Staffordshire County Council

Local Members Interest
N/A

Audit and Standards Committee - Tuesday 26 April 2022

Annual Report on Information Governance

Recommendation

I recommend that:

a. The Committee note the information contained in this report.

Report of the Director of Corporate Services

Report

Background

1. This report is designed to give the Audit and Standards Committee assurance how SCC are complying with the following legislation:

   a. Data Protection Act 2018 and GDPR
   b. Freedom of Information Act 2000
   c. Environmental Information Regulations 2004
   d. Regulation of Investigatory Powers Act 2000

2. The 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 penalties, including monetary penalties and custodial sentences on organisations or individuals who breach these rules.

Information Rights

Data Protection

3. Under the Data Protection Act individuals have a right to access their own information, known as a Subject Access Request. Ensuring compliance with Access to Information is the overall responsibility of the Information Governance Unit as shown in **Appendix 1**. However, Children's Access to Information Team manage children's requests separately as shown in **Appendix 2**.

Staffordshire County Council

Freedom of Information

4. Freedom of Information 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 working days. Freedom of Information statistics can be found at **Appendix 1**.

Cyber Security

5. Local Authorities continue to face challenges to ensure that appropriate information security is in place. The County Council remains focussed on working towards ensuring that resilient procedures are employed across the Authority and in particular when risks of Cyber threats are heightened. The council has added additional security measures designed to add extra resilience at this time. To ensure there is a documented formal plan of cyber actions, there is a refreshed Cyber Security Strategy being developed for the next 3 years which will soon be published. This is based on the Governments Cyber Security strategy and will utilise the Cyber Assessment Framework methodology to assess strengths and identify areas for improvement.

6. The Council continues to invest in appropriate people, processes and tools to combat security threats, as well as purchasing Tenable, a vulnerability scanning tool and Bullwall, which detects and quarantines ransomware, the reorganisation of SICT also created a focussed team that is responsible for ICT Security. The new team has been expanded and the council has recently appointed two graduates from Staffordshire University.

7. In mid-December a vulnerability was identified in the Log4j open-source logging library. If exploited the vulnerability can allow attackers to break into systems, steal passwords, extract data, and infect networks with malicious software. The National Cyber Security Centre (NCSC) describe it as potentially the most severe computer vulnerability in years. The recently purchased Tenable vulnerability scanner was used to search for the vulnerability on SCC systems and equipment. SICT also worked closely with Directorate leads to seek assurances from providers of software as a service solution to verify that their products did not pose a risk to SCC systems or data.

8. Zero Day vulnerabilities will continue to pose a high risk to internally and externally hosted ICT systems. Although SCC has robust technical security controls and an ICT major incident process the unknown nature

of zero-day vulnerabilities makes it impossible to predict when they may appear, the impact and what the required mitigating actions will be.

9. Staffordshire ICT has recently implemented an "Air-Gap" backup solution. This is a significant step in reducing the impact of a ransomware or similar cyber security attack on the councils systems and data. The air-gap between the network and the backups means that in the event of a breach that the council would have a recovery capability from which to restore compromised systems. Sophisticated ransomware attacks attempt to not only make primary systems unusable but also make backup media unusable.

Multi Factor Authentication for Microsoft 365

10. In February senior management were asked to trial the use of Multi Factor Authentication (MFA) for Microsoft 365. MFA enhances access control security by removing the reliance on passwords to confirm the identity of an individual. In a similar way to when accessing online banking accounts staff will be periodically asked to provide an authentication code sent to them via an app or an SMS or email message sent to their phone. The MFA authentication will only be required periodically or if a person attempts to access an application from a different device or location. This is now being rolled out across the Authority.

Minimum password length changing

11. The minimum length of our network passwords is changing from 8 to 12 characters. The change is being made in response to audit recommendations and in line with National Cyber Security Centre advice to help protect us against potential cyber-attacks.

    a. An 8-character password made up of a mix of numbers and upper and lower case letters takes six minutes to crack. Add in special characters and that increases to five days.
    b. A 12-character password made up of a mix of numbers and upper and lower case letters takes 162 years to crack. Add in special characters and that increases to 8,000,000 years.

12. The change will take effect the next time you are prompted to change your password so this will happen over the next 3 months. The change will be instigated in April.

13. After that, you'll only need to change your password every six month in line with National Cyber Security's Centre (NCSC) guidance.

14. Cyber Champions programme is expanded and there are now 54 champions who have received additional training from the Cyber Crime Team at Staffordshire Police. These champions can assist colleagues to assess if communication is malicious and will also receive regular updates on current threats from the Police.

15. There is a risk of threat actors exploiting the security vulnerabilities of our suppliers to bypass our perimeter security controls. The Cyber Security Manager and IG have worked with procurement to improve our due diligence process. We have developed a new set of security questions to determine the adequacy of a prospective supplier's technical and organisational controls. NCSC have recognised this as a threat and have added Supply Chain to their 10 Steps to Cyber Security.

16. 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. A total of 351 incidents were reported between April 2021 and March 2022 which is the highest level of incidents since we began formally recording and is an increase of 37 from the previous year This is an average of 29 per month. The increase can be partially explained by more areas of the Authority knowing what is reportable following the refreshed mandatory training roll-out. Details of Security incidents are also included at **Appendix 3**

17. During 2021 Staffordshire ICT worked on a programme to update all devices to the latest version of the windows 10 operating systems. Maintaining vendor supported and compliant software is a cornerstone of the Public Services Network (PSN) Code of Connection that the council must comply with. This applies to all ICT Infrastructure and systems including end user devices, servers, applications, databases and networks and is an ongoing resource pressure.

18. The newly appointed Cyber Security Manager will take up the post in June and will continue the programme of work that has been undertaken to date and drive forward the cyber security strategy.

Accreditation

19. Staffordshire County Council has successfully been granted Public Services Network (PSN) accreditation for 2022. PSN is a key part of Government ICT Strategy and accreditation means that the authority can continue to access a secure network that facilitates the safe access of Government shared services. 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. This included an externally procured Penetration test carried out in 2021

20. Staffordshire County Council has also been accredited with Cyber Essentials for the fourth year running that demonstrates that it has effective controls in place.

21. 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 2021 Staffordshire County Council obtained compliance to the latest local authority version of the toolkit for the whole County Council

Governance

22. Governance of information requirements is provided through the Corporate Governance Working Group, Information Governance Unit, Senior Information Risk Owner (SIRO) Data Protection Officer (DPO) and 2 Caldicott Guardians, one for adults and one for children.

23. Staffordshire County Council has a comprehensive retention schedule, which identifies the statutory and business requirements for how long a record should be kept.

24. The Information Governance Team developed the One Staffordshire Information Sharing Protocol in 2012. The protocol outlines the purposes for sharing information, the powers that organisations have to share information, the role of partners and what can be expected from them, the process for sharing and scheduled review dates. The protocol alone does not provide the legal right to share information, it sets out the boundaries and guides under which sharing can occur and shows a commitment from its signatories to uphold what is required of them. There are currently 329 signatories to this protocol.

Information Management Strategy

25. The Information Governance Team has developed an Information Management Strategy and Framework. The strategy will run between 2022 and 2024 and is designed to support every member of staff with their individual responsibilities regarding the processing of personal data.

26. There is a working group of stakeholders which includes, DPO, SIRO, Caldicott Guardians and Information Asset Owners. The group meet monthly and will promote the strategy within their own areas.

27. The information asset owners are responsible for the maintaining the new Information Asset Register which is now live and is utilising. There are currently 50 IAOs with 94 data guardians.

28. The procurement exercise for the EDRMS is nearing completion. The EDRMS will address the unstructured data that SCC currently store. The outcome will be a streamlined and structured document management system which has in-built compliance with GDPR. It will remove redundant, duplicated and other redundant data which holds no value from our infrastructure. This will benefit all staff in the ease of document searches as it will be organised by the functions of the Authority and will therefore be future proofed. It will be built on the Microsoft 365 SharePoint platform which is already licensed and will also release more costly on-premise hardware.

29. The Information Governance Team has supported many projects in a variety of service areas including but not limited to:

    a. The return of Household Waste and Recycling Centres to SCC
    b. VivUp Staff Benefit project
    c. North Staffordshire Local Air Quality Plan
    d. Mental Health Assessor Contract
    e. OPAS (new Occupational Health system)
    f. Holiday Activities and Food Programme for school children
    g. Use of Alexa and similar technology in client homes

30. The Information Governance Team offer a traded service to assist with Data Protection, Information and Cyber Security, DPO service and FOI/EIR and currently support:

    a. 429 maintained schools and academies, some of which are out of county
    b. 8 Parish Councils
    c. South Staffordshire College
    d. WM Employers

Training and Guidance

31. All new starters must complete the Data Protection and Cyber security and record management e-learning modules as part of the induction process. All staff can complete a suite of Information Governance e-learning modules.

32. A new Cyber Security refresh module was released in January 2022

Regulation of Investigatory Powers Act

33. 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. During 2021-2 there were 0 Directed Surveillance applications made. No operations involving Covert Human Intelligence Sources were undertaken.

34. Access to Communications Data from communication are processed by the National Anti-Fraud Network (NAFN). No requests have been made or processed. A new Code of Practice has been issued and further work will take place to comply.

35. Annual RIPA training is complete for 2021-2022.

36. A full audit has been carried out and a register of all instances of CCTV has been completed The IG Team has a full set of documentation to ensure CCTV systems, requests for images and processing of associated data is compliant with the surveillance commissioner's code of practice.

List of Background Documents/Appendices:

Appendix 1 - Freedom of Information Requests, Corporate Subject Access Request and other information rights
Appendix 2 - Social Care Subject Access Requests
Appendix 3 - Information Security Incidents.

Contact Details

Assistant Director: Tracy Thorley, Assistant Director for Corporate Operations

Report Author: Natalie Morrissey
Job Title: Information Governance Manager
Telephone No.: 01785 278314
E-Mail Address: Natalie.morrissey@staffordshire.gov.uk