Staffordshire County Council

Audit and Standards Committee - Tuesday 25 April 2023

Annual Information Governance Report (April 2022 – March 2023)

Recommendation(s)

I recommend that:

a. Committee is requested to consider this report and the assurances provided within it, accepting that the information governance arrangements are fit for purpose, up to date, are routinely complied with, have been effectively communicated and are monitored.

b. Note the reporting and management of data security incidents and/or those reported to the Information Commissioners Office (ICO).

c. Committee Members are asked to provide feedback or recommendations which will be used to inform the 2023/2024 workplan.

Local Member Interest:

N/A

Report of the Director of Corporate Services

Report

Background

1. Information is one of the Council's greatest assets and its correct and effective use is a major responsibility and is essential to the successful delivery of the Council's priorities within the Strategic Plan. Ensuring that the Council has effective arrangements in place to manage and protect the information, both personal and business critical, it holds is a priority.

2. Data protection legislation sets out the requirements on organisations to manage information assets appropriately and how they should respond to requests for information.

3. In April 2022, the Director of Corporate Services submitted the 2021/2022 Annual Report where specific reference was made at that time to cyber security risks and the increased focus on training for officers and members given the current circumstances. In addition, user

authentication requirements were being strengthened to add additional resilience.

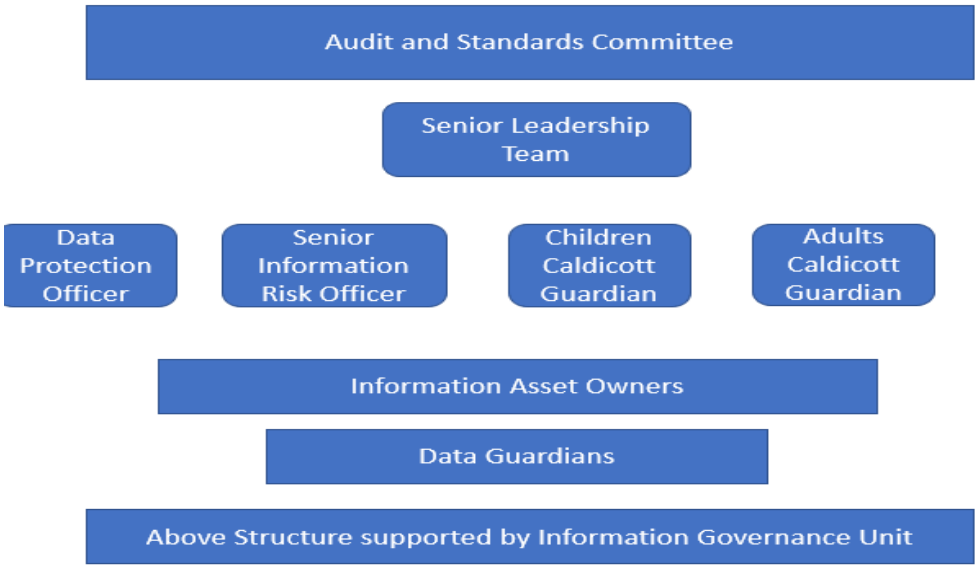
4. In response to member questions, it was reported that homeworking by County Council staff had initially seen increased need for support. However, this has since levelled out and during a recent audit of cyber security, the auditor was assured that appropriate measures were in place.

5. This report provides a summary of the Council's performance during April 2022 and March 2023 in responding to requests for information received under 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

6. 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.

7. It also reports on the management of data protection security incidents and/or those reported to the Information Commissioners Office (ICO) as well as mandatory training for Data Protection and Cyber Security.

8. Information Governance within the council is delivered through a distributed model of responsibility rather than the sole responsibility of the Information Governance Team, Data Protection Officer, and Caldicott Guardians. With key roles identified and assigned to ensure appropriate subject matter expert oversight and accountability, as shown in the structure chart below: -



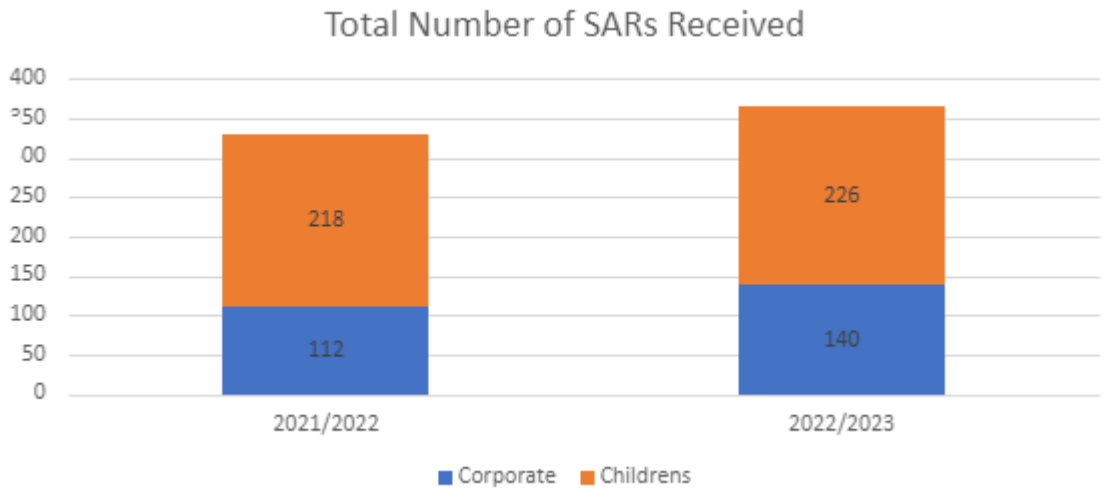
9. The Information Governance and access teams assist the organisation by monitoring internal compliance, informing, and advising on data protection obligations, providing advice and guidance, and raising awareness on data protection matters.

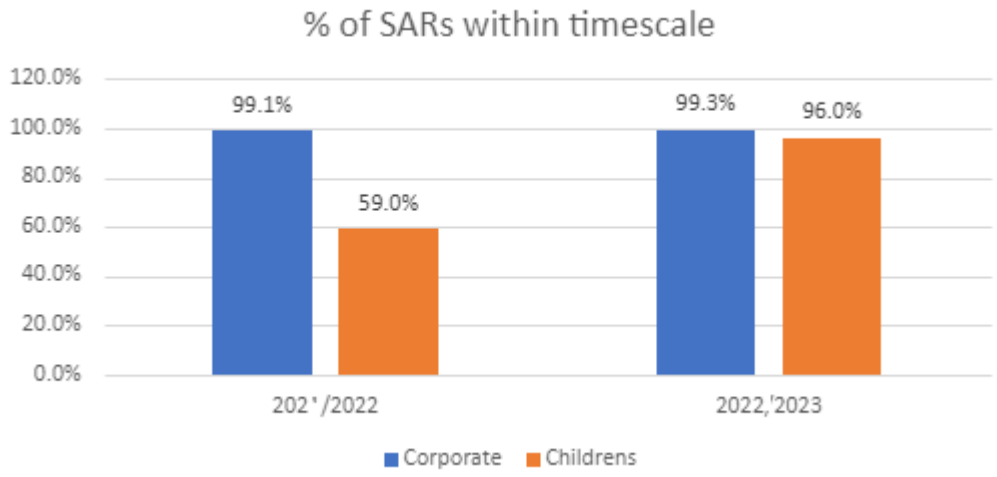
Information Rights

Data Protection

10. Under the Data Protection Act individuals have a right to access their own information that the Council holds about them, known as a Subject Access Requests (SARs). The timescale for responding to these requests is one month, starting on the day of receipt. Authorities can extend the time taken to respond by a further two months if the request is complex or a number of requests have been received from the individual, e.g., other types of requests relating to individuals' rights.

11. The tables below show the number of SARs received (366) which is a very slightly increase since last year (330), with a great improvement made by Children's Access Team to respond within timescale.





12. There is no formal requirement for the Council to have an internal review process for SARs, but it is considered good practice to do so. Therefore, the Council informs applicants of the internal review process on receipt of their request. However, individuals may complain directly to the ICO if they feel their rights have not been upheld.

13. Ensuring compliance with Access to Information is split across both the Access Team within the Complaints service and Children's Access to Information Team who manage children's requests. There is work about to commence to bring these two teams together under the corporate function.

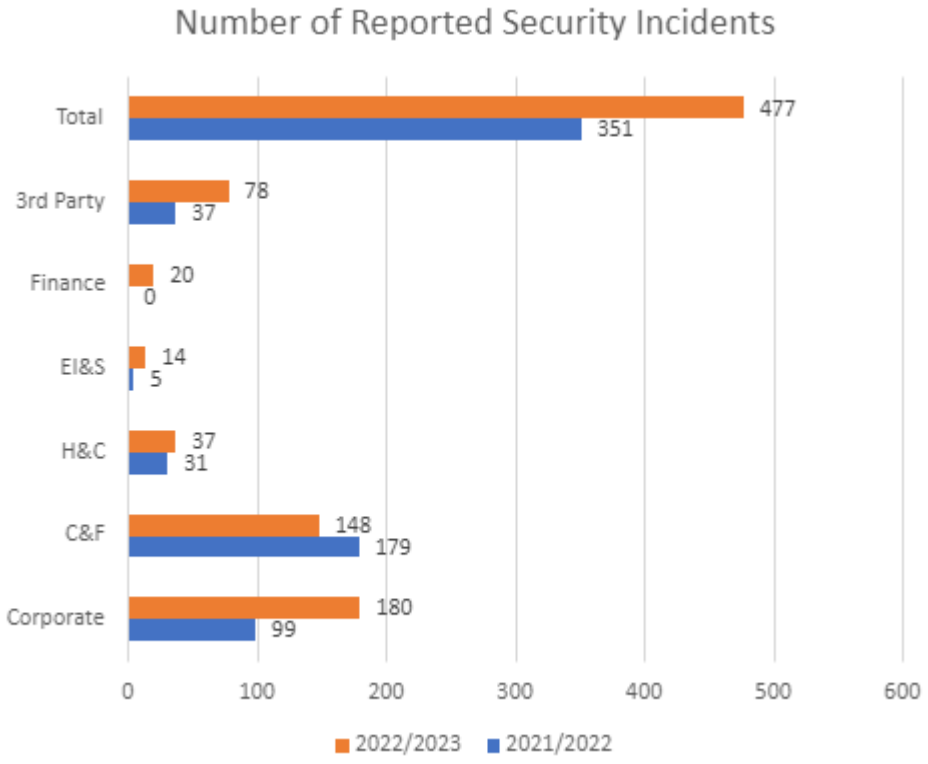
Security Incidents

14. Protecting information from theft, loss, unauthorised access, abuse, and misuse is crucial in order to reduce the risk of data breaches or financial loss incurred through non-compliance with key legislation.

15. An information security incident (both physical and electronic data) is classed as any situation involving personal or sensitive information where it:
    a. is accessed, used, disclosed, modified, or destroyed in an unauthorised manner.
    b. is placed outside of the normal organisational controls (increasing the risk of unauthorised access or use).
    c. cannot be accounted for by those who have a duty of custody for that information.

16. The Information Governance data protection security incident reporting process supports the Authority's objective that breaches are managed promptly, and outcomes of investigations are used to inform reviews of the control measures in place to keep personal information secure. Therefore, the Information Governance Unit record and investigate all reported security incidents and where necessary, recommend actions to be taken based on the impact risk level.

17. All incidents will be followed up with the appropriate manager to receive assurance from the service that recommendations have been implemented. A total of 477 incidents were reported between April 2022 and March 2023 compared to 351 reported the previous year. Corporate Services experienced a higher number of incidents, partly due to an increase in the number of admin staff transferred from Childrens into BEST and active promotion of reporting "near misses."



18. Not every data breach needs to be reported to the ICO. The Data Protection Officer (DPO) and/or Senior Information Risk Owner (SIRO) review any high-risk breach to consider the likelihood and severity of the risk to people's rights and freedoms. If it is likely there will be a risk, the Council will report breaches to the ICO. By law, the Council has 72 hours from the time of notification of the breach to report breaches that meet the threshold to the ICO. It was noted that thirty-eight incidents were reported outside of the 72-hour statutory deadline during the reporting period, which is a slight decreased from forty-five last year. We continue to increase awareness that any suspected breach or near miss must be reported to IGU immediately. However, none of these incidents met the criteria under GDPR for reporting to the ICO.

19. During 2022/2023, the Council reported five data breaches to the ICO. This is a slight decrease compared to same period last year where six breaches were reported. The five breaches relate to: -
    a. Provider using a sub-processor outside of the EEA.
    b. Third party breach
    c. Redaction error
    d. Reported to ICO by data subject which was later found not to be a breach of UK-GDPR
    e. Printing error (duplex rather than single print)

    In all cases the ICO's decision was that no further action required.

20. In addition, the Council encourages the reporting of "near misses" and potential breaches as this promotes awareness, avoids complacency therefore reducing the likelihood of a serious breach to information. Even where there is no breach, incidents can provide valuable insight into training requirements, processes, and procedures which may need to be strengthened as a preventative measure.

Data Sharing

21. The Information Governance Team supports the Council in understanding the impact of plans, projects, and activities on data protection through a process of impact assessments (DPIAs) to support decision-making. The number of DPIAs produced in the period was fifty-four. The Council also has arrangements in place to support the sharing of data where appropriate and the team provide support in the preparation and sign-off of ongoing and one-off data sharing agreements (DSAs). There are currently one hundred live DSAs as of 31st March 2023 recorded on our sharing register.

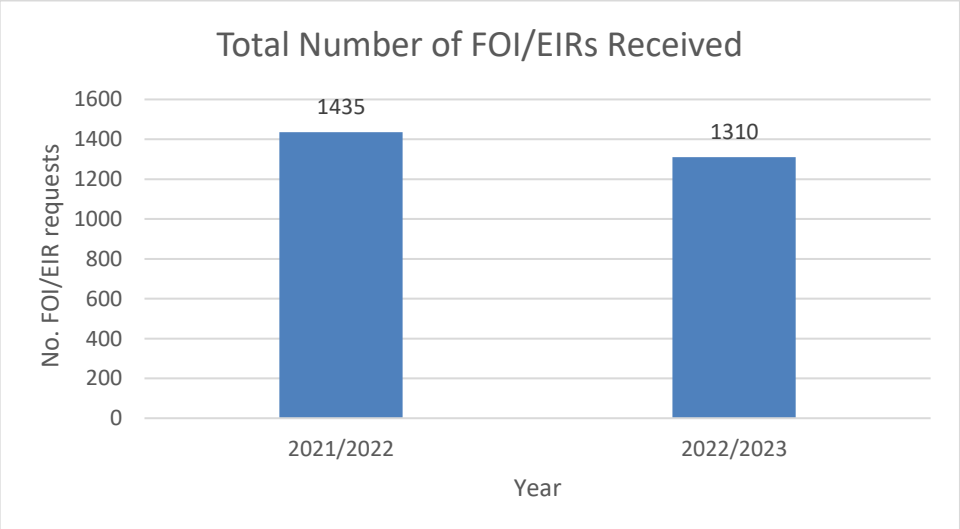
22. The Information Governance Team updated the One Staffordshire Information Sharing Protocol in 2022. The protocol outlines the

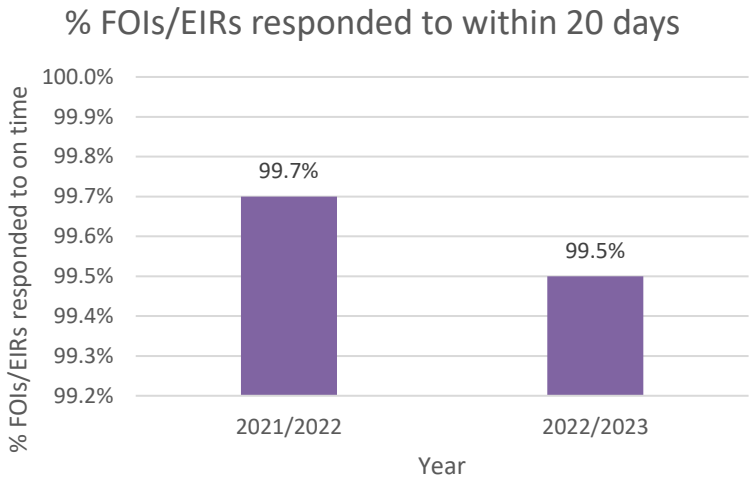
purposes for sharing information, the powers that organisations have to share information, the role of partners and what can be expected from them, the process for sharing and scheduled review dates. The protocol alone does not provide the legal right to share information, it sets out the boundaries and guides under which sharing can occur and shows a commitment from its signatories to uphold what is required of them. There are currently 314 signatories to this protocol.

Freedom of Information

23. Freedom of Information Act (FOIA) and Environmental Information Regulations (EIR) impose a statutory obligation on the Council to respond to requests for information within twenty working days, subject to relevant exemptions. The Code of Practice Section 45 of the FOIA, requires public authorities to have a procedure in place to deal with complaints regarding how their requests have been handled.

24. This process is handled by the Access Team within Complaints as an FOI/EIR internal review. After an internal review has been completed an applicant has a right to complain to the ICO for an independent ruling on the outcome. Based on the findings of their investigations, the ICO may issue a Decision Notice. The ICO may also monitor public authorities that do not respond to at least 90% of FOI/EIR requests they receive within twenty working days, which we are well above at 99.5%.

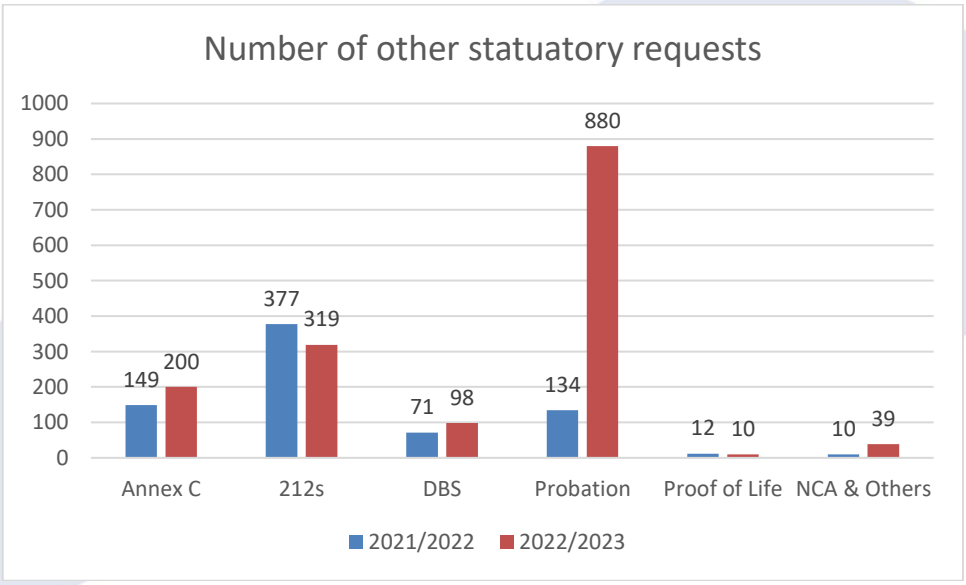




25. The Council already publishes a significant amount of information whilst recognising opportunities to increase the volume and type of information published (subject to legal compliance) to increase transparency and help to further reduce the number of FOI's the Council receives because the information will already be available.

Other statutory requests

26. The Council also receives one-off requests for personal information from third parties including the Police and other government agencies. The Access Team maintains a central log that includes exemptions relied on when personal data is shared with third parties and provide advice and assess whether the Council can lawfully disclose the information or not. Probation has seen a huge increase, and this is set to continue due to legislative changes, more resource is currently being sourced to meet our statutory obligations on timescales.



Data Security and Protection Toolkit

27. The Data Security and Protection Toolkit is an online self-assessment tool that allows relevant organisations that process health and care data to measure their performance against National Data Guardian's 10 data security standards and information governance requirements which reflect legal rules and Department of Health policy. This independently audited self-assessment tool enables the Council to demonstrate that it can be trusted to maintain the confidentiality and security of personal information, specifically health and social care personal records.

28. All organisations that have access to NHS patient data and systems must use this Toolkit to provide assurance that they are practicing good data security and that personal information is handled correctly.

29. For the 2021/22 reporting period, the submission deadline was 30 June 2022. Ordinarily this is 31 March each year, however due to national, regional, and local response requirements to Covid-19, there has been an extended timeframe for submissions over the past few years.

30. The 2021/22 Toolkit was successfully completed, and it was confirmed that the Council has appropriate evidence available for its assessment and the Toolkit standard was met. Our 2022/23 submission is due by 30th June 2023.

Cyber Security

31. The risks facing Local Authorities and their suppliers around Cyber, and Information Security continued to grow during 2022. The Council continues to address these risks robustly, engaging with partners in the National Cyber Security Centre (NCSC) and collaborating with them and their colleagues in the Department for Levelling Up, Housing and Communities (DLUHC) to undertake quarterly assessments of our security arrangements.

32. Email continues to present security challenges, with a marked increase in the sophistication of the phishing attacks that we see. For context, the Council's 4,500 ICT users send/receive in the region of seventeen million emails in a twelve-month period. Of these, over half a million inbound emails are blocked as being spam, with another 7,000+ blocked for containing malicious content. Due to the critical nature of email to the Council, significant effort is put into securing this vital tool.

33. The Cyber Security Strategy covering the 3 years to 2025 was agreed and published last year. As well as providing a documented formal plan

for Cyber Security as we move forwards, it is aligned to the NCSC Cyber Assessment Framework (CAF) which is a tool that is increasing in popularity within the public sector for benchmarking adherence to good security practices.

34. During 2022, Staffordshire ICT worked to implement a Security Incident and Event Management (SIEM) tool. This tool allows us to consolidate information from the various security tools that we employ across the ICT establishment and correlate and display the information in a centralised location. The implementation of a SIEM tool has been a key recommendation from Government for the Council, with it forming a cornerstone of our engagement with DLUHC around improving our Cyber Security. As part of a joint initiative with partners in the Integrated Care System the council is looking to jointly procure a Security Operations Centre. This will provide 7 x 24 oversight of the SIEM and couple this with threat intelligence to further improve our security defences. It is anticipated that this will be in place during 2023.

35. Following an extensive and carefully managed implementation, our anti-malware tool is now in widespread use across the Council. The tool continuously monitors all our shared filing, SharePoint, and OneDrive folders to identify any signs of malware on our network. Upon detecting an incident, it disables the affected computer and user account to help prevent the spread of malware (e.g., a Ransomware attack) and adds an additional layer of protection to Council data and systems.

36. During 2022 the use and embedding of vulnerability scanning commenced within SICT, using the market leading vulnerability scanner product. Rather than being reliant on annual scans and penetration tests commissioned as part of our ongoing compliance regimes, we are now able to undertake weekly scans across our ICT estate to pro-actively manage any vulnerabilities as they arise. This is further supplemented by the use of tools supplied by the NCSC that examine and report on any externally visible Internet addresses used by the council.

37. Throughout 2022 we engaged with the cyber security consultants, who were commissioned by DLUHC to collaborate with a cohort of local councils. As well as providing us with a list of work to complete to improve our cyber security, they undertook quarterly external scans of our network to search for any vulnerabilities that they could uncover. By the end of our engagement, we had completed all the actions assigned to us and our external scan results were not returning any vulnerabilities that we needed to address.

38. Work is continuing with colleagues across ICT, IGU and the Commercial Team to ensure that any ICT goods or services procured do not introduce any Cyber Security risks through supply chain arrangements. The recent incident affecting CareTech who operate the Cambian and By the Bridge services (delivering Fostering services in England) only serves to reinforce the importance of a robust approach to security assurance during procurement. The security questionnaires that are sent to potential vendors are under continual review to ensure they are relevant and provide as much assurance as possible around new and emerging threats.

39. The change to 12-character passwords for council ICT users, which now only need to be changed once every year has been well received. New laptops are increasingly being issued with biometric sensors, which allow users to login using their fingerprint, or facial identification technology, further assisting users to login quickly and conveniently while maintaining security. Any access to council networks including Microsoft 365 using "unmanaged devices" also requires Multi Factor Authentication which provides a significant risk reduction of unauthorised access to our systems and data.

40. 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.

41. Several face-to-face cyber training sessions were offered to all members during Autumn of 2022 which were well attended and received by members. Further sessions can be organised upon request.

42. An audit of the 2022-2023 Cyber Strategy has again had a positive outcome with an adequate assurance awarded.

Accreditation

43. Staffordshire County Council has successfully been granted Public Services Network (PSN) accreditation for 2023. PSN is a key part of the 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 the PSN is paramount and to achieve accreditation the authority had to satisfy a Code of Connection containing over sixty different security controls. This

included an externally procured Penetration test and IT Health Check that were carried out in 2022.

44. Staffordshire County Council is going through the accreditation process for Cyber Essentials for the fifth year running in order to demonstrate that it has effective controls in place.

Policy Review

45. The following IG policies have been reviewed and approved by the Corporate Governance working Group where appropriate and published.

System Logs and Data Requests	Reviewed by IG June 2022
Regulation of Investigatory Powers Policy	Approved by CGWG Aug 2022
One Staffordshire Information Sharing Protocol	Reviewed by IG Oct 2022

Training and Awareness

46. There is no requirement set out in the GDPR regarding data protection training for staff, however, principle 7 of the GDPR states that 'Data Controllers (the Council) are responsible for the compliance with the principles and must demonstrate this to data subjects and the regulator.

47. We recognise that training is key to ensuring staff are aware of their responsibilities. To ensure our compliance, all new starters and elected members are required to complete mandatory GDPR, records management and Cyber Security eLearning training as part of their induction. Thereafter, all staff and elected members complete a refresher eLearning module for Cyber Security after their first year at the Council. This ensures that an appropriate level of understanding and awareness is reached that is relevant to their role/responsibilities. We are working with the Learning & Development team within People Services to ensure this is seamless for users around refresher courses. This is a rolling programme of training with completion monitored by line managers and reported to SLT via the monthly assurance report.

48. Staff who do not have access to a computer in their role (not office based) and those with minimal personal data involved in their role are provided with appropriate level training. Staff can also complete a suite of Information Governance e-learning modules.

49. As part of our awareness work 'culture' is a key element and is ongoing due to the ever-changing cyber threats, so we will build on what we already have, to ensure the Authority is even more resilient.

Surveillance

50. Staffordshire County Council is entitled to use the Regulation of Investigatory Powers Act (RIPA) for carrying out overt and covert surveillance as part of our statutory duties. Extensive work was carried out during 2022 to ensure the Council is compliant with the Surveillance Code of Practice and the Regulation of Investigatory Powers (RIPA). This work involved a review of current overt surveillance systems (including ensuring that all necessary documentation DPIAs and ISAs are in place), the completion of a privacy notice for CCTV operations, an updated RIPA policy and delivery of training on RIPA to relevant officers.

51. All applications for surveillance must be approved by a Magistrate. During 2022-23 there were 0 Directed Surveillance applications made. No operations involving Covert Human Intelligence Sources were undertaken.

52. Access to Communications Data from communication are processed by the National Anti-Fraud Network (NAFN). No requests have been made or processed.

Equalities Implications

53. The Council's responsibilities under Section 149 of the Equality Act 2010 are supported by UK GDPR/DPA2018, requiring that Special Category Data be afforded extra measures of security to protect that data.

Legal Implications

54. There are no specific legal implications arising out of the report. However, the Council's performance is subject to external scrutiny and 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.

55. Failure to comply with the Regulation of Investigatory Powers Act (RIPA) 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

56. There are no specific financial implications resulting from the issues within this report although it is worth noting that the Information

Commissioner's Office is able to levy significant fines for serious non-compliance with the legislation surrounding the management of information.

Risk Implications

57. The reporting and monitoring on the Council's performance to information laws and outcomes of ICO complaints will help reduce the risk of the ICO upholding complaints and taking enforcement action against the Council.

58. Any risks identified are subject to inclusion within the IG risk register and are dealt with as a matter of priority accordingly and escalated for inclusion on the Corporate Risk Register as appropriate.

59. 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.

Climate Change Implications

60. There are no specific Climate Change implications arising out of the report.

List of Background Documents/Appendices:

None

Contact Details

Assistant Director: Tracy Thorley – **Assistant Director for Corporate**
Operations & Data Protection Officer

Report Author: Tracy Thorley
Job Title: **Assistant Director for Corporate Operations & Data Protection Officer**
Telephone No.: Via Teams
E-Mail Address: tracy.thorley@staffordshire.gov.uk

Report Contributor: Vic Falcus
Job Title: **Head of IT**
Telephone No.: 01785 278032
E-Mail Address: vic.falcus@staffordshire.gov.uk

Report Contributor: Natalie Morrissey

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

Report Contributor: Stuart Fletcher
Job Title: Cyber Security Manager
Telephone No.: 01785 278604
E-Mail Address: stuart.fletcher@staffordshire.gov.uk

Report Contributor: Kate Bullivant
Job Title: Complaints Manager
Telephone No.: 01785 277407
E-Mail Address: kate.bullivant@staffordshire.gov.uk