AUDIT COMMITTEE
23 MARCH 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.

2. Previously progress on information governance was included in the report on the implementation of the ICT Strategy. However, the recent ICT Strategy review recognised that information governance involved much more than ICT related issues, and as a consequence progress on the delivery of the information governance programme is now to be reported separately.

Summary

3. Information governance is an 'above the line' risk on the corporate risk register and has been recently highlighted as an area of concern in a letter from the Permanent Secretary for the Department of Communities and Local Government (DCLG) and the Information Commissioner's Office (ICO). The letter entitled "Information Governance Assurance" was sent to local authority Chief Executives on 23rd January 2012. The concerns expressed in the letter are all currently being addressed through the Council's information governance programme.

4. This report sets out progress in the delivery of each strand of the information governance programme, which are

   - 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

5. The letter from the DCLG and ICO recognises that Councils are delivering the information governance programme against a background of re-organisation and financial constraints and that practical difficulties are inevitable. Work is ongoing in all areas of the information governance programme but given the resource constraints progress is gradual. Consequently the information risks management programme is critical. The programme will enable the identification and prioritisation of information risks and ensure that available resources are used to best effect.

Recommendation

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

Reasons

7. 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

Letter on Information Governance Assurance from Department for Communities and Local Government/Information Commissioner's Office to Local Authority Chief Executives dated 23 January 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

8. 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.

9. 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 in April 2011. 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.

10. The importance of good information governance has been highlighted recently in a joint letter from the Permanent Secretary for the Department of Communities and Local Government and the Information Commissioner. The letter entitled "Information Governance Assurance" was sent to local authority Chief Executives on 23 January 2012 and sets out expectations in respect of the secure handling of sensitive personal information. Whilst there is recognition that Councils face practical difficulties in achieving information governance objectives against the background of re-organisation and financial constraint, the letter underlines the powers that the Information Commissioner has to impose significant financial penalties for breaches of the Data Protection Act. Financial penalties of up to £500,000 can be imposed for serious breaches.

11. The ICO has also set out guidance on the reasonable steps that they expect local authorities to take to safeguard personal data and avoid being subject to monetary penalties. These are

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

12. In order to reduce the risk of data loss the Information Governance Assurance letter states that the Council are expected to

    - identify and train a board level Senior Information Risk Owner (SIRO)
    - 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
    - ensure that all staff undertake regular and relevant information governance training

13. The letter also identifies the transfer of public health responsibilities to local authorities, and the data transparency agenda as key priorities in relation to information governance assurance.

Current Position

Senior Information Risk Owner (SIRO)

14. 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

15. The Council has a corporate policy statement endorsed by the Chief Executive and approved by Cabinet in December 2009 that sets out the policy and objectives of information security management. In addition there are a set of operational information management policies that support the corporate policy and align with the guidance set out in the Employees Guide to Information Security. The operational policies and associated guidance are currently under review.

Information risk assessments

16. The Council has adopted a standard approach to information risk assessments that involves the assessment of information risks against a pre-defined range of threats, and the identification and implementation of risk treatment actions. The assessment exercises are co-ordinated by service-based staff nominated by Assistant Directors. Briefing sessions were given to nominated staff to ensure common understanding and consistent application across the Council.

17. Some service areas have made significant progress in undertaking their risk assessments. In other areas where progress has been more limited due to a range of issues such as competing priorities action plans are being developed with the appropriate Assistant Directors.

18. Any service specific risks identified during the process will be reported to Heads of Service and Assistant Directors who will be obliged to either agree actions to mitigate the risks or to accept them. Any cross cutting risks will be reported to COB to consider and agree appropriate action.

Information governance training and awareness

19. 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.

20. The Information Management Team has attended each Group Senior Management Team to outline the Council's information management programme.

21. The Employees Guide to Information Security has been rolled out using the CALMS policy management system. 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.

22. A Member's Guide to Information Security has been distributed to all Members. Members are required to sign a statement of understanding confirming that they have read the protocols and understand their responsibility in relation to them.

23. For staff who have access to CALMS the current rollout position is given below.

Service Group	No of staff	%age complete
People	810	35
Place	370	39
Resources	197	93

24. For staff who have no access to CALMS briefing sessions are to be delivered by the Information Management Team, as agreed with the appropriate Assistant Director, to ensure that staff understand their responsibilities in relation to information security, and to give them the opportunity to raise any queries or concerns they may have.

25. A training programme has been developed that includes a mandatory face-to-face course for Heads of Service covering the main issues and key points of information governance in order that they have a good overall understanding of their responsibilities. This will be supplemented by a range of more detailed courses that will be delivered electronically for those officers nominated by their Heads of Service. The exception to this approach will be an information sharing course which will continue to be delivered face-to-face due to the nature and complexity of the subject.

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 delivering 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)

Information classification and handling

28. The Government has recently been encouraging public authorities to adopt their protective marking scheme which is a standard approach to classifying information and setting rules for how information of a particular classification should be handled. A draft policy and guidance on this matter has been developed for consideration and approval by COB. Adherence to the policy and guidelines will significantly reduce the risk of a Data Protection Act breach.

29. Technical controls have been implemented to ensure that Council laptops are encrypted and other removable storage media such as USB memory stick are controlled. In addition secure email services are being implemented to safeguard personal or sensitive information.

Information sharing

30. 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.

31. Last year, the Council signed up to the North East Information Sharing Guidelines, which contains a template for the creation of information sharing agreements. This template was recently circulated to all Heads of Service, who were asked to ensure that it was used to review existing information sharing agreements and draft new ones.

32. The Information Management Team has also provided detailed advice and guidance to staff in respect of projects where it is proposed that information be shared with partners. In particular, a pilot is underway in Tenancy Support (Key Point of Access) to map data flows and ensure that appropriate information sharing agreements are in place. The model resulting from this pilot will be used to review information sharing practices in other services.

Information security incidents

33. The consequences of an incident involving a serious breach of the Data Protection Act are potentially very serious, with the ICO having powers to impose financial penalties of up to £500,000. This was brought to the attention of staff in an article published in the September / October 2011 edition of the Flyer, together with advice on 'how do we make sure this never happens to us'.

34. To encourage staff to recognise and report information security incidents, to enable lessons to be learnt and improvements implemented a procedure has recently been developed, approved and publicised. This procedure involves the reporting of an incident to the Head of Service, Assistant Director and Information Security Team (IST). The IST will investigate the incident and recommend improvements where appropriate.

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

Data quality

36. A Data Quality Strategy was approved by Cabinet in June 2008. This document and the Council's approach to data quality are under review due to changes in roles and responsibilities following the Council restructure.

Public health

37. The transfer of public health responsibilities to the Council from NHS County Durham and Darlington by April 2013 presents its own set of information governance issues and risks. A local transition plan has been developed to manage the transfer that includes a range of work streams. One such work stream is information governance and the Council's Information Management Team is represented on this working group.

Transparency

38. Central Government is advocating that local authorities publish more information as part of its Transparency Agenda; the first phase being the requirement to publish expenditure data online in open formats, which the Council achieved in January 2011. Following phases are likely to include requirements to publish contractual data and other key information. In addition, the Protection of Freedoms Bill, which is currently passing through Parliament, contains a requirement to publish the full data sets of information disclosed under the Freedom of Information Act 2000.

39. Internally, the Access Channels Strategy, which aims to influence the way the Council communicates with the public in order to improve efficiency, contains a sub-strategy that seeks to encourage services to publish more information. The Complaints and Information Governance Manager is responsible for delivering this sub-strategy, the objective of which is to achieve efficiencies by reducing the workload associated with the processing of requests for information.

40. The annual Freedom of Information, Environmental and Subject Access Request Report uses statistical information gathered about requests for information to identify themes and make recommendations about the proactive publication of information. The first report and associated recommendations was approved by COB on 28 July 2011 and many services have begun to publish the information identified therein.

Conclusion

41. The Information Governance Assurance letter from the DCLG and ICO emphasises the importance of good information governance and underlines their expectations for local authorities to have appropriate information management controls in place, but recognises that Councils may face practical difficulties in securely handling personal information. However, it is clear that the ICO will not hesitate to impose substantial financial penalties for serious breaches of the Data Protection Act, and they have outlined reasonable steps that they expect Councils to take to avoid being subject to them.

42. Work is ongoing in all of these areas as part of the information governance programme but given resource constraints progress is gradual. Consequently the information risks management programme is critical. The programme will enable the identification and prioritisation of information risks and ensure that available resources are used to best effect.

Outcome of consultation

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