AUDIT COMMITTEE
26 SEPTEMBER 2013

ITEM NO. 8

INFORMATION GOVERNANCE PROGRAMME PROGRESS REPORT

SUMMARY REPORT

Purpose of the Report

1. The Chief Officer's Board (COB) is required to report six monthly to the Audit Committee on progress and planned developments of the information governance programme.

Summary

2. Information governance is an 'above the line' risk on the corporate risk register. This report sets out progress in the delivery of the information governance programme, focussing on the following key areas

   (a) Information security policy
   (b) Information risk assessment and improvement action plan
   (c) Information governance training and awareness
   (d) Information classification and handling
   (e) Information sharing
   (f) Information security incidents
   (g) Data quality

   and also addresses particular issues relating to

   (h) the transfer of Public Health responsibilities to local authorities, and
   (i) the transparency agenda

3. The Council continues to make steady progress on delivery of the information governance programme against a background of re-organisation and financial constraint. Critical to the effective implementation of the programme is information risk management, as it identifies and evaluates risks to enable available resources to be used to best effect. Significant progress has been made in this area and action plans are being developed by Heads of Service to ensure improvements are implemented across services effectively and in a timely manner.

Recommendation

4. It is recommended that progress on the implementation of the Information Governance Programme be noted.

Reasons

5. The recommendation is supported to provide the Audit Committee with evidence to reflect on progress in delivery of the Council's Information Governance Programme.

Paul Wildsmith
Director of Resources

Brian James, Head of Corporate Assurance : extension 2140
Peter McCann, Information Security Manager, extension 156494

Background Papers

Local Public Services Data Handling Guidelines, Version 2, August 2012

S17 Crime and Disorder	There is no specific crime and disorder impact.
Health and Well Being	The report refers to information management risks on the transfer of Public Health responsibilities to local authorities.
Carbon Impact	There is no specific carbon impact.
Diversity	There is no specific diversity impact.
Wards Affected	All wards are affected equally.
Groups Affected	All groups are affected equally.
Budget and Policy Framework	This report does not recommend a change to the Council's budget or policy framework.
Key Decision	This is not a key decision.
Urgent Decision	For the purposes of the 'call-in' procedure this does not represent an urgent matter.
One Darlington: Perfectly Placed	There is no specific relevance to the strategy beyond a reflection on the Council's governance arrangements.
Efficiency	Implementation of effective information governance systems and procedures has a positive impact on efficiency.

MAIN REPORT

Background

6. Information governance is an 'above the line risk' on the corporate risk register. This is a generic risk reflecting a number of specific information management areas that are currently assessed as high risk to the Council and as such require appropriate treatment.

7. The information risk management process informs the information governance work programme, ensuring that areas for improvement are identified and prioritised. An information risk actions toolkit has been developed to support the consistent implementation and application of improvements across services.

Current Position

Information Security Policy

8. The Council's corporate policy statement endorsed by the Chief Executive and approved by Cabinet in December 2009 sets out the policy and objectives of information security management. The policy statement is reviewed annually by the Information Security Manager and remains relevant and fit for purpose in its original form.

9. The publication 'Local Public Services Data Handling Guidelines (Version 2 August 2012)' produced by the National Local Authority Warning, Advice and Reporting Point (NLAWARP) Programme builds on the 'Data Handling Procedures in Government' published by Sir Gus O'Donnell, Cabinet Secretary, in June 2008. The guidelines identify a minimum set of policies and procedures which should be implemented. The guidelines are shown in Appendix 1 together with the Council's current position which shows good progress has been made.

Information Risk Assessments

10. A risk actions toolkit has been published and action plans are currently being completed by Heads of Service for each service area. The plans will be approved by the relevant Assistant Director and successful and timely completion of the actions will be monitored by Chief Officers Board (COB).

Information Governance Training and Awareness

11. Mandatory face-to-face awareness training for Heads of Services was developed and delivered in June 2012.

12. The Employees Guide to Information Security has been rolled out using a policy management system, and is part of the corporate induction pack. The Guide contains protocols that clearly set out how information should be managed, and the system requires employees to confirm that they understand the protocols and their responsibilities in relation to them. This confirmation is held as an electronic record and provides evidence that staff are given appropriate awareness training. The

Guide also advises that depending upon the seriousness of a breach the Council could take disciplinary action up to and including dismissal.

13. For those staff without access to the system a leaflet has been developed covering information management issues and responsibilities that will be distributed by line managers and staff will have the opportunity to raise any queries or concerns they may have. The leaflet is currently being printed with a view to distribution to staff in October 2013.

14. In addition to the mandatory Employees Guide to Information Security a range of optional information governance courses is being developed for delivery through the policy management system for which Heads of Service will be requested to nominate staff to complete as appropriate. Pending availability of the courses face to face training is being delivered on request covering key aspects of Data Protection and Information Security.

Information Classification and Handling

15. An information classification and handling policy has been communicated through the risk actions toolkit. Information classification and handling covers all types of information in all forms, presenting a range of different risks and requiring a number of different solutions, from manual paper based processes to sophisticated technical controls. Procurement of a classification and protect marking solution for electronic documents and emails is currently being progressed.

Information Sharing

16. The Chief executive re-signed the refreshed over-arching Multi-Agency Information Sharing Protocol on behalf of the Council in April 2013. This protocol covers key partners, e.g. County Durham and Darlington NHS Foundation Trust, Durham Constabulary and Tees, Esk and Wear Valley NHS Trust, and sets out the high level commitments and responsibilities of the signatories with regards to information sharing.

17. The Complaints and Information Governance (CIG) Team is concentrating its effort on working with these key partners to ensure that service-level information sharing agreements are implemented in an efficient and effective manner, reducing duplication where possible. In addition, services are continuing to develop sharing agreements with other parties where necessary, with the support of the CIG Team.

Information Security Incidents

18. The Council's information security incident reporting procedure is embedded and staff are aware of and understand the importance of incident reporting and management.

19. The reporting and subsequent management of security incidents provides the opportunity to improve processes, procedures and training, and to identify information security themes that support, supplement and validate the information

risk management process.

20. The ICO has issued guidance on the requirement to notify them of information security breaches. In line with this guidance management of the Council has reported no information security breaches to date.

Data Quality

21. The Chief Officer's Executive have approved a corporate Systems and Information Strategy and agreed that COB, chaired by the Director of Resources, will act as the Systems and Information Governance Group. The Group is overseeing a programme of work to produce a development plan for all the Council's major business systems and through a series of business process improvements will systematically address data quality.

Public Health

22. The transfer of public health responsibilities to the Council from NHS County Durham and Darlington by April 2013 was managed through the local transition plan, and there were no significant information management risks identified with the transfer. The Council is currently completing a code of connection for approval to access the appropriate NHS systems.

Transparency

23. The CIG Team will be presenting the third annual Freedom of Information, Environmental Information and Subject Access Request report to COB in October 2013 and Cabinet in November 2013. The report will make further recommendations regarding the publication of frequently requested information with the aim of reducing the costs of responding to individual requests for information and improving transparency.

24. The Protection of Freedoms Act 2012 has amended sections 11 and 19 of the Freedom of Information Act 2000 (the FOI Act) giving new rights to receive datasets in a form capable of re-use. For the first time, the FOI Act will give users the right to re-use datasets under the terms of the Open Government Licence (OGL). The amendments also require the Council to publish any requested datasets as part of its publication scheme, if appropriate to do so. The provisions came into force on 1 September 2013.

25. It is important to note that the changes do not give new rights of access – they are concerned with form and format and the ability to re-use datasets once the Council has decided that no exemptions or other provisions (such as the cost limit) in the FOI Act apply.

26. The Ministry of Justice has published a 'Code of Practice (Datasets)', which explains how public authorities are expected to make datasets available to the public and, to support the implementation, the Information Commissioner's Office has also published a guidance note entitled 'Datasets' The CIG Team is currently reviewing information request handling processes and procedures to address the

requirements of this guidance.

Conclusion

27. Delivering regular appropriate awareness/training and having documented, well understood and consistently applied policies, procedures and guidelines remains critical to the development and continual improvement of the information management system. The information risk assessment process is embedded and working well and we need to ensure that the actions identified for the treatment of significant risks are implemented properly and in a timely manner. The development of improvement action plans by Heads of Service based on the risk action toolkit will facilitate this.

28. The information governance programme is well structured and the Council continues to make steady progress on its delivery against a background of re-organisation and financial constraint. However, the overall information governance risk will remain 'above the line' until the improvement action plans are delivered and associated controls are embedded and proven to be effective.

Outcome of consultation

29. No formal consultation was undertaken in production of this report.

Appendix 1 – Minimum Set of Policies and Procedures

Issue	Status
Acceptable use	Covered by the Employees Guide to Information Security which is being rolled out via a policy management system (see paragraph 12)
End user awareness training	• On-line information security awareness course available (see paragraph 12) • Face to face training being delivered on request (see paragraph 14)
E-mail usage	Policy approved and published
Use and control of portable media	• Encryption controls in place • Risk actions toolkit guidance under development
Home and mobile working	Policy and procedures to be reviewed
Secure document printing	Process implemented
Manual (paper) document handling	• Information classification and handling guidance included in risk actions toolkit • Confidential waste project completed
Handling of faxes	Policy approved and published
Secure disposal and destruction	• Policy and procedure in place for ICT equipment • Confidential waste procedures in place
Information asset valuation	In place as part of the information risk management process
Information risk management	Process implemented
Protective marking	• Guidance included in risk actions toolkit • Procurement exercise of a protective marking system currently underway
Use of personal devices	Corporate policy to be considered
The use of encryption software	• Disk and removable media encryption implemented • Email encryption pilot now in place
Incident reporting	• Process agreed and published
Incident management	• Process agreed and published
Log management	Technical controls being implemented by Xentrall ICT Services as part of the ICT Strategy
Intrusion detection	
System access control	
Configuration management and change management	