AUDIT COMMITTEE
28 SEPTEMBER 2012

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 remains 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
   (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. It is recognised that the Council is delivering the information governance programme against a background of re-organisation and financial constraint and that practical difficulties are inevitable. Work is ongoing in all areas of the programme but given the resource constraints progress is gradual. Consequently the information risk management strand of the programme is critical, as it enables the identification and prioritisation of information risks and ensures that available resources are 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. An information governance work programme has been developed to address the need for appropriate controls to be embedded and consistently applied across all services. A key aspect of this is the information risk management programme approved by COB. This programme involves the identification and assessment of risks, consideration of risk treatment options, development and implementation of risk treatment plans, and the monitoring and measurement of the effectiveness of the controls once they have been implemented.

8. The Information Commissioner has the power to impose monetary penalties of up to £500,000 for what he considers to be serious breaches of the Data Protection Act. The importance of good information governance has been highlighted recently by the number and value of monetary penalties imposed by the Information Commissioner’s Office (ICO) for breaches by Councils who, in their view, have not taken reasonable steps to safeguard their information.

9. Reasonable steps have been defined by the ICO as

   (a) having clearly defined information governance roles and responsibilities
   (b) having information governance policies, procedures, and training and awareness programmes
   (c) undertaking information risk assessments
   (d) compliance with good practice such as ISO27001 Information Security Management Standard

10. The ICO also expects Councils to

    (a) identify and train a board level Senior Information Risk Owner (SIRO)
    (b) continuously make staff aware of the existing information governance policies and guidelines, emphasising the importance of following them in practice and highlighting that a breach of policy will be regarded as a disciplinary offence
    (c) ensure that all staff undertake regular and relevant information governance training

11. Further to these expectations the ICO and the Department of Communities and Local Government have identified the transfer of public health responsibilities and the data transparency agenda as key priorities in relation to information governance assurance.

12. Since June 2011 the ICO has issued monetary penalties to ten Councils ranging from £60,000 to £140,000, the average penalty being £95,000. Details of the monetary penalties issued are published on the ICO’s website at http://www.ico.gov.uk/what_we_cover/taking_action/dp_pecr.aspx

Current Position

Senior Information Risk Owner (SIRO)

13. The role of SIRO within the Council is undertaken at board level by the Director of Resources in line with the ICO's recommendations.

Information security policy

14. 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.

15. The recently published '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. These are shown in **Appendix 1** together with an initial self-assessment of the Council's position in relation to them. A more detailed assessment is being undertaken to establish an action plan to include timescales and responsible officers.

16. The core of the report is structured around the five main headings of Policy, People, Places, Processes and Procedures and provides checklists of best practice for each.

Information risk assessments

17. The Council has adopted a standard approach to information risk assessment, and assessment exercises have been undertaken in the vast majority of Services.

18. A corporate information risk action plan has been drafted based on the results of the completed information risk assessments. This plan identifies actions relating to identified risks for which there is a requirement for a corporate action or solution to be implemented. The plan will be presented to COB for consideration/approval.

19. Service-based action plans are currently being drafted relating to identified risks which are service specific. Once completed the action plans will be presented to Assistant Directors for consideration/approval.

Information governance training and awareness

20. 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.

21. Mandatory face-to-face awareness training for Heads of Services was developed and delivered in June 2012. A mop-up session to cover the few officers who could not attend in June was delivered on 7th September. The training identified Heads of Service as

Information Asset Owners for all information assets within their service area. This role carries with it a number of key responsibilities as set out in **Appendix 2**.

22. The Employees Guide to Information Security has been rolled out using the CALMS 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.

23. For staff with access to CALMS the current rollout position following restructuring is given below. The position is a gradual improvement on that previously reported but individual Assistant Directors have been provided with a report covering their service areas to enable progress to be expedited.

Service Group	**No of staff**	**%age complete**
People	821	39
Place	330	70
Resources	205	90

24. For staff with no access to CALMS briefing sessions are in the process of being scheduled to ensure they understand their responsibilities in relation to information security, and to give them the opportunity to raise any queries or concerns they may have.

25. The intention is to supplement the mandatory face-to-face awareness training mentioned in paragraph 21 above with the following 5 courses for all staff that will be delivered electronically via the Academy10 corporate e-learning system. These courses are currently under development.

    (a) Data Protection – General Overview
    (b) Records Management – General Overview
    (c) Information Sharing – Principles
    (d) Information Rights
    (e) Day-to-Day Information Management

    The timescale for roll-out of the courses is subject to approval by the e-learning working group.

26. Over and above the standard courses the Information Management Team is on hand to provide appropriate support as and when required, for example by attending team meetings to discuss information governance issues or deliver bespoke training sessions.

27. Work also continues to develop the Information Management Framework on XIP (Xentrall's intranet) to provide advice and guidance on all aspects of information governance. (http://xip/1527/infosec/dbc/ISDoc_DBC/DBC_IMF)

28. Improvements to the framework since the last report include the addition of the following key processes and procedures

(a) Information assurance self-assessments
(b) Secure transfer of information
(c) Information sharing
(d) Information risk management
(e) Secure fax
(f) Redaction

Information classification and handling

29. A draft information classification and handling policy has been developed based on the Government's protective marking scheme. This approach has been widely adopted across public services, providing a common approach to classifying, labelling and handling information. This is invaluable when sharing information or seeking assurances that information is being appropriately handled in line with its sensitivity and importance.

30. 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. Some of the controls are already in place, others are part of current or pipeline projects, and a number of issues have yet to be formally addressed. A detailed self-assessment of the Council's current position is being documented and this will lead to the production of an implementation programme which will be presented to COB for consideration/approval.

Information sharing

31. The Council shares a range of information with partners for service delivery purposes, either as part of a partnership arrangement or under contract. It is best practice to ensure that such arrangements are put in writing to ensure that all parties are aware of their information governance responsibilities and obligations. These documented arrangements are known as information sharing agreements.

32. In order to ensure that services have information sharing agreements in place, where appropriate, the Complaints and Information Governance Team (CIG Team) is to undertake a strategic review of information sharing. This will involve an assessment of current information sharing practices and a gap analysis to determine where information sharing agreements are needed but not currently in place.

33. Those services advised to implement information sharing agreements will be provided with standard guidance and templates to create their own agreements. Support from the CIG Team will be provided where necessary and will be prioritised to areas of highest risk.

Information security incidents

34. The Information Commissioner's Office (ICO) has continued to issue monetary penalties for what they consider to be serious breaches of the Data Protection Act 1998, drawing

attention to their expectations of the reasonable steps that should be taken to ensure sensitive personal information is securely handled.

35. The Council has a formal information security reporting and management procedure in place.

36. 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

37. The Council's corporate approach to data quality is to be reviewed as part of specific work around systems and information strategy as it plays a major role in improving the Council's corporate knowledge and intelligence.

38. Areas for improvement in relation to service-specific data quality will be addressed as part of the information risk assessment process (see paragraphs 17 to 19).

Public health

39. 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, and a data cleansing exercise is currently being undertaken to ensure that data is relevant and accurate prior to transfer. There are no significant information management risks identified with the transfer at this time.

Transparency

40. The Protection of Freedoms Act 2012, enacted in May 2012, 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. In addition, the Government's ongoing commitment to the release of public sector datasets was evidenced in its Open Data White Paper 'Unleashing the potential', published in June 2012.

41. Last year, in anticipation of the requirements that were expected to be imposed by the Protection of Freedoms Act 2012, the CIG Team produced its first Freedom of Information, Environmental and Subject Access Request Report. This annual report uses statistical information gathered about requests for information to identify themes and make recommendations about the proactive publication of information. Following this report, many services have published information on the Council's website. There is now a significant section of the website dedicated to the publication of Open Data. The second annual report was approved by COB on 30 August 2012 and will be considered by Cabinet on 9th October, 2012.

42. To support the Council's approach to Open data the DarlingtonLIS, which is a local information system developed by the Council and its partners, makes available a wealth of information about Darlington in a variety of formats. The DarlingtonLIS can be accessed at http://lis.darlington.gov.uk

43. The INSPIRE regulations came into force on 31st December 2009 and this Directive is now law that applies to the Council. The INSPIRE Directive aims to provide consistent datasets about the environment so that they can be shared to benefit the development and monitoring of environmental policy. The authority must make available to the public relevant environmental datasets. A plan is in place to identify, quality control and publish these datasets as required by the INSPIRE regulations by December 2013 and onwards.

Conclusion

44. The ICO continues to emphasise the importance of good information governance and underline their expectations for local authorities to have appropriate information management controls in place, outlining the reasonable steps that they expect Councils to take to avoid information security incidents and avoid being subject to monetary penalties.

45. Delivering appropriate and regular awareness and training and having documented, well understood and consistently applied policies, procedures and guidelines remains critical to the development and continual improvement of the Council's information management system. Whilst the information governance programme has progressed, particularly with regard to establishing the risk position, due to current resource constraints progress is gradual. As a consequence the overall information governance risk remains 'above the line', and will remain so until key actions identified by the information risk assessment process are completed and associated controls are embedded and proven to be effective.

Outcome of consultation

46. 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 CALMS (see paragraph 23)
End user awareness training	• Head of Service awareness training complete (see paragraph 21) • End user training courses under development (see paragraph 25)
E-mail usage	• Revised policy in draft • Policy guidance to be completed
Use and control of portable media	• Encryption controls in place • Policy statement and guidance to be reviewed
Home and mobile working	Corporate policy to be reviewed and agreed
Secure document printing	Currently being implemented as part of the Print Consolidation Project
Manual (paper) document handling	• Policy and guidance in draft • Confidential waste review project PID approved
Handling of faxes	Procedure published
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	Integral part of the information risk management process
Information risk management	• Process agreed and published • Awareness / briefing sessions delivered to designated officers
Protective marking	Under consideration (see paragraphs 29 and 30)
Use of personal devices	Corporate policy to be reviewed and agreed
The use of encryption software	• Disk and removable media encryption implemented • Email encryption to be implemented
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	

Appendix 2

Head of Service responsibility as Information Asset Owner

As a Head of Service you are responsible for ensuring that the information within your service is properly protected and its value to the Council is fully realised. Some of your responsibilities will require you to take action, others simply to assure that action is being taken by others. It is fine to delegate responsibility to particular areas or officers of your service, but in doing so you must remember that you retain the accountability for proper information management and handling.

What do I need to do?

You need to ensure that information risk assessments are performed at least annually. To do this you need to know

- what your information assets are
- what information your assets hold, and what information is transferred in or out
- who has access to your assets and for what purpose

What is an information asset?

Information assets come in various forms ….

Databases	Current and archived
Paper records	Current and archived
Software	Applications, programs
Physical	Infrastructure, equipment, removable media
Services	Computing and communications, power, air-conditioning
People	Qualifications, skills and experience
Policies	Policies, procedures, guidance, training
Intangibles	Public confidence, reputation

How do I do an information risk assessment?

The Information Security Management Team (ISMT) has developed an information risk management process which will help you to undertake information risk assessments and identify areas and action for improvement. Guidance on the process is published on the intranet at http://xip/1527/infosec/sbc/19761/InfoRisk

A copy of the spreadsheet that needs to be populated is available by clicking here.

Do I need to do this work myself?

No – the best approach is to nominate appropriate officers within your service to liaise with ISMT in order to understand the process and then undertake the assessments. You will be involved in reviewing the completed assessments and agreeing actions that need to be taken within your service to reduce identified risks to an acceptable level. Risks identified that are corporate in nature will be referred to COB by the Information Security Manager.

What if I need help?

Simply contact the Information Security Management Team who will be happy to provide any advice or guidance required.