NORTH YORKSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

3 March 2016

INFORMATION GOVERNANCE – PROGRESS REPORT

Report of the Corporate Director – Strategic Resources

1.0 PURPOSE OF THE REPORT

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

2.0 BACKGROUND

2.1 Since 2010, the County Council has had a comprehensive policy framework covering all aspects of Information Governance (IG). Significant work has been undertaken since then in order to raise awareness of the policy requirements and ensure compliance. Information is a key asset for the Council (like money, property, or the skills of its staff) and must be protected accordingly. Much has been achieved in this area but there is a continuing need to maximise compliance and embed a culture of sound information governance, particularly in relation to information security.

2.2 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

2.3 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 <u>despite</u> the Council's actions to mitigate those risks.

3.0 INFORMATION GOVERNANCE POLICY FRAMEWORK

3.1 The objective of the policy 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 original policy suite has been reviewed and revised to take account of recent developments and current best practice. The opportunity has also been taken to consolidate and simplify the previous policies. This updated suite of policies now consists of:

- **Information Governance Policy**
  This Policy sets out the value of information as a key asset for the council (like money, property, or the skills of its staff) and how it must be protected accordingly. It provides details including the framework for data and its security, as well as employees' roles and responsibilities.

- **Personal Privacy Policy**
  This Policy aims to guide the Council in managing the personal data it holds, to protect the rights of data subjects; and to allow the Council to effectively use the personal data it holds as a resource for the delivery of its services, both to individuals and to the public as a whole. It applies to all Council employees, Council contractors, volunteers and other unpaid or temporary workers (for example, work experience placements) and elected Members.

- **Information Access Policy**
  This Policy sets out how the Council will fulfil its duty to disclose information to enquirers under the Data Protection Act 1998, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004. The Council has obligations and responsibilities in responding to requests under this legislation and this Policy sets out those responsibilities and provides a framework for managing and responding to requests.

- **Document and Records Management Policy**
  This policy provides a framework for managing the Council's records and documents. Effective management of records and documents (such as identifying what records need to be kept and for how long) helps the Council to deliver quality services for example, by having timely access to meaningful and appropriate information, responding appropriately to information requests from the public, and by protecting records from threats, including unauthorised or accidental disclosure. This policy applies to employees, contractors, volunteers and other unpaid or temporary workers.

- **Mobile Device Policy**
  This Policy states how employees or workers of the Council, Members and contractual third parties who have access to a mobile device for Council business, should use a mobile device whilst working for the Council. It outlines personal responsibilities and advises what must and must not be done.

3.3 For information, the published intranet versions include hyperlinks to related documents such as the Publication Scheme and the ICO website.

3.4 It is recognised that operational demands and changes in working practices , such as those to support more mobile working, will potentially raise significant IG risks. These issues will need to be carefully considered and sufficient safeguards put in place to mitigate those risks where possible.

4.0 INFORMATION SECURITY COMPLIANCE

Information Security Compliance Checks

4.1 Internal Audit has been carrying out unannounced compliance audits relating to information security for some time. Out of the 13 audits that have been carried out in the past year, 8 have been classified as 'Limited Assurance'. Examples of non-compliance include:

- Sensitive data relating to children and adults being left unsecured, such as child protection reports; health details and details of physical abuse; fostering files; application forms for residential disabled parking; deprivation of liberty forms; care plans; clients' files and lists containing personal details
- Sensitive data relating to staff being left unsecured, such as details of staff sickness; disciplinary files and employees' personal files and information
- Unsecured laptops and passwords and PIN numbers

4.2 Where non-compliance has been identified this has been brought to the attention of the relevant managers promptly with appropriate remedial action taken as necessary. Details of non-compliance have also been reported to the Corporate Information Governance Group (CIGG) and directorate information governance champions so as to help develop further guidance, training and other awareness raising measures. Information security is now regularly considered by directorate management teams and a number of services have instigated their own ongoing compliance checks.

4.3 There are also examples of good practice such as at Swaledale House, Colburn and Belle Vue Square, Skipton where the audits were classified as 'High Assurance'.

Data Security Incidents

4.4 There have been 68 data security incidents reported in the first 9 months of 2015/16. All reported incidents are investigated with the most serious ones being referred to Internal Audit. The majority of these incidents have been caused by human error. Typical examples include:

- Documents sent to incorrect recipients by email or post (because address or email details were not properly verified);
- Documents containing personal information left in unsecure locations;
- Documents containing personal information attached to emails in error;
- Documents containing personal information incorrectly enclosed with information relating to someone else;
- Documents delivered to the incorrect address (by Royal Mail);
- Personal information not deleted when forms or letters re-used;
- E-mail recipients disclosed because the blind copy function not used;

- Documents left on printers.

4.5 The reporting of incidents has increased significantly in the last few years. On the surface this may not be seen as a positive sign but it does indicate that there is heightened awareness of the issues. Staff are encouraged to quickly flag breaches and data security incidents so that recovery arrangements can be made and lessons subsequently learned. It is accepted that human error will never be eradicated but care and attention is essential when handling sensitive data. For this reason, work is ongoing to raise awareness, provide guidance and the necessary tools (for example secure e-mail facilities) and test compliance.

5.0 MANDATORY TRAINING

5.1 There has been mandatory training in place for some time. The 3 in depth mandatory online learning courses have recently been revised and re-launched. These must be completed by all identified employees by the end of March 2016. If this is not achieved then the employee's annual increment could be in jeopardy. The introductory course is presently being refreshed and is mandatory for everyone else.

5.2 The online courses have helped employees to understand their responsibilities in relation to personal and sensitive information. However, as can be seen in Section 4, there remains a concern that the connection between the training and the application of the knowledge learnt is not always being made by employees.

6.0 DATA SHARING WITH PARTNER AGENCIES

6.1 There is a need for the Council to share information with a variety of external partners. Whether this is between social care and health, District Councils or the Police, the information governance requirements and standards that have to be adhered to are the same.

6.2 It is accepted that there is already a great wealth of information sharing practice happening within the council and externally with key partners. However it has been identified through various information governance sources that we need to align our processes to ensure we are sharing information appropriately, at the right time, with the right people and by the correct means.

6.3 In response to this significant progress has been made, and one of the major pieces of work completed with partners over recent months is the production of a collaborative Multi Agency Overarching Information Sharing Protocol (the "Protocol").

6.4 The aim of the Protocol is to create a positive culture of sharing information and facilitate more effective data sharing practices between partner agencies, with the ultimate aim of improving service delivery. Refusing to share data can be a risk just as much as sharing too much data.

6.5 The Protocol applies to all information being shared by signatory partner agencies, with the aim of establishing the types of data which these agencies will share, how

data is handled and the legislation which allows the information to be shared, as well as outlining processes for developing individual Information Sharing Agreements.

6.6 The Protocol has been developed to ensure that information is being shared lawfully, appropriately and in compliance with best practice. The Protocol aims to establish consistent principles and practices to govern sharing of personal and non-personal information taking place within and between partner agencies. The ethos of the Protocol is for partner agencies to share information in all situations to improve service delivery and resident outcomes and to support safeguarding, except where it would be unlawful to do so.

6.7 The Protocol has already been signed by City of York Council, NY Fire and Rescue Authority, NY Police, York Teaching Hospital NHS Foundation Trust, Scarborough Borough Council, Richmondshire District Council, Ryedale District Council, Craven District Council, Selby District Council, Harrogate Borough Council, Broadacres, Yorkshire Coast Homes, Together Housing Group and Veritau. Hambleton District Council has indicated an intention to sign the Protocol. A number of other NHS organisations are also considering becoming signatories.

6.8 The Steering Group is working to extend the list of signatories. NHS organisations including CCGs, housing associations and other public bodies are being approached as part of the roll-out.

7.0 **RECOMMENDATIONS**

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

GARY FIELDING
Corporate Director – Strategic Resources

County Hall
Northallerton

March 2016

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

Background papers: None