General Data Protection Regulation (GDPR) was adopted into European law in April 2016. The GDPR aims to strengthen consumer protection and enhance trust and confidence in how personal data is used and managed, giving citizens more control over their own private information. In addition, the GDPR provides important new safeguards, including new fines of up to 4% of an organisation's annual global turnover, or €20 million, in the most serious cases of breaches of the regulation. As a regulation, it will directly apply to all European Union member states from 25 May 2018 and as the UK will still be in the EU at that time the UK Government has stated that the GDPR will be adopted directly into UK law, superseding the Data Protection Act 1998 with new legislation.

14. The County Council has already undertaken some preparatory work to understand the impact of GDPR on the organisation and a substantial work programme will take place throughout 2017 to ensure that the County Council is compliant with the new requirements.

Information Security

16. Local Authorities continue to face challenges to ensure that appropriate cyber security is in place therefore the County Council remains focussed on working towards ensuring that resilient procedures are employed across the Authority.

17. The authority continues to be subject to a high-level of cyber-attacks. It is not believed that the authority is being specifically targeted but more as an inevitable consequence for any organisation that has a high level of activity on the internet. In particular denial of service attacks have seen an increase both directly attacking the Authority's network but also that of our Internet Service Provider and this can lead to significant disruption to the network. An increase in malware email campaigns (software which is specifically designed to disrupt or damage a computer system) has led to limits being placed on downloading executable files. Blocked traffic is monitored and a breakdown of blocked malicious and threat emails are in Appendix B. In 2016 SCC systems dealt with over 750,000 security events of varying threat levels.

18. The Council has developed a Cyber Security Incident Plan in case of a cyber-attack and a desk top exercise was carried out in 2016 to test the plan. Work is ongoing to review the plan due to the outcomes identified by the exercise.

19. The Council continues to invest in appropriate software and hardware to combat security threats and also works closely with its Internet Service Provider to improve its security and to ensure the earliest possible waning of cyber-attacks. The firewall hardware and software continues to provide protection to our network.

20. As an organisation we are committed to ensure that we only use legitimate software for which we hold a valid licence. Hosting unlicensed software is illegal and can lead to monetary penalties. A software auditing tool to ensure that there are no instances of unauthorised software with the SCC network and that all instances are licensed.

21. The Information Governance Unit record all reported security incidents and investigate where necessary. Security incidents include both physical and electronic data. All incidents will be followed up with the appropriate manager to receive assurance from the service that recommendations have been implemented. The security incidents are also reported quarterly to the Senior Information Risk Officers.

22. All security policies are regularly reviewed to reflect changes in technology and knowledge of potential threats; this involves revision of policies and also technical improvements to software, hardware and networks on an ongoing basis.

23. Staffordshire County Council has successfully been granted Public Services Network (PSN) accreditation for 2017. PSN is a key part of Government ICT Strategy and accreditation means that the authority can continue access a secure network that facilitates the safe access of Government shared services. Accreditation is an annual requirement. The safety of PSN is paramount and to achieve accreditation the authority had to satisfy a Code of Connection containing over 60 different security controls. The security control responses were audited by means of independent ICT security health checks and an onsite assessment conducted by a government accredited third party auditor.

Governance

24. Governance of information requirements is provided through the Corporate Governance Group, Information Governance Unit and Senior Information Risk Owners (SIRO).

25. The role of SIRO is to foster a culture of best practice in how the organisation uses, shares and keeps information, and to own the risk policies and procedures for managing information. In 2016 SIROs were appointed for Families and Communities and Economy, Infrastructure and Skills to ensure that there are representatives across the authority. In Health and Care a Caldicott Guardian fulfils that role.

26. The SCC Information Asset Register (IAR) identifies information that enables the organisation to perform its business functions and all rules associated with the management of that information. The IAR is intended to be a resource for managers and to inform decision-making about the management of our information assets in order to mitigate information risks. In 2016 work was undertaken to develop and implement a comprehensive risk assessment framework to be applied to the assets that have been identified.

27. The NHS IG Toolkit is an online system which allows organisations to assess themselves or be assessed against Information Governance policies and standards. The NHS require the County Council to be compliant with the toolkit to enable integrated working between the County Council and NHS bodies, including connection to systems and the transfer and sharing of sensitive personal data. In 2016 Public Health passed the requirements, building on this success work is currently ongoing to obtain compliance to the latest local authority version of the toolkit for the whole County Council.

Training and Guidance

28. All new starters are expected to complete the Privacy e-learning module as part of the induction process. All staff can complete a suite of Information Governance e-learning modules including Freedom of Information, Data Protection, Information Security, Records Management, Protective Marking and Privacy. The modules are reviewed at least annually to ensure information is current and reflects regulations and procedures and the modules have been classified as 'essential'.

29. A review of the completion of e-learning was undertaken in 2016 where the numbers of people undertaking the modules was deemed to be insufficient. The Senior Leadership Team have approved the introduction of mandatory training to be implemented to all staff in 2017.

30. In 2016 new guidance was produced to assist all staff with Information Governance considerations for smart working. This is available to all staff via the SCC intranet.

Regulation of Investigatory Powers Act

31. Staffordshire County Council is entitled to use the Regulation of Investigatory Powers Act for carrying out covert surveillance as part of our statutory duties. All applications for surveillance must be approved by a Magistrate. In 2016 no Directed Surveillance applications were made. No operations involving Covert Human Intelligence Sources were undertaken.

32. Access to Communications Data from communication are processed by the National Anti-Fraud Network (NAFN). In 2016 Two Access to Communications Data applications approved and no applications were rejected. These requests are still subject to the Magistrate approval process.

33. There is a regulatory obligation to report the outcome of any Surveillance Commissioner Inspections to members. No Commissioner inspections took place in 2016.

34. The Surveillance Camera Commissioner requires the completion of a self-assessment tool by local authorities operating CCTV systems. This was completed and returned in 2016.

Equalities Implications

35. There are no direct implications arising from this report.

Legal Implications

36. Failure to comply with legislation or legal requirements (i.e. Data Protection Act, Regulation of Investigatory Powers Act) can result in external censure, financial loss (including fines and compensation) and reputational damage.

37. Failure to comply with the Regulation of Investigatory Powers Act can result in censure by the Surveillance Commissioner, including reporting to Parliament, and judgement by the Investigatory Powers Tribunal.

Resource and Value for Money Implications

38. Continued adherence to good information assurance practice will help to ensure that the Council does not suffer financial loss through fine(s) for breaches.

Risk Implications

39. Any risks identified are subject to inclusion within the Authority's risk register and are dealt with as a matter of priority accordingly.

40. It is a key part of the Committee's role to give assurance to the Authority and the council tax payers that the public resources invested in the Authority are being properly managed. This report is one way by which that assurance can be given.

Climate Change Implications

41. There are no implications for climate change.

Report author:

Author's Name: Philip A. Jones
Ext No: 278364

Appendix A: Information Requests January 2016 – Dec 2016 – FOI & EIR

Statistic	January - March	April - June	July - September	October - December	Annual total
Number of Freedom of Information (FOI) requests received	382	324	317	325	**1348**
Number of Environmental Information (EIR) requests received	728	720	753	735	**2936**
Total number of FOI and EIR requests received	1110	1044	1070	1060	**4284**
Number of requests that took 20 working days or less	1056	986	996	1027	**4065**
Number of requests processed within 25 working days	1094	1004	1008	1035	**4141**
Number of FOI requests not answered within 20 working days	14	44	72	54	**184**
Number of EIR requests not answered within 20 working days	3	14	2	1	**20**
Number of requests where 20 working days deadline extended as permitted in legislation - Clarification	13	20	12	18	**63**
Number of requests where 20 working days deadline extended as permitted in legislation - Public Interest Test	2	4	3	7	**16**
Number of requests where a fee was charged	0	0	0	0	**0**
Number of requests refused in full because SCC does not hold information	80	59	65	77	**281**
Number of requests refused because requests considered vexatious	0			1	**1**
Number of request refused due to repeated requests	0				**0**
Number of requests refused as costs would exceed the 'appropriate' limit	14	11	26	10	**61**
Number of FOI requests refused under sections 22 - 44	8	1	8	10	**27**
Percentage of requests answered within 20 working days	95	94	93	97	**95**
Percentage of requests answered within 25 working days	99	96	94	98	**97**

Appendix A: Information Requests January 2016 – Dec 2016 – Data Protection

	s29 and Annex C Cases		Subject Access Requests	
Month	**s29**	**Annex C**	**SARs Due for completion**	**SARs Completed on Time**
Jan	19	19	10	6
Feb	16	15	8	7
March	11	6	12	12
April	10	18	8	3
May	123	18	11	4
June	11	16	6	5
July	6	8	7	7
August	17	9	16	16
Sept	15	22	8	7
Oct	7	10	2	2
Nov	14	15	9	8
Dec	9	4	7	5
Total	**258**	**160**	**104**	**82**

Appendix B: Email Gateway Statistics

Executive Summary (Inbound and outbound)

Total Messages

Message Types	**Count**	**%**
Single Threat Messages	898,053	6.3
Multiple Threat Messages	24,209	0.2
Total Threat Messages	**922,262**	**6.5**
Clean Messages	13,227,213	93.5
Total Messages	14,149,475	100

Threat Types

Threat Type	**Count**	**%**
Content Filtering	85,594	9.3
Malware	16,890	1.8
Invalid recipients	538,047	58.4
Bad reputation	135,859	14.7
Spam and unwanted mail	145,650	15.8
Disarmed message	0	0
Total Threats	**922,262**	**100**

In additional the DDoS prevention identified 764, 852 security events in 2016.