ITEM 13

NORTH YORKSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

5 DECEMBER 2013

INFORMATION GOVERNANCE

Report of the Corporate Director – Strategic Resources

1.0 PURPOSE OF THE REPORT

1.1 To update Members on the progress on Information Governance arrangements.

2.0 BACKGROUND

2.1 In March 2010, the County Council adopted a comprehensive policy framework covering all aspects of Information Governance (IG). Significant work has been undertaken since then in order to ensure that policies and procedures are in place. Much has been achieved in this area and the focus now needs to turn to ensuring maximum compliance and embedding a culture of sound information governance, particularly in relation to information security.

2.2 This report seeks to provide an update on progress since the governance themed meeting of the Audit Committee in June 2013.

3.0 INFORMATION GOVERNANCE FRAMEWORK

3.1 The IG Framework incorporates the core measures identified in the Government's Data Handling review, the HMG Security Framework and ISO 27001. The objective of the Framework is to set out how the County Council will improve its information management by establishing:

- core measures to protect personal data and other information across the County Council.
- a culture that properly values, protects and uses information.
- stronger accountability mechanisms within the County Council.
- stronger scrutiny of performance in relation to the above.

3.2 The various IG policies that are born out of the Framework are attached as **Appendix 1** for information.

3.4 The Corporate Director – Strategic Resources has been appointed as the County Council's Senior Information Governance Risk Owner (SIRO). The SIRO chairs the **Corporate Information Governance Group (CIGG),** which addresses new and emerging issues as well as coordinating the development of the IG Framework. The focus of CIGG has changed recently to enable the group to take a more strategic oversight of information governance. Membership of the group will henceforth be at Assistant Director level and include the Head of Internal Audit.

3.5 The priority areas for CIGG to address in the future are as follows:-:

(a) review and updating the County Council's Information Governance strategy;

(b) review of training material and delivery;

(c) information sharing with partners;

(d) enabling agile working for staff whilst balancing information security risks;

(e) role of social media; and

(f) further identification of gaps and actions required to address.

3.6 It is recognised that the operational demands, such as those to support more mobile working, will raise some significant IG risks. These issues will need to be considered explicitly and sufficient safeguards put in place to mitigate those risks where possible. The Audit Committee will be updated on issues which raise such fundamental issues.

4.0 INFORMATION SECURITY

4.1 Since 6 April 2010, the Information Commissioner's Office (ICO) has had the power to fine organisations up to £500,000 for serious data breaches or losses (the previous maximum fine that could be imposed was £5,000). In the period since the last report, the ICO has imposed a significant number of fines on local authorities – details are attached as **Appendix 2**.

4.2 Within NYCC, a variety of data security incidents have been reported since December 2012. These include:

- fourteen incidents where personal or sensitive personal data was sent by post to the wrong recipient;
- eleven incidents where e-mails containing personal or sensitive personal data was sent to the wrong recipient;
- two cases where personal or sensitive personal data relating to a third party was incorrectly included in responses to subject access requests;
- one instance where a surplus filing cabinet was sold but was found to contain sensitive personal data;
- two thefts of personal data;
- three cases where files containing personal data were lost/left in a public place; and
- one case when personal data was left overnight in a bin instead of being shredded.

4.4 In each of the security incidents listed above action was taken immediately to recover the data and each incident was subject to a formal breach review by either an independent officer appointed by the DIGC, or in some cases directly by the DIGC or by Veritau. Recommendations arising from the breach investigations were implemented locally and, where Veritau identified a pattern, these were brought to CIGG for consideration.

4.5 The incidents detailed above were largely isolated incidents and none fell within the criteria requiring reference to the Information Commissioner. The Information Commissioner did, however, request that its enforcement team investigate an incident within the Council. The ICO was subsequently satisfied that the Council had responded appropriately to the incident but it does highlight the increasing vigilance of the ICO.

4.6 Veritau's auditors have carried out further unannounced visits to County Council premises. These visits found that a large quantity of information and data was unsecured including significant numbers of sensitive client data and staff data. Laptops and items of equipment such as digital cameras, projectors and mobile telephones were also found unsecured through out the visits. Overall, standards were well below expected levels. Individual reports with the detailed findings were issued to each directorate area in respect of all of the security visits undertaken.

4.7 Further visits are planned throughout the remainder of the year. A summary audit report has been issued to the SIRO and an action plan identified.

5.0 ACTIONS TO ADDRESS INFORMATION SECURITY

5.1 An action plan has been produced specifically to address the deficiencies identified in information security. The key highlights are:-

a) We will review the arrangements for allocating laptops. If there are a number of laptops that are often left in an office then perhaps their use is infrequent and they should be pooled and located in a central location with ICT.
b) Messages will be reinforced to staff about the need for vigilance and the risk of theft and the subsequent financial and reputational loss. Staff will be reminded of their obligations and the possible disciplinary consequences of a failure to comply. Key messages, team meetings and the intranet will be used to promote and embed the message.
c) Arrangements for VPN tokens will be reviewed to establish if there is a better way of "booking out" VPN tokens.
d) A report will be taken to Management Board and the Audit Committee (hence this paper) in December 2013 outlining the key challenges, a series of proposals (many of which are outlined below) and updates on information governance.
e) Each DIGC has produced a short action note which can be used to inform the general approach and to ensure that there is sufficient action being taken to address the issues raised.
f) Messages are to be relayed to managers and staff about the serious nature of information governance and how it is "part of the day job". These messages will be conveyed countywide. Consideration is currently being given as to how a campaign is carried out – a series of articles, messages to staff etc. or whether there is a more formal campaign.
g) Veritau are requested to carry out more compliance visits and on this occasion sufficient details will be required to attribute non-compliance to individuals and for that to be reported explicitly. Where incidents are of a sufficiently serious nature then disciplinary action will be investigated.
h) Guidance will be produced to advise people on how they can keep their equipment and information safer. This will be informed by experience from the compliance visits – e.g. clear desk policy combined with lockable cabinets / drawers etc.

i) Information security training to be reviewed to establish if more needs to be done or done differently. Consideration will then be given to what is then mandated or otherwise.

5.2 It is almost inevitable that there will be security breaches despite all of the above actions. The Council needs to ensure though that it is systematic in its approach and learns lessons where incidents arise. Further suggestions on possible actions are welcomed from the Committee.

6.0 FREEDOM OF INFORMATION (FoI) ACT 2000

6.1 Between 1 November 2012 and 31 October 2013, the County Council received a total of 1,196 FoI requests. This compares with 1,069 received between the same period in 2011/12 (a 12% increase). The County Council has responded to 97.7% of these requests within the 20 working days time frame defined by the legislation (compared to a performance target of 95%).

6.2 The challenging financial climate is likely to see a further increase in FoI requests.

7.0 RECOMMENDATION

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

Gary Fielding
Corporate Director – Strategic Resources

November 2013

Appendix 1

NYCC INFORMATION GOVERNANCE POLICY MAP

September 2013

	Resp.	Approved	Next Review
Currently Under Discussion at CIGG			
Document and Records Management (inc R&D schedule and email archiving)	IK		**Nov 13**
Charges for enquiries	GF		
External cyber bullying & internet harassment policy & guidance	KH		
To be Drafted			
Information Security Management Standard - ISMS (suite of technical IT policies)	CC		
Service Continuity Management Policy	CC		
Approved by CIGG			
Information Governance	RB	Mar 10	Mar 11
Data Protection	RB	Dec 10	Dec 11
Freedom of Information	RB	Dec 10	Dec 11
Data Security	CC	May 12	May 13
Data Quality	RB	May 12	May 13
Records Management	IK	Sept 10	Sept 11
Anti Virus Policy	CC	May 12	May 13
Blackberry Policy (not yet “mobile phones”)	CC	May 12	May 13
Data Processing (by Contractors) Policy	RB	Sept 13	Sept 14
Email Policy	CC/KH	Sept 12	Sept 13
Gov Connect Usage Policy	CC	May 12	May 13
Info Security Incident Policy/Procedure	RB	Sept 13	Sept 14
Information Sharing with Partners Policy	RB	Sept 13	Sept 14
Internet Usage Policy	CC/KH	May 12	May 13
Monitoring Policy	CC	Dec 10	Dec 11
Network Access Policy	CC	May 13	May 14
Non-NYCC Network Access	CC	May 13	May 14
Portable Media	CC	May 12	May 13
Privacy Statement (Customer Service Centre) [call recording]	RB	Oct 10	Oct 11
Scanning Policy	IK	Jun 12	Jun 13
Security Classification Policy	RB	May 11	May 12
Software Policy	CC	May 12	May 13
Use of Social Media Policy	HE	Nov 10	Nov 11

Appendix 2

Information Commissioners Office (ICO) Action Against Councils

Leeds City Council fined £95,000 - sensitive personal details about a child in care sent to the wrong person, revealing details of a criminal offence, school attendance and information about the child's relationship with their mother.
Devon County Council fined £90,000 - a social worker used a previous report as a template for an adoption panel report they were writing, but a copy of the old report was sent out instead of the new one. The mistake revealed personal data of 22 people, including details of alleged criminal offences, extended family details, religion and mental and physical health
London Borough of Lewisham fined £70,000 - a social worker left sensitive documents in a plastic shopping bag on a train, after taking them home to work on.
City of Glasgow Council fined £150,000 - following the loss of two unencrypted laptops, one of which contained the personal information of 20,143 people
Hatton Borough Council fined £70,000 - when a council employee sent a letter about an adopted child to the birth mother, and mistakenly included a covering letter giving details of the adoptive parents' home address.
Islington Borough Council fined £70,000 - after personal details of over 2,000 residents were released online. The information was inadvertently released in response to a freedom of information request, and revealed sensitive personal information relating to residents housing needs, including details of whether they had a history of mental illness or had been a victim of domestic abuse.
Aberdeen City Council fined £100,000 - council employee accessed documents, including meeting minutes and detailed reports from their home computer. A file transfer program installed on their home computer automatically uploaded the documents to a website, publishing sensitive information about several vulnerable children and their families, including details of alleged criminal offences; and
North East Lincolnshire Council fined £80,000 - serious data breach resulted in the sensitive information of hundreds of children with special educational needs being lost. The information was stored on an unencrypted memory stick and has been missing since the 1 July 2011 when the device was left in a laptop at the council's offices by a special educational needs teacher. When the teacher returned to the laptop the memory stick was gone and it has never been recovered.

Other breaches resulting in Councils being required to sign undertakings:-

Mansfield District Council - following a number of incidents where personal data of housing benefit claimants was disclosed to the wrong landlord.
East Riding of Yorkshire Council - following incidents last year in which personal data was inappropriately disclosed
Central Bedfordshire and Bedford Borough Councils - relating to the removal of legacy data from a social care database and in relation to the preparation of planning application documentation for publication
Cardiff City Council - the Council agreed to put measures in place to ensure greater compliance with subject access requests.
Luton Borough Council - following several incidents involving inappropriate handling of sensitive personal data. Investigation of these incidents revealed that previous recommendations made by the ICO had not been implemented.
Aberdeen City Council - after inadequate homeworking arrangements led to 39 pages of personal data being uploaded onto the internet by a Council employee.