NORTH YORKSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

1 March 2018

INFORMATION GOVERNANCE – PROGRESS REPORT

Report of the Corporate Director – Strategic Resources

1.0 PURPOSE OF THE REPORT

1.1 To update Members on a range of current Information Governance issues.

1.2 To update Members on the progress made to further develop the County Council's Information Governance arrangements.

2.0 BACKGROUND

2.1 Information governance is a holistic approach to managing and protecting corporate information by implementing processes, roles, controls and metrics that treat information as a valuable business asset.

2.2 The County Council has adopted a comprehensive policy framework covering all aspects of information governance. Significant work has been undertaken since then in order to raise awareness of requirements and to ensure compliance. Information is a key asset for the Council (like money, property, or the skills of its staff) and must be protected accordingly.

2.3 Much has been achieved in this area but there is a continuing need to embed a culture of sound information governance, particularly in relation to information security. If this is realised then information can be used even more powerfully by the Council, and partners, to improve decision making and to reduce the financial and reputational risks.

2.4 According to the Terms of Reference of the Audit Committee, its role in respect of information governance is:

(i) to review all corporate policies and procedures in relation to Information Governance

(ii) to oversee the implementation of Information Governance policies and procedures throughout the County Council

2.5 Information governance remains a high risk area as identified on the Corporate Risk Register. This is, in part, due to the ever increasing risks in a hi-tech environment and the behavioural challenges encountered. The current view is that this will be an area of on-going high risk despite the Council's actions to mitigate those risks.

3.0 INFORMATION SECURITY

Information Security Compliance Checks (security sweeps)

3.1 Last year (2016/17) Veritau carried out 6 information security compliance checks, of which 5 resulted in only Limited Assurance. So far in 2017/18, Veritau has completed 9 compliance checks (covering both County Hall and other establishments). Six of the reports have been finalised with two ranked as High Assurance, three Reasonable Assurance and one Limited Assurance.

3.2 Whilst there has been a noticeable improvement in some areas (for example Employment Support Services) sensitive and personal information is still not being secured properly in many offices throughout the Council. The programme of information security compliance checks will therefore continue.

3.3 Non-compliance is brought to the attention of the relevant managers promptly and remedial action is taken as necessary. Reports are also made to the Corporate Information Governance Group (CIGG) and Directorate Information Governance Champions (DIGC). Information security is also discussed at management teams.

Breaches

3.4 The number of reported data security incidents in each quarter since April 2016 is as follows.

Year	Quarter	Red	Amber	Green	Total
2016/17	Q1	4	29	12	45
	Q2	0	11	20	31
	Q3	0	8	13	21
	Q4	1	15	5	21
2017/18	Q1	3	14	5	22
	Q2	0	18	6	24
	Q3	3	10	10	23

Green incidents are unlikely to result in harm but indicate a breach of procedure or policy; Amber incidents represent actual disclosure, but harm is unlikely to be serious; and Red incidents are sufficiently serious to be considered for self-reporting to ICO.

3.5 The overall trend is down over the period, although three red incidents in the latest quarter is disappointing. The majority of incidents are “human error” lapses. A series of visits to team meetings, by managers from Veritau and Technology and Change has been completed. This was to increase awareness of the need for attention to detail and the avoidance of such mistakes.

Recent Information Commissioner's Office Case

3.6 Only one security incident has been reported to the ICO in the last twelve months. A social worker had left her lap-top and paper files in the boot of her car when it was stolen. The risk was that sensitive casework, including details of offences allegedly committed, was in the hands of criminals, who might realise its significance. Following a Veritau audit investigation, the Council explained to the ICO how appropriate training and instruction had been given to the social worker and other staff, and how its policy framework and disciplinary procedures were appropriate and reasonable measures. The ICO agreed and closed the case with no regulatory action to be taken. Although the laptop and case notes have not been recovered, there has been no report of further incident.

4.0 PHISHING EXERCISES

4.1 As with any organisation the Council is under constant threat of cyber-attack and one of the most common is a phishing attack (phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.).

4.2 The Technology and Change service (T&C service) have systems in place to reduce the number of these phishing emails that get into your email inbox, over 400,000 a month are stopped at the perimeter. The number of attacks are increasing and the methods used constantly changing. Although every effort is made to secure the perimeter we can't stop them all and staff become the last line of defence in ensuring the network isn't compromised.

4.3 The processes we have put in place have proved very effective and to measure this we ran a number of controlled phishing exercises to see the response to the email if we did not carry out our normal processes and instead leave the email in everyone's inbox. These exercises have no security impact on the network.

4.4 Over the initial exercises we found that between 10% and 15% of staff would provide their user id and password. However with an increased awareness campaign and running the exercise a number of times we are seeing these figures reduce.

4.5 We will continue to support these exercises with new training material and regular awareness articles on the intranet along with key messages to highlight the importance of the correct staff responses to phishing emails and how to recognise them.

5.0 DATA GOVERNANCE TEAM AND DIRECTORATE INFORMATION GOVERNANCE CHAMPIONS (DIGCs) - ROLES AND RESPONSIBILITIES

5.1 The Data Governance Team has met with all current DIGCs within the Council and has documented their current remits to understand the role and responsibilities that have previously been carried out by the DIGCs. These responsibilities include:

- To provide a point of contact with Senior Management, Directorate staff and Veritau for all information governance issues.
- To coordinate the investigation of any security incident/breach within the directorate with responsible officers to ensure investigations are conducted in

an efficient and standard manner and that all stakeholders are briefed accordingly.

- To provide regular management information updates on breaches/mitigations along with analysis reports.

These responsibilities have moved to the Data Governance Team with each Directorate having an allocated officer to support them. They will work closely with the Directorates supporting them in the use of data and it's governance including compliance and security. They will link with and be supported by the Information Asset Owners and Administrators in each of the Directorates.

6.0 SERVICES' INFORMATION ASSET OWNERS AND REGISTERS

6.1 To comply with the current Data Protection Act and the new General Data Protection Regulations (GDPR) it is important that the Council records all the data it processes to deliver services. This information in each service area is recorded on an information asset register.

6.2 Information Asset registers have largely been completed for all Directorates, and are now under the control of the Data Governance Team in T&C. The registers identify an "information asset owner" for each asset, as well as its location, retention period, and the inclusion of personal data. The register therefore identifies a cohort of owners, so that corporate or cross-service tasks and projects which impinge on information governance issues can be managed more efficiently. As the new Data Protection Bill will oblige the Council to amend its data processing contracts and privacy notices throughout all services, the Register will be an important and useful tool for preparation and compliance. The Register is expected to continue to develop as new information governance objectives and priorities emerge, and should not be regarded as complete, or even able to be completed.

7.0 CYBER SECURITY STRATEGY

7.1 A Cyber Security Strategy that protects the Council's information systems, services and data against unauthorised use, disclosure, modification, damage and loss, has been produced.

7.2 Local authorities must have the public's trust that they will handle their information properly and protect the public, commercial and financial interests they are responsible for. This requires good local cyber security and resilience.

7.3 The Council's Cyber Security Strategy adopts a common set of security goals based on threats that we face. These are:

- Our cyber security defences operate consistently across all technology domains;
- We recognise malicious activity and can act swiftly to limit the damage;
- We understand the extent of our exposure to attack;
- Our systems are developed and maintained to keep step with evolving threats;
- Our people recognise the cyber security risk and act with due care.

7.4 Our approach to Cyber Security and Resilience, is the Prevent, Detect, Respond, Predict framework. We are building on the solid foundations we have by increasing

the functionality of our perimeter network defences enabling us to recognise threats earlier and respond to minimise any potential damage.

7.5 We will continue to offer a range of training and advice to all staff to ensure they are equipped to play a key role as the last line of defence in cyber security.

7.6 We have a Cyber Security response plan in place if we detect any incidents occurring on the network and this plan is regularly tested and updated to ensure it remains fit for purpose.

8.0 DATA PROTECTION BILL, GENERAL DATA PROTECTION REGULATION (GDPR) and the DIGITAL ECONOMY ACT

8.1 The Government has published a Data Protection Bill which will bring together the General Data Protection Regulation (GDPR) and the Law Enforcement Directive within UK law. The majority of the requirements are an extension of those already in place and the Council is able to utilise the good controls and processes previously put in place for the Data Protection Act.

8.2 The Data Governance Team and Veritau are working through a compliance action plan with service areas and creating a communication plan to ensure there is a good awareness and understanding of the implications on the use of data during service delivery.

8.3 The Digital Economy Act 2017 also has a significant impact on processing personal data within the Council, and a review of Information Governance policies will also take account of many of its features.

8.4 The Digital Economy Act allows the ICO to charge fees. The Department for Digital, Culture, Media and Sport (DCMS) is currently consulting on a charging structure which includes fees of up to £1,000 a year for large organisations such as NYCC.

8.5 A key area to ensure compliance is understanding all the data the organisation owns, the Data Governance Team are working with Information Asset Owners in each Directorate to document this appropriately, this work does require the support of senior management to ensure it is completed and maintained.

9.0 INTERNET BANDING

9.1 Unmanaged Internet access presents many challenges and introduces unnecessary risk to the Council. Internet filtering helps the Council manage productivity, reduce legal liability and improve bandwidth to make employee Internet use efficient and effective.

9.2 There are currently 10 Internet bands in use, all staff have access to the default band with the others provided if approved by an Assistant Director. This allows access to such sites as social networking and other sites that may be required for certain job roles.

9.3 The implementation of a new firewall infrastructure creates an opportunity to review the internet filtering that is currently in place in relation to employees' access to the Internet from Council owned assets. To meet the Council's staff requirements and ways of working the number of Internet bands will be reduced to 4.

9.4 The current risk mitigation measures will continue to be in place and the move to the new firewall together with increased functionality will heighten the security infrastructure further.

9.5 Band 1 is the default staff access band, all the others require a business need to be provided. The Internet bands are:

- Band 1 –Staff Access
- Band 2 – Web Based Personal Email
- Band 3 – Online Network Storage and Backup
- Band 4 – Special Access (used to allow access for investigations)

10.0 **RECOMMENDATIONS**

10.1 Members are asked to note the progress made on information governance issues.

GARY FIELDING
Corporate Director – Strategic Resources

County Hall
Northallerton

March 2018

Authors of report: Fiona Sowerby, Corporate Risk and Insurance Manager, Max Thomas, Head of Internal Audit and Jon Learoyd, Head of Technology Solutions
Tel 01609 532400, 01609 532143 and 01609 536389

Background papers: None