| Local Members Interest |
| --- |
| N/A |

# Audit and Standards Committee - Monday 12 October 2020

# Annual Report on Information Governance – 1 April 2019 to 31 March 2020

### Recommendations

I recommend that:

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

### Report of the Director of Corporate Services

## Summary

### 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. RIPA
    e. Local Government Transparency Code 2014

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. However, Families First manage children's requests separately. Compliance statistics for Families First and IGU are included at **Appendix 1**.

### 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 2**.

**Information Security**

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

6. 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.

7. The Council continues to develop the Cyber Security Incident Plan in case of a cyber-attack.

8. The Council continues to invest in appropriate software and hardware to combat security threats and works closely with its Internet Service Provider to improve its security and to ensure the earliest possible warning of cyber-attacks. The firewall hardware and software continue to provide protection to our network. The council is currently looking to invest in a Security and Information Events (SIEM) solution.

9. 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 202 incidents were reported between April 2019 and March 2020 which is the highest level of incidents since we began formally recording. This is an average of 17 per month. 8 incidents were reported to the Information Commissioner's Office, no further action was taken. Details of Security Incidents are also included at **Appendix 2**.

10. Staffordshire County Council has successfully been granted Public Services Network (PSN) accreditation for 2019. 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. 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 Pen test carried out in August 2019 where there were no critical or high actions. A stress test was carried out on CareDirector portal and Staffordshire ICT are scheduling more test with Nessus.

11. Staffordshire County Council has also been accredited with Cyber Essentials Tier 1 for the second year running.

## Governance

12. 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 for Health and Care, the Caldicott Guardian.

13. An 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. Further work to improve the IAR is being scheduled.

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

15. 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 March 2019 Staffordshire County Council obtained compliance to the latest local authority version of the toolkit for the whole County Council.

## Training and Guidance

16. All new starters must complete the Privacy, Data protection and Cyber security e-learning modules as part of the induction process. All staff can complete a suite of Information Governance e-learning modules.

17. The new DOJO videos have been rolled out and a further set of videos designed for members were released in March 2020.

## Regulation of Investigatory Powers Act

18. 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 2019 there were 3 Directed Surveillance applications made. No operations involving Covert Human Intelligence Sources were undertaken.

19. 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 before 27 May 2019.

20. RIPA training was delivered in November 2019 for the high-level policy requirements and a practitioners training day was delivered in December. A further course scheduled for March had to be postponed due to COVID-19. A

reviewed RIPA policy and new guidance on use of social media for investigation will be delivered in 2020. A RIPA inspection is also due during 2020.

**March 2020 COVID-19**

21. From March the Information Governance Team were responsible for the downloading and dissemination of data relating to the Staffordshire residents who were deemed Extremely Vulnerable to the virus.

22. This has been a very challenging time with the high volumes of inconsistent data the team have ensured accurate and timely reports to IMT. As the volumes increased, IGU enlisted the help of ICT and the procedure is now more streamlined with automated dashboards.

23. The team deserve praise for their hard work and dedication over the past several months.

**Equalities Implications**

24. There are no equalities implications arising as a result of this report.

**Legal Implications**

25. 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.

26. 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**

27. 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**

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

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

## List of Background Documents/Appendices:

Appendix 1 – Subject Access Requests
Appendix 2 – Freedom of Information Requests, Information Security Incidents, Training Stats

## Contact Details

**Assistant Director:** Tracy Thorley, Assistant Director for Business Support and Assurance

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