Local Members' Interest
N/A

Audit and Standards Committee – Wednesday 12 June 2019

Annual Report on Information Governance

Recommendation

a. That the Audit and Standards Committee are asked to receive and note this report.

Report of the Director of Corporate Services

Background

1. Staffordshire County Council recognises the need to protect its information assets from both accidental and malicious loss and damage. Information Governance is taken very seriously by the council and this is evidenced by the ongoing work to improve the management and security of our information as outlined in the report.

2. This report is designed to give the Audit and Standards Committee assurance how SCC are complying with the following legislation and to provide assurance for the annual governance statement:

    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

3. 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.

4. The County Council is currently reviewing the 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 provide and commission services in new and innovative ways across Staffordshire. All policies are being reviewed and cross referenced against ISO standards.

Freedom of Information

5. 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 days, we are currently at 86%.

	2016/17	% compliance with statutory timescale	2017/18	% compliance with statutory timescale	2018/19	% compliance with statutory timescale
FOI	1364	77%	1382	83%	1603	86%[1]
EIRs	2875	99%	2797	99%	2565[2]	99%

6. It should be noted that the volume of requests can really give no indication of the amount of time spent in answering each one. Some requests involve reporting on data that we routinely collect/publish and can be completed relatively quickly. However, others may involve large amounts of work by different departments and we frequently must judge whether answering a request would fall under the 'complex' category. This relates to both FOIs and SARs (as mentioned below).

7. Highways, Finance & contracts and Social Care receive the majority of FOI requests with Education and Human Resources close behind. Most departments and services receive some requests. Co-operation is good across all departments, but some requests are complex, and delays can occur when information is required from different specialities and departments. FOI remains a challenge to manage and for different areas of the business to respond to with staff reductions and volumes increasing and becoming more complex.

Data Protection

8. 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 (since 2017).

	2016/17	% compliance with statutory timescale	2017/18	% compliance with statutory timescale	2018/19	% compliance with statutory timescale
Corporate	104	79%	30	83%	119	89%
Children's			97	43%	160[3]	46%

9. Throughout 2018/19 the IG team provided support to other organisations (Borough, Schools; Parish Councils) bringing income into the Authority in relation to both the implementation of GDPR and ongoing DP and Information Security support.

Records Management

10. Work is underway to review the current Information Asset Register (IAR). The Register is intended to inform decision-making about the management of our information assets in

[1] An additional 9% were responded to within 25 days
[2] There has been an 83% drop in Land Charge FOIs since Jan 2019 due to additional information being posted on the internet
[3] 25% were deemed complex requests

order to mitigate information risks. It has been recognised that this needs to be done in a more devolved, user friendly and dynamic way. Once a robust methodology for implementing the IAR is approved, training material will be refreshed and reviewed ready for launch late 2019. The opportunity will be taken once again to raise awareness across the organisation of the role of Information Asset Owners (IAOs).

11. With both the office moves and roll-out of O365 the IG team are supporting both the project team and all service areas regarding data cleaning. Which has involved the destruction of paper records, digitisation or archive of records to mitigate the risk of breaching DPA principles. It has been highlighted during this work that further work needs to be undertaken to ensure staff are aware of their roles and responsibilities in relation to the management of information. Therefore, training material and guidance notes will be reviewed and communicated as necessary.

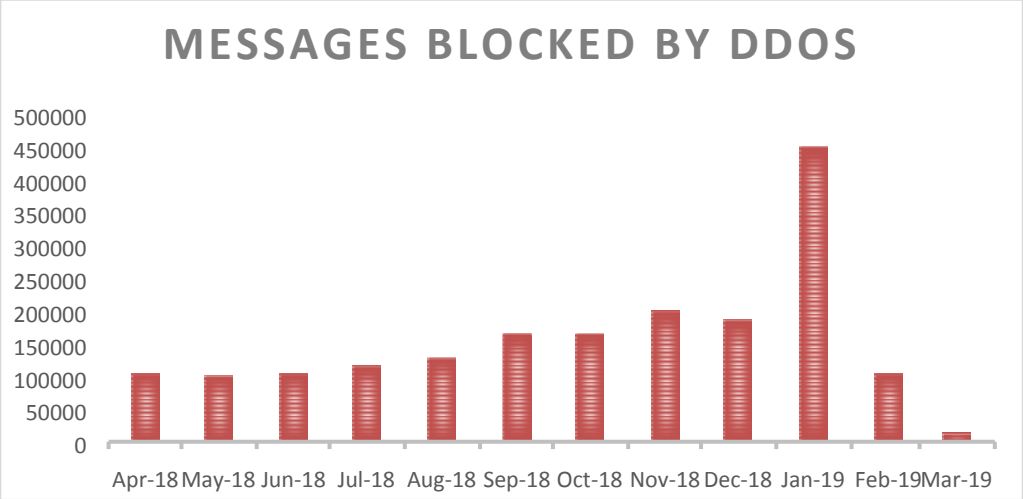
12. The ongoing work to develop the IAR and role of IAOs will include a review of retention periods. This in turn may mean an update to retention schedules which will drive the policy for O365 data storage. This is a major piece of work that must be done ahead of any roll-out or configuration of One Drive and SharePoint (replacing Home and Shared drives) to ensure compliance.

Information Security/Cyber

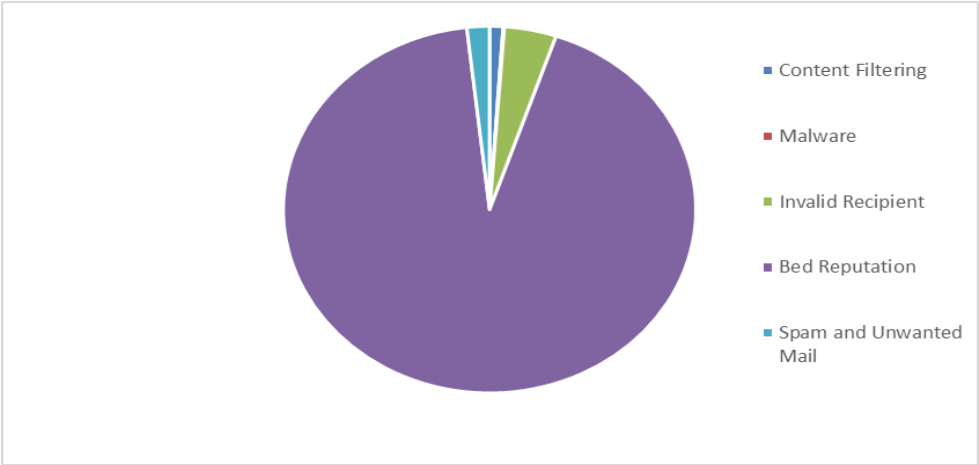
13. Local Authorities continue to face challenges to ensure that appropriate information security is in place. Therefore, the County Council has continued to invest and develop further protection in Cyber and Information Security across several areas over the past year to ensure that resilient procedures are employed across the Authority. We continue to work closely with our Internet Service Provider to improve its security and to ensure the earliest possible warning of cyber-attacks.

14. The authority continues to be subject to a high-volume of cyber-attacks, some of the low level can be classed as ‘internet traffic’. 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. Denial of service attacks has 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.

15. The County Council has a layered approach to security protection. The first layer is provided by our internet service provider which will filter out a certain amount of threats and spam message, even before they reach our network. The County Council defences start with our DDoS protection, which is designed to specifically stop Distributed Denial of Service attacks. These are attacks where a perpetrator will use a single source (DoS) or multiple sources (DDoS) will attempt to disrupt systems and services, usually by flooding the target with superfluous requests to overload the systems. The chart below indicates the number of messages blocked by the DDoS protection each month.



16. Our networks and systems are further protected by the Symantec Email Gateway. Between April 2018 and March 2019, the email gateway handled a total of 26,913,318 incoming messages. Of those messages a total of 12,904,165 messages contained single and multiple threats, an average of 48%. The types of threats are identified as follows:

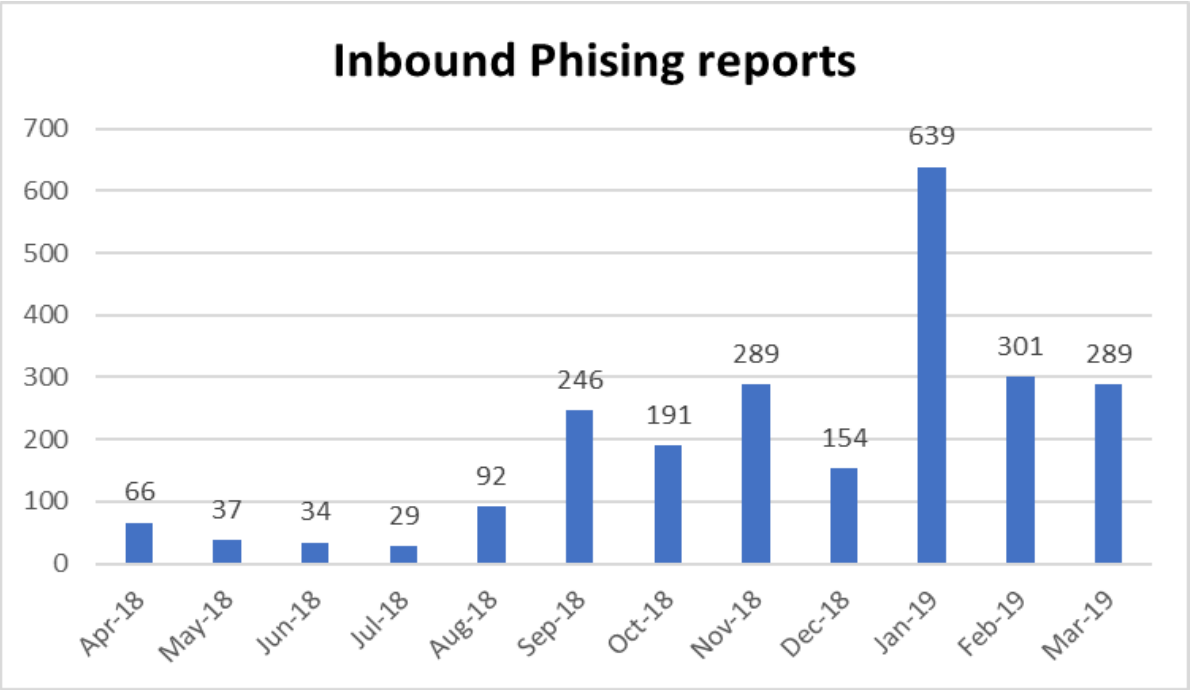


17. An increase in malware email campaigns (software which is specifically designed to disrupt or damage a computer system) has led to limits being placed on downloading executable files. End user machines also have local anti-virus protection and ICT have a managed process for malware found on machines. In general, this is a very low amount (between 10 – 40 machines per month out).

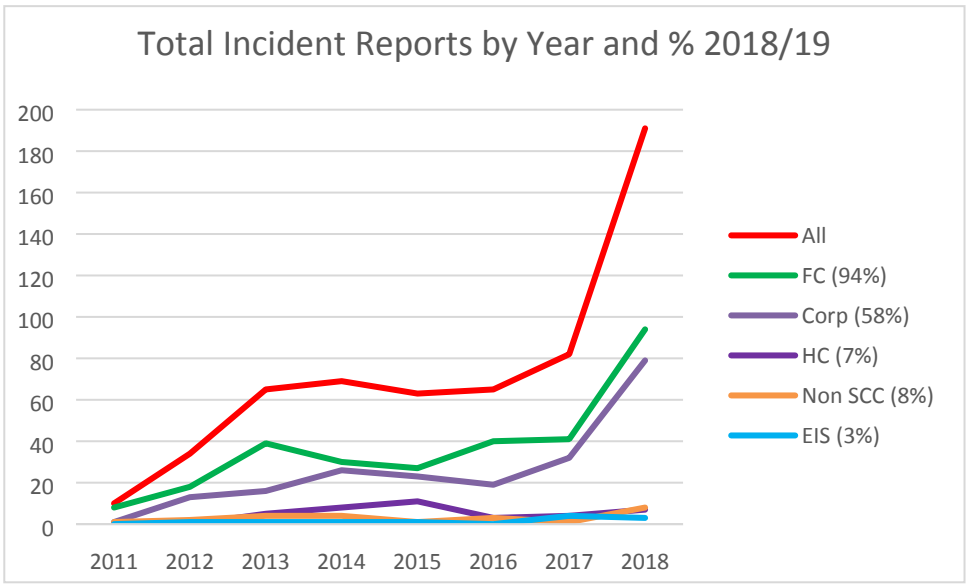
18. There are technical preventions in place, including filtering and blocking software. However, these are not guaranteed in blocking all potentially malicious emails and these measures must be balanced against the ability to carry out business with minimal disruption in a digital environment. As the volume and sophistication of malicious emails increases, users need to be more aware about recognising the threats posed including malicious links or attachments containing malicious software.

19. It is accepted that in nearly all cases users will not be taking these actions deliberately, however the consequences of these actions can be potentially highly damaging in terms of system downtime, data loss and reputational damage. Global communications will still be used to raise general awareness, but individual, targeted communications will be focussed on users who have clicked on suspected malicious links or opened attachments containing malicious software.

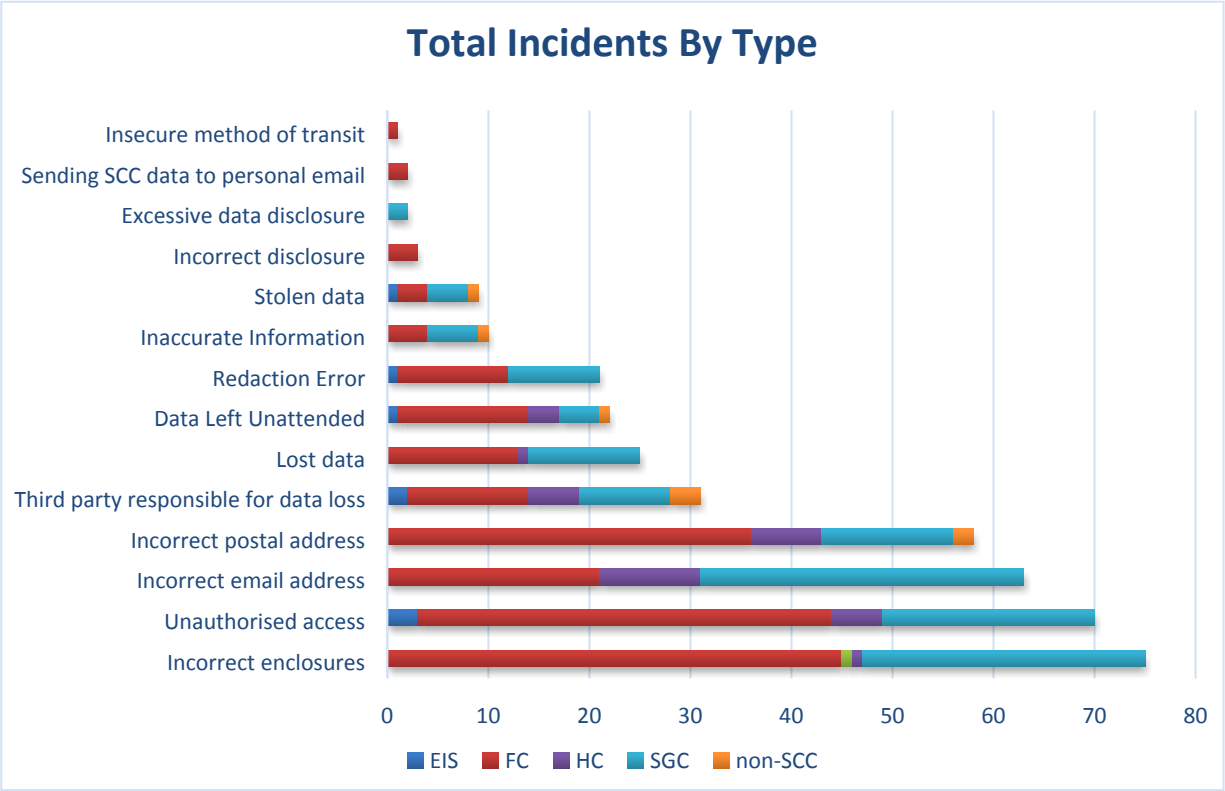
20. All users can report suspicious, malicious and/or spam emails to a central email address. The below table shows the amount of reports we have received between April 2018 and March 2019.



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 Officer.



22. A total of 191 incidents were reported in 2018/19 which is the highest level of incidents since we began formally recording, we believe this is because we are promoting the reporting more regularly via different means. This is an average of 16 per month. The highest categories are incorrect enclosures, incorrect email or postal address and unauthorised access to data, which can be seen by the chart below.



23. The Council has developed a Cyber Security Incident Plan in case of a cyber-attack. Work is ongoing to review the plan due to the outcomes identified by recent audits and to further test the organisations' plans to respond to an attack. Information Governance Team have been working with the Regional Organised Crime Unit (ROCU) on the promotion of their Cyber Champion initiative within SCC. Over 20 members of staff from across the service areas have received training so far in Cyber Awareness from the Digital PCSO and are now able to provide their colleagues with advice and guidance to help prevent cyber-attacks.

24. Some of the Cyber Champions have also been involved in the Cyber Breach desktop exercise facilitated by CCU.

25. 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 has been implemented to ensure that there are no instances of unauthorised software within the SCC network and that all instances are licensed.

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

27. Staffordshire County Council has successfully been granted Public Services Network (PSN) accreditation again in 2018. 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 has 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.

28. In 2019 SCC achieved Tier 1 Cyber Essentials which is a UK Government information assurance scheme operated by the National Cyber Security Centre that encourages organisations to adopt good practice in information security.

29. A Cyber Security Strategy is being developed and will be signed off by the Corporate Governance Working Group to ensure that the requirements of security are maintained whilst ensuring the authority is flexible to meet working requirements of a digital world. Reporting against the outcomes of the strategy will be included in this report from 2019 onwards.

Governance

30. The Council, in line with recommended practice for all public authorities in the UK, continues to provide demonstratable arrangements which ensure that information assurance is addressed along with other aspects of information governance. This is provided through the Corporate Governance Working Group; Information Governance Unit; Senior Information Risk Owner (SIRO); Data Protection Officer (DPO) and for Children's and Health and Care, their Caldicott Guardian.

31. 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 again to the latest local authority version of the toolkit for the whole County Council.

32. It has been recognised through work with Audit that there would be a benefit of IG carrying out 'spot check' audits regarding areas such as contract information security compliance; IAR to undertake risk assessments from an information security and data protection legislation perspective, follow up recommendations after an information breach for services that report higher than usual incidents.

Training and Guidance

33. All new starters are expected to complete the mandatory e-learning modules (Cyber Security and Privacy) 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 and Protective Marking. The modules are reviewed at least annually to ensure information is current and reflects regulations and procedures and the modules have been classified as either 'mandatory' or 'essential'.

34. In the past 12 months the Information Governance Team have been collaborating with other LAs and CC2i in the production of short videos which will enhance our GDPR training, also Information security modules have been purchased and all will be rolled out in the coming months. The Authority will form part of a future collaboration to produce e-learning/videos specifically designed to support Councillors in their local role.

Regulation of Investigatory Powers Act

35. 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 2018 no Directed Surveillance applications were made. No operations involving Covert Human Intelligence Sources were undertaken.

36. 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.

Priority Areas for 2019/20

37. Review of the Information Governance Framework in-line with the upgrade of the Authorities intranet/internet to continue to embed Information Governance best practice within the culture of the organisation, through additional awareness and training.

38. Review of policies in-line with HR Policy review, including cross referencing against ISO standards.

39. Review of Information Asset Register, to ensure more user-friendly; further devolved accountability and dynamic reporting. Also carry out 'spot check' audits to advise staff on the best approach to ensure the information is protected in relation to its confidentiality, integrity and availability and to check that that personal data is being processed lawfully.

40. Raise awareness of the scope of the Information Asset Owner role and support them to embed effective information risk management activities. As well as individual's role and responsibilities for records management.

41. Support O365 implementation especially regarding data architecture, data cleanse/digitation; migration and retention.

Equalities Implications

42. Equalities, diversity, cohesion and integration are all being considered as part of delivering the Information Management Framework. This refers to the way training is being delivered as well as how policies will impact on staff and partners.

Legal Implications

43. 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.

44. 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

45. 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

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

47. 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

None

Contact Officer

Name and Job Title: Tracy Thorley, Head of Executive Support and Compliance
E-Mail Address: tracy.thorley@staffordshire.gov.uk

List of Background Papers/Appendices:

None