**Audit and Standards Committee**

**12 March 2018**

# Annual Report on Information Governance

1. **Recommendation:**

   That the Panel note the information contained in this report.

   ***Report of the Director of Strategy, Governance and Change***

2. **Background**

   2.1 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.

   2.2 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. 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.

   2.3 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 provide and commission services in new and innovative ways across Staffordshire.

3. **Transparency**

   3.1 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 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.

4. **Freedom of Information**

4.1 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 continue to increase 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).

4.2 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. Freedom of Information statistics can be found at **Appendix A**.

4.3 We publish a selection of questions and answers under FOI, based on 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.

5. **Data Protection**

5.1 Data protection is primarily concerned with personal data about individuals rather than general information. 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.

5.2 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 170 public sector bodies across Staffordshire who are committed to effective information sharing. The County Council lead on the management of Protocol to ensure that the protocol is up to date and fit for purpose.

5.3 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 HMRC, 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 is evidence of our commitment to give the highest priority to such matters.

5.4 Under the Data Protection Act 1998 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 are included at **Appendix B**.

5.5 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.

5.6 Through 2017 and into 2018 a project has been in place to ensure the authority is ready to meet the changes the GDPR will bring in. This has involved conducting a gap analysis and project managing the changes. Please note most of these principles already exists within the current legislation, however the publicising of this by the media may increase volumes of requests.

## 6. Information Security

6.1 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.

6.2 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 C**.

6.3 In April 2017 the council implemented a process for raising user awareness and for identifying and preventing users clicking on malicious links. Details are also included in **Appendix C**. All users can report suspicious, malicious and/or spam emails to a central email address.

6.4 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 the exercise.

6.5 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.

6.6 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.

6.7 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. A total of 82 incidents were reported in 2017 which is the highest level of incidents since we began formally recording. This is an average of 7 per month. Details of Security Incidents are included at **Appendix D**.

6.8 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.

6.9 Staffordshire County Council has successfully been granted Public Services Network (PSN) accreditation for 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 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.

6.10 In 2017 a Cyber Security Strategy was introduced to ensure that the requirements of security are maintained whilst ensuring the authority is flexible to meet working requirements of a digital world. The strategy is included at **Appendix E**. Reporting against the outcomes of the strategy will be included in this report from 2018 onwards.

## 7. Governance

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

7.2 The role of a 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. Health and Care do not have a SIRO but a Caldicott Guardian fulfils that role.

7.3 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. 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. It includes a comprehensive risk assessment framework to be applied to the assets that have been identified. In 2017 development work has taken place on the IAR to identify and record compliance with GDPR requirements.

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

7.5 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 2017 Staffordshire County Council obtained compliance to the latest local authority version of the toolkit for the whole County Council.

## 8. Training and Guidance

8.1 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’.

8.2 In June 2017 a mandatory Privacy e-learning module replaced the previous module. At 31 December 2017, only 54% of staff had undertaken the training.

8.3 In 2017 guidance has been reviewed to ensure that it complies with smart working and new cyber security guidance has been added to include how to create strong passwords and how to spot fake or scam emails. These are available to all staff on the intranet.

9. **Regulation of Investigatory Powers Act**

9.1 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.

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

9.3 There is a regulatory obligation to report the outcome of any commissioner Inspections to members. In 2017 the Office of the Surveillance Commissioner completed a compulsory regulatory inspection. Some minor recommendations were made with regard to how we use social media in a RIPA context which we are considering further.

**Appendix 1**

## 1.0. Equalities Implications

1.1 None

## 2.0. Legal Implications

2.1 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.

2.2 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.

## 3.0 Resource and Value for Money Implications

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

## 4.0 Risk Implications

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

4.2 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.

**Report Author**:

**Author's name**: Tracy Thorley Tel No: (01785) 276337

**E-mail**: tracy.thorley@staffordshire.gov.uk

**List of Background Papers:**

Appendix A: Information Requests

Appendix B: Families First Information Requests

Appendix C: Information Security Statistics

Appendix D: Incident Statistics

Appendix E: Cyber Security Strategy

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

| Statistic | January-March | April-June | July-September | October-December |
|---|---|---|---|---|
| Number of Freedom of Information (FOI) requests received | 398 | 336 | 344 | 333 |
| Number of Environmental Information (EIR) requests received | 667 | 750 | 902 | 705 |
| Total number of FOI and EIR requests received | 1065 | 1086 | 1246 | 1038 |
| Number of requests that took 20 working days or less | 920 | 937 | 1167 | 936 |
| Number of requests processed within 25 working days | 987 | 1031 | 1190 | 986 |
| Number of FOI requests not answered within 20 working days | 145 | 149 | 79 | 102 |
| Number of EIR requests not answered within 20 working days | | | | |
| Number of requests where 20 working days deadline extended as permitted in legislation - Clarification | 15 | 15 | 5 | 7 |
| Number of requests where 20 working days deadline extended as permitted in legislation - Public Interest Test | 7 | 2 | 1 | 3 |
| Number of requests where a fee was charged | 0 | 0 | 0 | 0 |
| Number of requests refused in full because SCC does not hold information | 89 | 75 | 88 | 59 |
| Number of requests refused because requests considered vexatious | 0 | 0 | 0 | 0 |
| Number of request refused due to repeated requests | 0 | 0 | 0 | 0 |
| Number of requests refused as costs would exceed the 'appropriate' limit | 9 | 10 | 9 | 11 |
| Number of FOI requests refused under sections 22 - 44 | 8 | 3 | 1 | 40 |
| Percentage of requests answered within 20 working days | 86 | 86 | 94 | 90 |
| Percentage of requests answered within 25 working days | 93 | 95 | 96 | 95 |

**Appendix B: Information Requests January 2016 – Dec 2016 – Data Protection**

## ACCESS TO INFORMATION PERFORMANCE STATISTICS

Families First

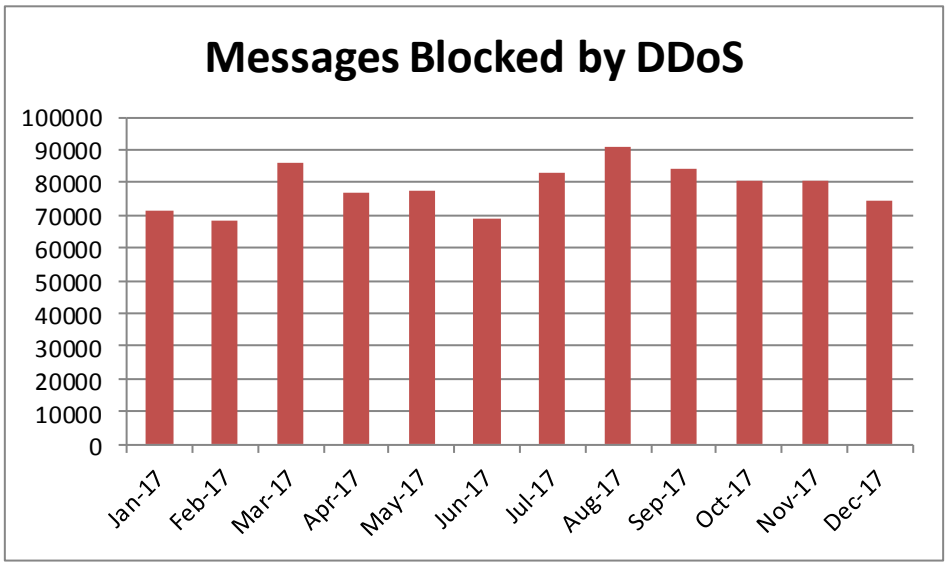
| | | January | February | March | April | May | June | July | August | September | October | November | December | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CLOSED SAR | Initial Requests | | | | | | | | | | | | | 0 |
| | SAR Requests | 6 | 6 | 5 | 9 | 8 | 10 | 7 | 4 | 15 | 9 | 14 | 4 | 97 |
| | SARs due for completion | 3 | 4 | 8 | 5 | 5 | 10 | 8 | 11 | 2 | 14 | 7 | 13 | 90 |
| | Completed in time | 1 | 2 | 3 | 1 | 1 | 6 | 5 | 6 | 0 | 6 | 5 | 6 | 42 |
| | Completed out of time | 2 | 2 | 5 | 4 | 4 | 4 | 3 | 5 | 2 | 8 | 2 | 7 | 48 |
| | % Completed in time | 33% | 50% | 38% | 20% | 20% | 60% | 63% | 55% | 0% | 43% | 71% | 46% | 47% |
| OPEN SAR | Full SAR Requests | 1 | 1 | 3 | 3 | 3 | 4 | 2 | 8 | 2 | 1 | 7 | 4 | 39 |
| | SARs due | 1 | 1 | 3 | 3 | 3 | 4 | 1 | 9 | 2 | 1 | 7 | 4 | 39 |
| | Completed in time | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 4 |
| | Completed out of time | 0 | 1 | 0 | 3 | 4 | 3 | 3 | 1 | 6 | 3 | 1 | 4 | 35 |
| | % Completed in time | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 100% | 0% | 0% | 50% | 10% |
| S29 | S29 & Annex C requests received | 18 | 21 | 15 | 18 | 18 | 15 | 19 | 6 | 16 | 29 | 24 | 28 | 227 |
| IS | Info Sharing requests received | 12 | 26 | 25 | 24 | 28 | 24 | 35 | 28 | 25 | 38 | 43 | 21 | 329 |
| SEND | SEND requests received | 8 | 9 | 16 | 16 | 12 | 39 | 67 | 6 | 7 | 5 | 5 | 7 | 197 |
| STAT | Stat Checks Received | 7 | 12 | 7 | 7 | 8 | 6 | 10 | 18 | 20 | 13 | 9 | 7 | 124 |

## Appendix C: Information Security Statistics

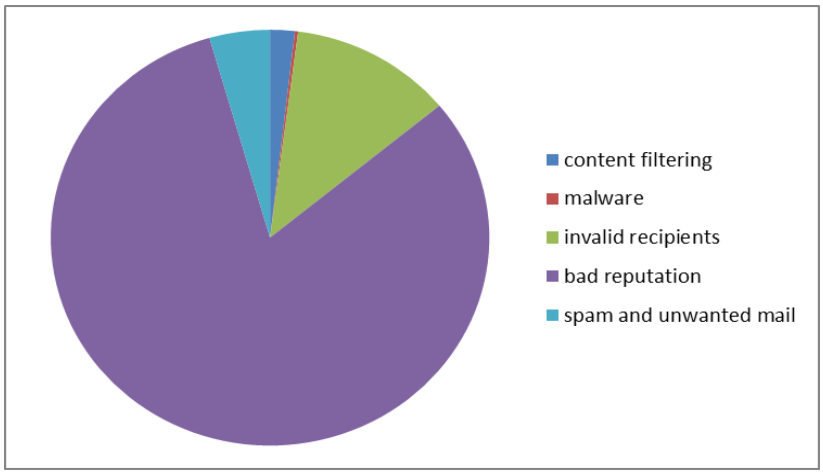
The County council has a layered approach to security protection. The first layer is provided by our internet service provider which will filter out a certain amount of threats and spam message, even before they reach our network.

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 in an attempt to overload the systems.

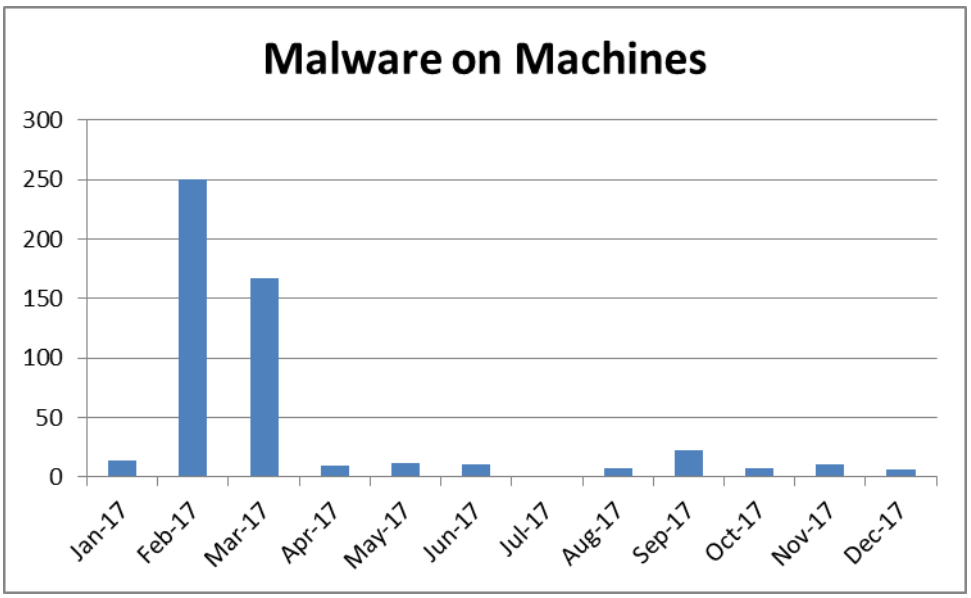
The chart below indicates the number of messages blocked by the DDoS protection each month.



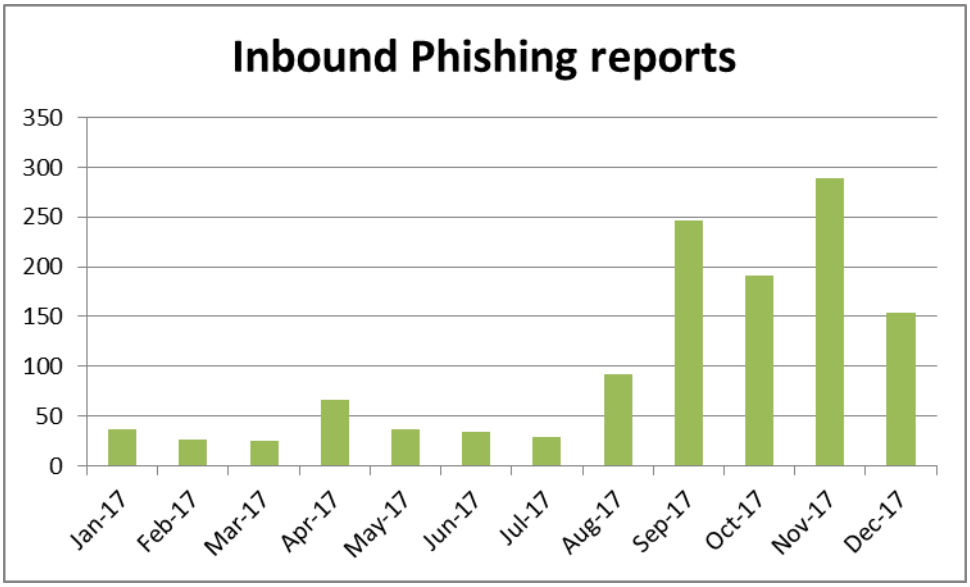

Our networks and systems are further protected by the Symantec Email Gateway. In 2017 the email gateway handled a total of 24,104,353 incoming messages. Of those messages a total of 10,816,188 messages contained single and multiple threats, an average of 55%. The types of threats are identified as followed:




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 – 20 machines per month out) however we did see a spike in February and March. After investigation it is believed that this was a virus that got through our first layers of protection however it was dealt with by the local AV which illustrates the benefit of a multi-layered approach.




Finally, user awareness is key to maintaining the security of our systems. There is an email address where users can report spam and other suspicious emails. The below table shows the amount of reports we have received in 2017 by month.




We believe that the increase in the reporting is in line with the IronPort spam filter no longer available.

*Malicious Links Process*

It is identified that one of the major threats to organisational security is user behaviour. This particularly applies to the use of emails and recognising those that are spam, or contain scam and malicious content. Global communications have been sent sporadically to users, via global emails and standard SCC communication channels such as Team Talk or the intranet, both in response to individual incidents or as general awareness-raising.

There are technical preventions in place, including filtering and blocking software, and measures such as the limitation on downloading executable files. However these are not guaranteed in blocking all potentially malicious emails and these measures have to 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.

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 and further action will be focussed on individual users who have clicked on suspected malicious links or opened attachments containing malicious software.

In April 2017 IGU and ICT implemented a joint process which compared logs identifying potentially malicious actions and user behaviour. From this data the group are able to identify specific sites and trends that are then blocked. There is also a process whereby individual users who have clicked on a malicious link are sent an email with advice and guidance on how to spot malicious emails. From 1 April 2017 to 31 December 2017 we have seen 171 unique users clicking on suspicious or malicious links. There were 6 users who have clicked on links on two or more occasions.

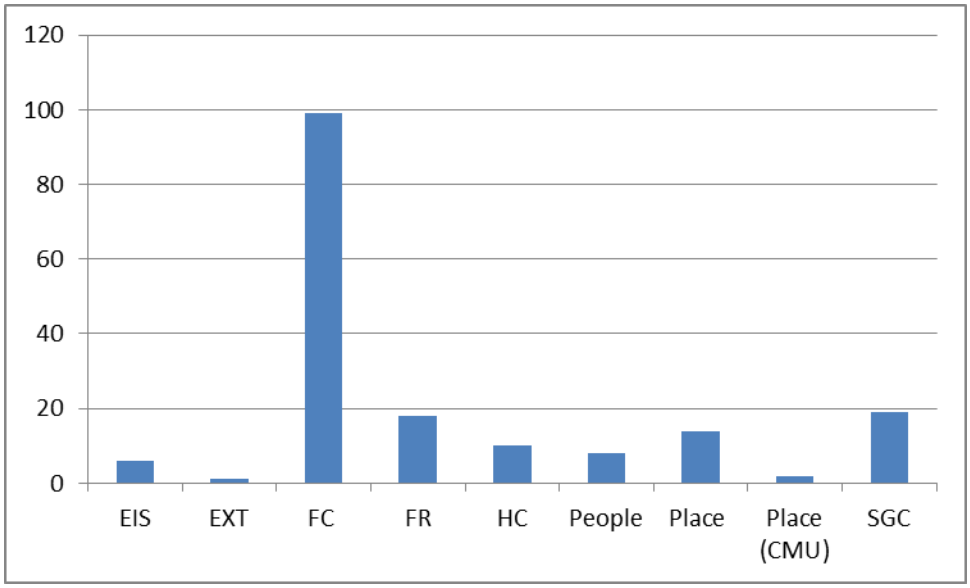



**Figure 1: Number of Clicks per Directorate**

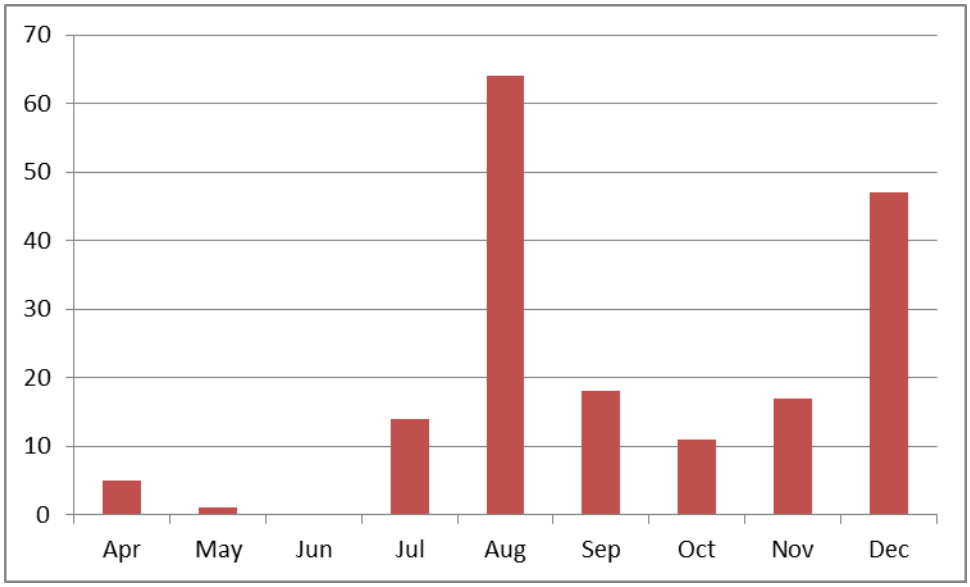
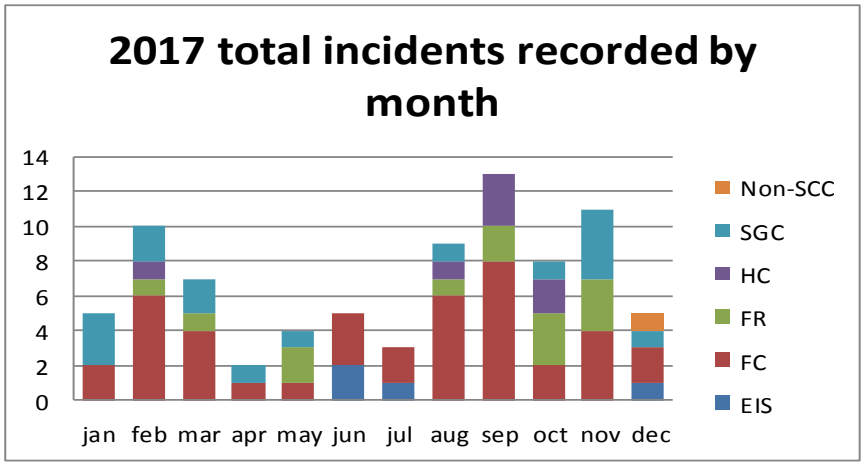



**Figure 2 Number of clicks per month**

## Appendix D: Incident Statistics 2017

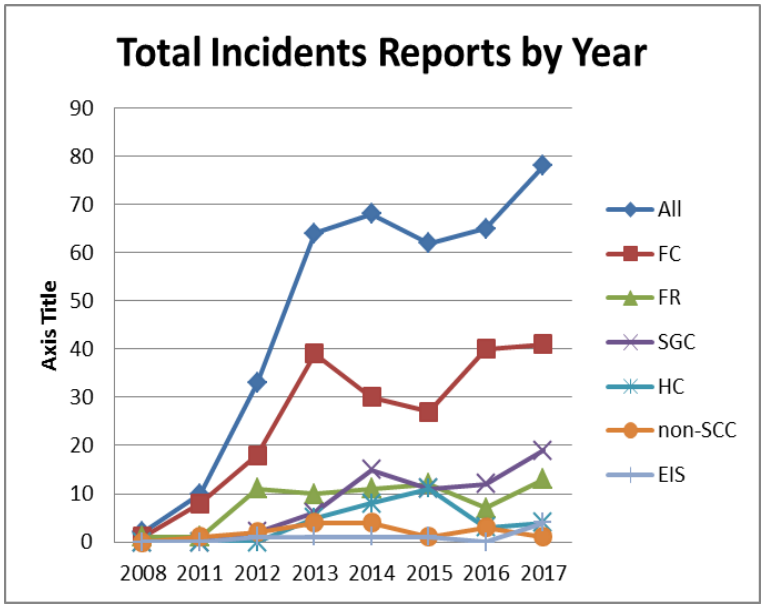
A total of 82 incidents were reported in 2017 which is the highest level of incidents since we began formally recording. This is an average of 7 per month.



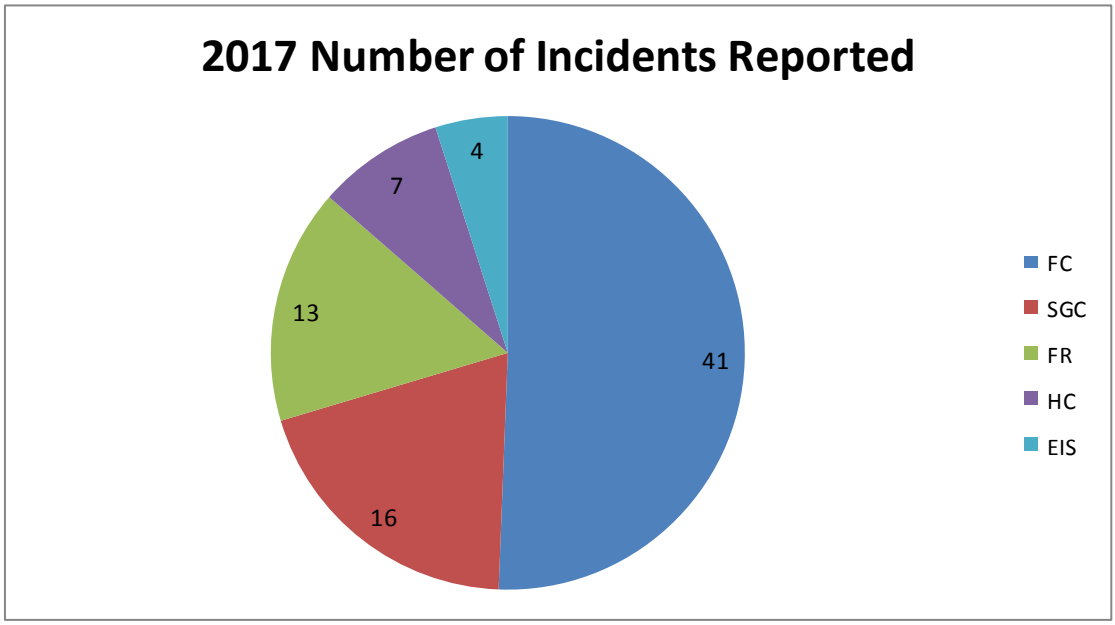

There may be two reasons for this increase:

1. Increased staff awareness of the reporting procedure and increased awareness in general as a result of the mandatory privacy training. In terms of the latter we see more incidents reported in the second half of the year after the training was introduced.

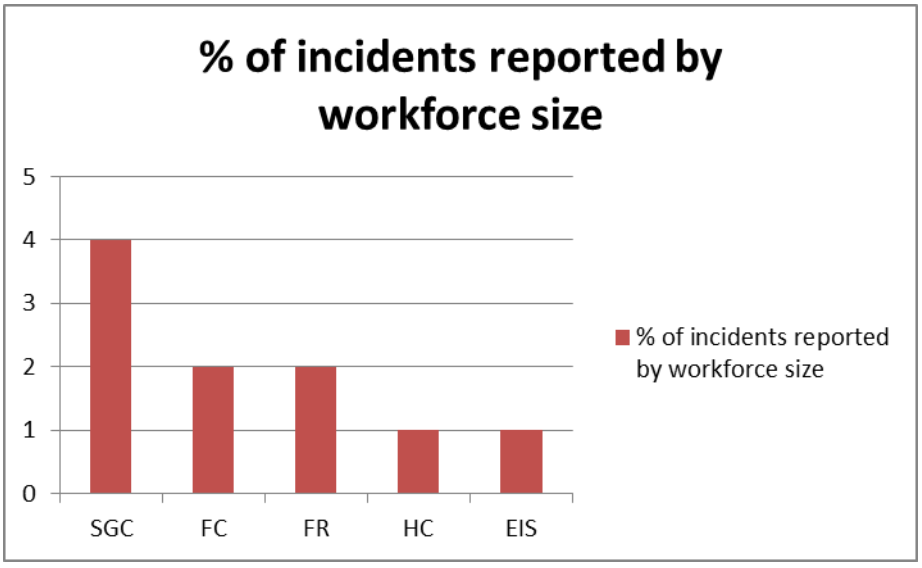
2. An amendment to the recording process to include IT incidents as a result of an internal audit.



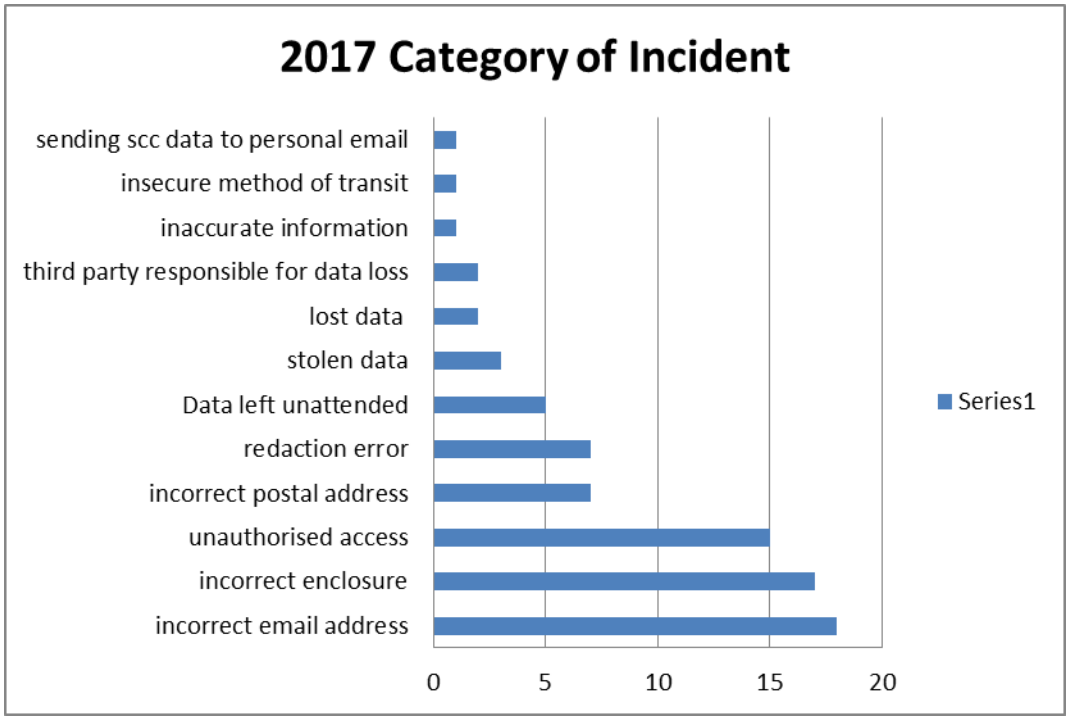
With the service areas F & C have the most reported incidents.

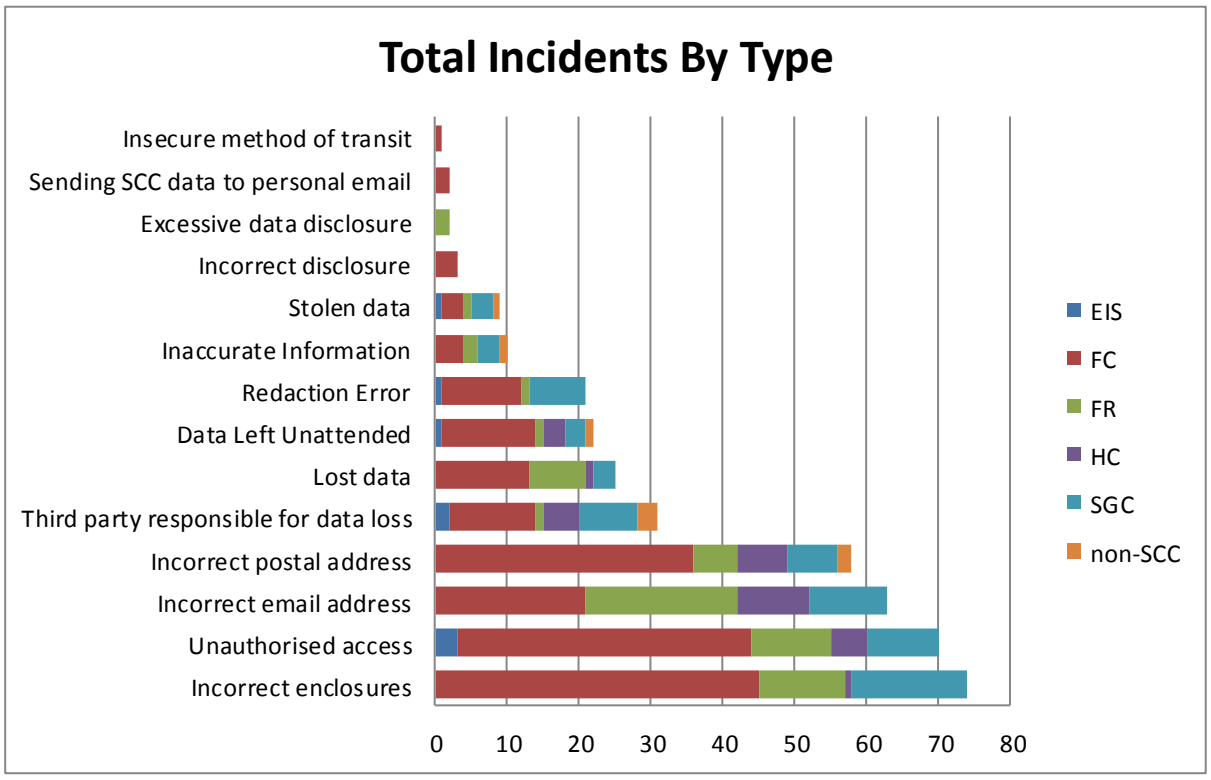



However when taking into account the size of the workforce S,G & C has the highest ratio of incidents per head.



In terms of the type of incident 50% of all incidents were either postal or email correspondence errors (incorrect address and incorrect enclosures).



## Appendix E: Cyber Security Strategy

### Background

*The future of the UK's security and prosperity rests on digital foundations. The challenge of our generation is to build a flourishing digital society that is both resilient to cyber threats, and equipped with the knowledge and capabilities required to maximise opportunities and manage risks.* National Cyber Security Strategy 2016 – 2021

This strategy outlines what measures the Council is taking in order to preserve the confidentiality, integrity and availability of its information and systems and to ensure that SCC can operate and prosper in a digital world.

### Aims of the strategy

To ensure that Staffordshire County Council

- takes a corporate 'one council' approach to protecting information
- adopts the principle of 'privacy by design'
- assures the appropriate security of the data it collects and creates
- takes a proactive role in making information available for customers and partners in secure formats
- manages its information in a secure, efficient and coordinated way with respect for the privacy and confidentiality of customers and partners
- shares sensitive information in a controlled and secure manner only with those to whom it is appropriate to share ensuring bureaucracy is kept to a minimum

### Framework for Strategy

### Vision

To ensure SCC systems and the information we hold are kept securely and are available when needed. Citizens and organisations that provide and share information with us can be confident that we provide adequate protection for that information.

## Legislative Framework

There is a comprehensive and complex legal landscape within which the Council must operate governed by many acts and regulations including, but not limited to:

*Freedom of Information Act 2000*
Requires us to make information available to the public, we have an obligation to proactively publish what is available. It also applies rules on how we manage records and information.

*Data Protection Act 1998*
We have a legal duty to manage personal data in a way that is fair and lawful, not excessive, secure and not hold personal data any longer than is required. We have an obligation to answer requests about personal data from those whose data it is. This is further refined by requirements under the Caldicott principles and NHS information governance toolkit.

*Local Government Act 1972*
We have an implied authority to share certain kinds of information with partners for the economic, social and environmental well-being Staffordshire.

There are also many information requirements in a whole range of legislation relating to Children & Adult Services and the general provision of council services.

*Re-use of Public Sector Information Regulations 2015*
The legislation allows the public to apply for a licence to re-use information held by Staffordshire County Council.

Failure to manage information appropriate can lead to considerable financial penalties.

## Security Principles

### Principle 1

Information is an asset and needs to be available to legitimate users – see Annex A.

**Principle 2**

Information needs to be kept securely and appropriate safeguards need to be employed to ensure that information is protected – see Annex B.

**Principle 3**

Our systems for managing information need to be accessible to everyone who is authorised to use them but must be protected from accidental or deliberate harm – see Annex C.

**Principle 4**

Good information security requires that we create and maintain a culture where staff can confidently navigate the balance between privacy and transparency – see Annex D.

**Governance**

The Cyber Security Strategy is owned by the Corporate Governance Working Group (CGWG) who will collectively and individually be the champion(s) of this strategy across SCC.

The Corporate Governance Working Group will ensure that the environment in which this strategy can be enabled is maintained and will provide an assurance role against performance.

Corporate Governance Working Group will set the agenda for the Cyber Security Strategy and the Senior Information Risk Owners will take responsibility for ensuring that the agenda is achieved.

All employees of the Council are responsible to ensure they adopt the appropriate behaviours for managing information and work towards the aims and objectives of this policy in a one-council approach to the management of information.

## Our Behaviours

As an organisation we will adopt appropriate behaviours in the way we hold, obtain, receive, use and record information. To allow SCC to:

- Ensure we secure and protect sensitive information
- Promote a culture of appropriate sharing with partners
- Encourage openness and transparency
- Dispose of redundant information quickly and effectively
- Ensure information that colleagues and partners are authorised to use is available when needed
- Apply corporate and national security standards where appropriate

## Measuring Performance

All of the projects and activities that deliver this strategy will have both governance and performance measures in place to ensure the delivery meets quality requirements and targets.

This strategy is also about some things which are less tangible to measure such as culture and behaviours found in delivering the strategy.

## Outcomes

By 2020 we will have:

- A clear understanding of what information we hold, how it is used and its security requirements through use of an accurate and up to date Information Asset Register
- Appropriate security in place for all sensitive information and a targeted 25% reduction in information security incidents every year
- Improved information security skills and competencies across the organisation with all staff having completed the Information Security e-learning module
- Earlier identification of privacy risks for projects involving personal data by embedding the use of Privacy Impact Assessments into project methodology

- Improved access to inter-departmental data by having a robust Information Governance process for resolving internal sharing differences
- Better and formal monitoring of SCC data where large quantities are being processed by partners through clear contractual requirements and annual auditing
- Increased protection of the Council's network where staff will not be provided with access to the network until appropriate training has been completed

**Scope**

This strategy applies to all SCC data, regardless of media

**Annex A**

**Principle 1**

Information is an asset and needs to be available to legitimate users.

**Key Tools**

- Information Asset Register
- Protective Marking Scheme
- Corporate Classification Scheme
- Password Policy
- Retention Schedules
- Privileged Access Policy
- Business Continuity Plans

How we meet these requirements:

- Availability of shared filing/Records Manager/SharePoint/service specific databases
- Process to provide/manage access to information/systems to ensure relevant authorisation is given, i.e. starters and leavers process
- Third Party Access Agreements/signing of the Acceptable Use Policy for external users
- Ability to restrict/enable access on filing systems and databases
- Holding records for appropriate periods of time and destroying them accordingly once reached their retention
- Storage and retrieval of manual documents at the Corporate Records Centre
- Processes to handle request for information from staff, service users, members of the public and other organisations
- Senior Information Risk Owner to take decisions on use of data
- Information Asset Owner to identify and classify data sets

**Annex B**

**Principle 2**

Information needs to be kept securely and appropriate safeguards need to be employed to ensure that information is protected.

**Key Tools**

- Password Policy
- Privacy Training & guidance
- Information Security Policy
- Acceptable Use Policy
- Clear desk and screen policy
- Mobile device and removable media guidance
- One Staffordshire Information Sharing Protocol
- Penetration Testing

How we meet these requirements:

- Automatic screen locks after a period of time
- Process to provide/manage access to information/systems to ensure relevant authorisation is given, i.e. starters and leavers process
- Third Party Access Agreements/signing of the Acceptable Use Policy for external users
- Ability to restrict/enable access on filing systems and databases
- Limited manual filing available and lockable drawers/cabinets
- Availability of secure logon facilities when remote working – OWA/Citrix Access Gateway
- Secure storage and retrieval of records from the Corporate Records Centre
- Protective Marking Scheme to identify what security should be afforded to data and who should be able to access it
- Encryption on devices and documents sent outside of the Council's domain
- Secure File Transfer facility for sending data frequently outside of the Council's domain

- Information sharing agreements have provision for audits and checks to be carried out
- Confidential waste service to manage the secure disposal of confidential data
- Mandatory training on induction – Information Security, Privacy, Data Protection and Protective Marking Scheme e-learning
- Penetration Testing takes place annually as part of the Council's PSN compliance accreditation

**Annex C**

**Principle 3**

Our systems for managing information need to be accessible to everyone who is authorised to use them but must be protected from accidental or deliberate harm.

**Key Tools**

- Anti-Virus
- Patching
- Password Policy
- Encryption
- Mobile Device and Removable Media Guidance
- Information Asset Register
- Penetration Testing

How we meet these requirements:

- Encryption for removable media (laptop/USB stick)
- Secure File Transfer facility for sending data frequently outside of the Council's domain
- Third Party Access Agreements/signing of the Acceptable Use Policy for external users
- Public Services Network compliance provides confidence of a secure connection to internet content and allows shared services to be controlled
- Anti-malware defences are in place to scan for malware across the Council's domain
- Network security is in place to protect against external and internal attack
- Vulnerability scan are ran and both desktops and servers are patched when updates are made available
- Availability of secure logon facilities when remote working – OWA/Citrix Access Gateway
- System backups are carried out every night
- Disaster recovery and contingency plans are in place

**Annex D**

**Principle 4**

Good information security requires that we create and maintain a culture where staff can confidently navigate the balance between privacy and transparency.

**Key Tools**

- Security Incident Procedures
- Protective Marking Scheme
- E-learning
- Policy & Guidance
- Penetration Testing

How we meet these requirements:

- Corporate Governance Working Group
- Senior Information Risk Owner to take decisions on use of data
- Information Asset Owner to identify and classify data sets
- Mandatory training on induction – Information Security, Privacy, Data Protection and Protective Marking Scheme e-learning
- Privacy Impact Assessments are completed at the beginning of projects to consider what risks are likely to occur and how those risks can be managed
- A security incident process is in place to allow for formal investigation of incidents involving information. Reports are provided to the relevant SIRO
- A cyber resilience exercise has been completed to assess the effectiveness of dealing with certain unforeseen circumstances