**AUDIT COMMITTEE**
**27 MARCH 2015**

**ITEM NO.** .....

# INFORMATION GOVERNANCE PROGRAMME PROGRESS REPORT

## SUMMARY REPORT

### Purpose of the Report

1. The Systems and Information Governance Group (SIGG) is required to report six monthly to the Audit Committee on progress and planned developments of the information governance programme.

### Summary

2. There are a number of external information assurance requirements that shape our information governance programme. They all represent good practice and have common objectives

   (a) compliance with information related legislation
   (b) approval to use essential external party systems and services
   (c) improvement in service delivery

3. At present information governance is an 'above the line' risk on the corporate risk register. Delivery of our information governance programme will provide the assurance required and will reduce our information risks to an acceptable level.

4. The Council continues to make progress on the implementation of the information governance programme. Recent work includes

   (a) revised information security governance framework
   (b) revised information governance policies
   (c) refreshed Caldicott Guardian role and associated confidentiality work programme
   (d) Health and Social Care Information Centre (HSCIC) Information Governance (IG) Toolkit 'satisfactory' assurance level for Public Health

5. The area of highest priority in the information governance programme is compliance for social care services with the HSCIC IG Toolkit which has a deadline for submission of April 2015. This differs from the Public Health submission which was a 'slimmed-down' version of the full IG Toolkit due to the nature of their activity and their previous experiences with Health Service governance arrangements.

6. Failure to demonstrate compliance with the full IG Toolkit may seriously compromise the ability of social care services to share information with health partners and access essential services, such as connection to the N3 network, required for collaborative working.

7. We are currently unable to evidence compliance with the HSCIC IG Toolkit to attain an overall 'Satisfactory' assurance level. The required improvements have been identified and prioritised in the information governance programme. It is, however, uncertain whether we will be in a position to evidence the required assurance level by the deadline date, given competing demands on limited resources.

**Recommendation**

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

**Reason**

9. To provide the Audit Committee with a status report on the delivery of the Council's Information Governance Programme.

**Paul Wildsmith**
**Director of Neighbourhood Services and Resources**

Brian James, Head of Corporate Assurance : Extension 5408
Peter McCann, Information Security Manager : Extension 156494

**Background Papers**

| | |
|---|---|
| S17 Crime and Disorder | There is no specific crime and disorder impact. |
| Health and Well Being | There is no specific health and well being impact. |
| 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

10. Information governance remains an 'above the line' risk on the corporate risk register. This is a reflection of the improvements required to evidence that we meet all of the information assurance requirements set out by government and industry standards.

11. In a letter to local authority Chief Executives in January 2012 the Permanent Secretary for the Department of Communities and Local Government and the Information Commissioner clearly set out their minimum expectations with regard to information governance as follows

    (a) clearly defined information governance roles and responsibilities
    (b) information governance policies, procedures, training and awareness
    (c) information risk management
    (d) compliance with good practice

12. These expectations are reflected in the requirements of the other assurance frameworks with which the Council needs to comply, for example, HSCIC IG Toolkit, Public Service Network (PSN) and Payment Card Industry Data Security Standards (PCIDSS).

### Current Position

### Roles and responsibilities

13. Systems and Information Governance Group (SIGG) approved a refreshed Information Security Governance Framework at their meeting on 4 December 2014. The framework sets out the key information governance roles and responsibilities (see **Appendix A**).

### Policies and procedures

14. A full refresh of information governance policies has been undertaken. The policies set out high level Council commitments, which will be underpinned by standards, processes and procedures, as well as guidelines for staff and elected members. The effectiveness of the policies in delivering their objectives will be monitored and reported through an appropriate set of performance metrics. A list of refreshed policies is set out in **Appendix B**.

15. The Information Management Team is currently developing the standards and corporate processes, procedures and guidelines. Gaps in service-specific processes, procedures and guidelines continue to be identified through the information risk management process, and risk treatment plans are being developed or updated by the appropriate Head of Service.

## Training and awareness

16. The Employees' Guide to Information Security is continuing to be rolled out via the Council's intranet as a mandatory course for all staff with access to the corporate network. For those staff with no access, a leaflet developed covering information management issues and responsibilities was provided to line managers for distribution to the relevant staff.

17. To reflect the changes in working practices and the information security landscape, the Employees' Guide to Information Security and Members' Guide to Information Security are being reviewed and updates will be communicated once finalised and approved.

18. More detailed specialist guidelines and awareness courses for staff on subjects, such as the use of social media, are being developed and will be provided to staff in due course.

## Information risk management

19. Undertaking information risk assessments and implementing appropriate risk treatment plans is an essential element of good information governance and a key part of each of the assurance frameworks with which we need to comply.

20. The previously implemented information risk management process has been reviewed and improved to better reflect the risks in terms of the confidentiality, integrity and availability of information. This will be rolled out across all Council services in due course.

21. However, spurred on by the requirements and deadlines of the HSCIC IG Toolkit information risk assessments, following the new process, have been completed and risk treatment plans have been developed in Public Health, Children's Social Care and Adult Social Care. Implementation of the risk treatment plans is the responsibility of the Assistant Director and/or Head of Service for these service areas.

## Information classification and handling

22. A pilot is now underway in ICT Services and Corporate Assurance for the classification and labelling of emails. Subject to the success of the pilot, corporate roll-out will commence in March 2015.

## Information sharing

23. The Complaints and Information Governance (CIG) Team is continuing to work with key public sector partners to review and implement service-level information sharing agreements where required.

24. Services have made significant progress in this regard. The most recent example being the agreement between Tees, Esk and Wear Valleys NHS Trust and the Council's Mental Health Service to reflect the new co-located model of mental

health service delivery. Internal information sharing agreements are also being put in place to formalise arrangements for reciprocal information exchange in areas such as Housing and Revenues and Benefits.

**Caldicott Guardian**

25. The role of Caldicott Guardian was previously split between the Assistant Director, Adult Social Care and the Assistant Director, Children, Families and Learning. Following the senior management restructure within Services for People, it was decided that the role would be carried out solely by the Assistant Director, Adult Social Care, supported by a Caldicott Function. The Caldicott Function is made up of managers with responsibility for services that process personal and confidential information in a social care context, supported by relevant advisors. A description of the responsibilities of the Caldicott Function is provided in **Appendix C**.

26. Current Caldicott activity is centred on providing guidelines and awareness for staff in dealing with confidential information. Further activity will be logged and will be reported as part of future Information Governance Programme progress reports.

**Information security incidents**

27. The information security incident reporting process is embedded. The identification, reporting and the initial response phases of the process are working effectively. However, the timely documentation of remedial action plans and their successful implementation and sign-off by senior management, which is effectively the risk treatment part of the process, still requires improvement.

**Data quality**

28. Work continues to progress on improving data quality across the Council's major business systems, with a specific focus on data within the CareFirst system used by Adults and Children's Services. This work on improving data quality is being aligned with the requirements for data quality as determined by Ofsted and also in preparation for the replacement of the current case management system.

**Transparency**

29. The CIG Team's fourth annual Freedom of Information, Environmental Information and Subject Access Request Report was presented to Cabinet in November 2014.

30. The report outlined further information to be published by the Council in response to frequently requested information with the aim of reducing the cost of responding to individual requests and improving transparency.

31. The report also detailed amendments made to the Council's FOI and EIR Request Procedure following the introduction of the Protection of Freedoms Act 2012.

32. The Local Government Transparency Code 2014, published by the Department of Communities and Local Government, outlined the requirement on all local authorities to publish certain data within certain timescales and in certain formats.

The Organisational Planning Unit is working with Chief Officer's Board (COB) to comply with the mandatory requirements of the Code.

## Conclusion

33. The Council's information governance programme clearly sets out key objectives, roles and responsibilities, priorities and risk treatment plans. As such we are aware of the improvements required.

34. The timely delivery of the information governance programme remains an issue of concern given the competing demands on limited resources. In the short term, failure of social care services to evidence compliance with the requirements of the HSCIC IG Toolkit may adversely affect their ability to deliver services effectively.

## Outcome of consultation

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

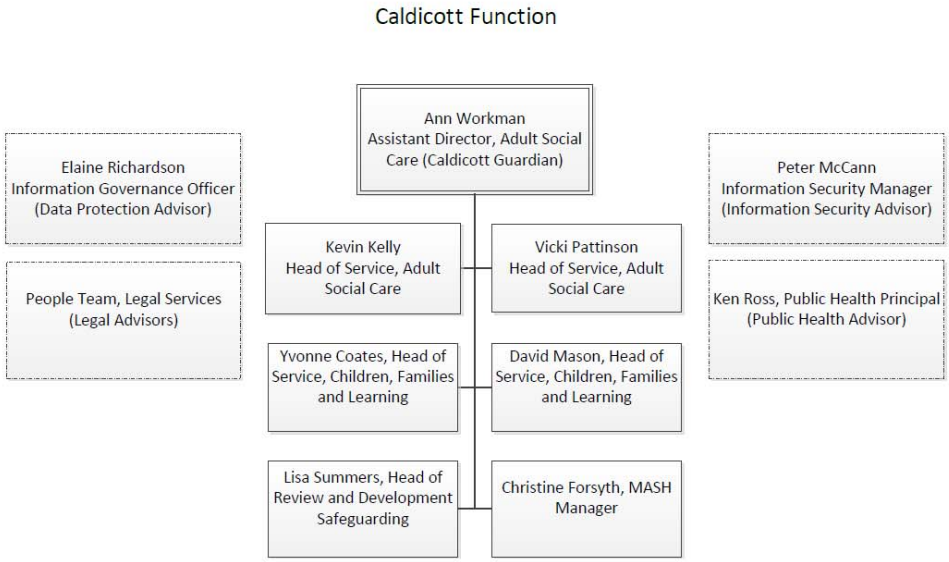
**Appendix A – Information Security Governance Framework**

| Roles and responsibilities | |
|---|---|
| **Audit Committee** | Monitor activity and progress in relation to the development and implementation of the information security governance programme |
| **SIRO** | Own the information risk management process |
| | Agree corporate information risk treatment plans |
| | Ensure that the approach to information risk is effective in terms of resource, commitment and execution |
| | Ensure that chief officers and members are adequately briefed on information risk issues |
| **COE** | Ensure that investment in information security governance is aligned with business strategy and risk profile |
| | Support a continual improvement culture based on the understanding that security is a process, not an event |
| **SIGG** | Approve the information security governance framework |
| | Approve information security policies and standards |
| | Approve corporate information security processes, procedures and guidelines |
| | Ensure that information security policies and standards are effectively and consistently applied |
| **Information Asset Owners (ADs)** | Lead and foster a culture that values, protects and uses information for public good |
| | Know what information the asset holds, and what information is transferred in or out of it |
| | Know who has access and why, and ensure that the use of the asset is appropriately controlled |
| | Understand and address risks to the asset, provide assurance to the SIRO and ensure any information security incidents are appropriately managed |
| | Ensure that the asset is fully used for the public good, including responding to information requests |
| **Heads of Service** | Undertake information risk assessments |
| | Develop risk treatment plans |
| | Understand and implement information security policies and policy standards |
| | Implement corporate information security processes and procedures |
| | Develop and implement service specific information security processes and procedures |
| | Ensure that staff receive appropriate information security awareness training |
| | Monitor compliance with information security processes and procedures |
| **Staff** | Comply with information security processes, procedures and guidelines |
| | Recognise and report information security incidents |
| **Third parties** | Adhere to instructions given to them by the Council in respect of processing Council information |

## Appendix B – Information Governance Policies

| Policy | Status |
|---|---|
| Information Security Statement of Management Intent | Approved |
| Data Protection Policy | Approved |
| Records Management Policy | Approved |
| Data Quality Policy | Approved |
| Freedom of Information and Environmental Information Policy | Approved |
| Information Security Organisation Policy | Approved |
| Mobile Device and Teleworking Policy | Approved |
| Human Resources Security Policy | Approved |
| Information Asset Management Policy | Approved |
| Access Control Policy | Approved |
| Physical and Environmental Security Policy | Approved |
| Operational Information Security Policy | Approved |
| Information Transfer Policy | Approved |
| Systems Acquisition, Development and Maintenance Policy | Approved |
| Supplier Relationship Policy | Approved |
| Information Security Incident Management Policy | Approved |
| Social Media Policy | Awaiting approval |

## Appendix C – Caldicott Function




Responsibilities of the Caldicott Function:

1. Support the Caldicott Guardian in championing confidentiality issues at a management level.
2. Provide advice and guidance to staff in relation to ethical information sharing issues, seeking advice from advisors where necessary (complex or serious issues must be considered directly by the Caldicott Guardian).
3. Assist in the delivery of the confidentiality and data protection work programme across Adult and Children's Social Care and Public Health.
4. Assist in the completion of the Confidentiality and Data Protection Assurance component of the HSCIC Information Governance Toolkit.
5. Provide reports to the Caldicott Guardian when confidentiality or data protection issues arise.
6. Deputise for the Caldicott Guardian at Systems and Information Governance Group when the Caldicott Guardian is unable to attend.