AUDIT COMMITTEE
22 MARCH 2013

ITEM NO. ....

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

   - Information security policy
   - Information risk assessment
   - Information governance training and awareness
   - Information classification and handling
   - Information sharing
   - Information security incidents
   - Data quality

   and also addresses particular issues relating to

   - the transfer of Public Health responsibilities to local authorities, and
   - the transparency agenda

3. The Council continues to deliver the information governance programme against a background of re-organisation and financial constraint and as a result progress has been gradual. 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.

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 ext 2140
Peter McCann, Information Security Manager, ext 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 outlines how the Council's information governance function is to contribute to the arrangements for the transfer of duties and functions in relation to health and well being.
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 position that is positive.

Information risk assessments

10. A risk actions toolkit for Heads of Service has been developed to support the consistent application of controls identified by the information risk assessment process across services. The toolkit facilitates the planning and completion of improvement actions and requires evidence to show that the actions have been completed. This evidence will be reviewed by the Information Management Team in order to provide assurance to the Council that the risks have been appropriately addressed, and that expected improvements have been realised.

11. Certain risks identified by the risk assessment process are service specific rather than corporate in nature, and actions required for improvements in these areas will be appended as required to the risk action toolkit of the appropriate Head of Service.

Information governance training and awareness

12. Information governance training and awareness is delivered in a variety of ways, utilising on-line training courses, corporate communications channels, the intranet and face-to-face training courses and workshops.

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

14. 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.

15. For staff with access to the policy management system the roll-out position is given below.

	No of staff	**%age complete as at 28th February, 2013**	**%age complete as at 30th November, 2012**
People	611	69	67
Place	457	88	88
Resources	218	94.5	94

16. For those staff with no access a leaflet is to be produced 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.

17. In addition to the mandatory Employees Guide to Information Security the following courses are being developed for delivery through the policy management system.

- Data Protection – General Overview
- Records Management – General Overview
- Information Sharing – Principles
- Information Rights
- Day-to-Day Information Management

These courses are not mandatory, and Heads of Services will be requested to nominate staff to undertake the courses as appropriate. The timescale for roll-out of the courses is to be agreed with the Assistant Director – Finance.

Information classification and handling

18. An information classification and handling policy is to be 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.

Information sharing

19. The Complaints and Information Governance Team (CIG Team) has completed a baseline assessment of information sharing practices within the Council.

20. The assessment has provided the CIG Team with an overview of the information sharing agreements that are currently operational across the Council. However, as anticipated, it also indicates that information sharing agreements are not in place in a number of services where personal data is shared either internally or with external partners. To remedy this, the CIG Team has provided Heads of Service with a template for creating an information sharing agreement and will provide advice and support in assisting them to complete it, concentrating on those services that share the most sensitive data.

21. The survey has also indicated that a number of services are sharing personal data with key external partners, i.e. County Durham and Darlington NHS Foundation Trust, Durham Constabulary and Tees, Esk and Wear Valleys NHS Trust. To ensure information sharing agreements are implemented in an efficient and effective manner the CIG Team will coordinate a single agreement with each of the partners, liaising with the relevant services to ensure that their specific arrangements are addressed.

Information security incidents

22. The Council's information security incident reporting procedure is embedded and working effectively. The number of information security incidents reported since the procedure was implemented has increased mainly due to greater awareness and understanding by staff of the importance of incident management reporting.

23. 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.

24. 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

25. The Chief Officers Executive recently 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. This Group will oversee a programme of work which will produce a development plan for all the Council's major business systems and through a series of business process improvements will seek to address data quality in a systematic way.

Public health

26. The transfer of public health responsibilities to the Council from NHS County Durham and Darlington by April 2013 continues to be managed through the local transition plan. There are no significant information management risks identified with the transfer at this time.

Transparency

27. The CIG Team published its second annual Freedom of Information, Environmental Information and Subject Access Request report which was presented to COB in August 2012 and approved by Cabinet in October 2012. The report recommended that services publish frequently requested information on the Council's website with the aim of reducing the costs of responding to individual requests for information and improving transparency. Services have responded to the recommendations and there is now a large volume of information published on the Council's Open Data website pages.

28. The Protection of Freedoms Act 2012 (the PF Act) makes consequential amendments to the Freedom of Information Act 2000 (the FOI Act). It includes a requirement for public authorities to publish datasets requested under section 1 of the FOI Act.

29. Central Government published a consultation document for a 'Code of Practice (Datasets)'which explains how public authorities are expected to publish datasets. The consultation period closed in January 2013 and to date there has been no further communication from Central Government. The CIG Team is monitoring developments and will provide a further update in due course.

Conclusion

30. 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 and issue of the risk action toolkit for Heads of Service will facilitate this.

31. Whilst the information governance programme is well structured the Council continues to deliver it against a background of re-organisation and financial constraint, resulting in progress being gradual. Consequently the overall information governance risk is considered to remain 'above the line', and will do so until key actions identified in the information risk actions toolkit are completed and associated controls are embedded and proven to be effective.

Outcome of consultation

32. 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 14)
End user awareness training	• Head of Service awareness training complete • End user training courses under development (see paragraph 17)
E-mail usage	Included in the risk actions toolkit
Use and control of portable media	• Encryption controls in place • Risk actions toolkit guidance under development
Home and mobile working	Risk actions toolkit guidance under development
Secure document printing	Implemented as part of the Printer Consolidation Project
Manual (paper) document handling	• Information classification and handling guidance included in risk actions toolkit • Confidential waste project in progress
Handling of faxes	Included in risk actions toolkit
Secure disposal and destruction	• Policy and procedure in place for ICT equipment • Paper documents and records being considered in confidential waste review project
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
Use of personal devices	Corporate policy to be considered
The use of encryption software	• Disk and removable media encryption implemented • Email encryption pilot to be implemented in March 2013
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	