AUDIT COMMITTEE
21 SEPTEMBER 2017

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. 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.

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

   (a) appointment of a Data Protection Officer in line with the new General Data Protection Regulations (GDPR)

   (b) ongoing development of a compliance programme for GDPR

   (c) face-to-face information security and governance update sessions with senior management teams

   (d) continued adoption of the corporate secure information sharing and collaboration system across services

   (e) progress on service based information risk assessments and associated action plans

   (f) achieving our target for the completion of on-line mandatory information governance training courses

4. The areas of highest priority in the information governance programme are

   (a) the completion of the revised information risk assessments and the timely delivery of the associated improvement action plans

   (b) effectively communicating and embedding the revised incident management process across all services

(c) the effective and timely implementation of the GDPR compliance programme, and

(d) approval to connect to the Health and Social Care Network (HSCN)

Recommendation

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

Reasons

6. 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

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

7. 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 relevant information assurance requirements set out by government and industry standards.

Current Position

Training and awareness

8. The table in **Appendix 1** shows the position at the end of July 2017 with regard to the completion of the mandatory on-line information governance courses.

9. Completion rates of over 95% for all of the courses represents an acceptable level of take up which must be maintained. The completion of the courses is a mandatory element of the employee induction process so there is no reason to anticipate a drop in the completion rates going forward.

General Data Protection Regulations (GDPR)

10. The Complaints and Information Governance Manager has been appointed as the Council’s Data Protection Officer (DPO) and will fulfil the role as specified in the GDPR, which is specifically to provide advice and guidance on compliance. The Complaints and Information Governance Manager will be supported by the Information Governance Officer in fulfilling the requirements of the DPO role.

11. The DPO has recently completed the GDPR Practitioner Certificate which is a nationally recognised accredited training programme subscribed to by most local authorities in the region. Having done so the DPO is currently assessing the Council’s position across all services and will provide specific advice and guidance to service areas as part of the compliance programme.

HSCIC information governance toolkit

12. Completion of the version 14.1 of the toolkit is ongoing, co-ordinated by the Head of Performance and Transformation. Following approval by the Health and Social Care Information Centre (HSCIC) of the toolkit submission connection to the Health and Social Care Network (HSCN) will be progressed.

13. The HSCIC has advised that version 14.1 is an interim solution pending the introduction of a redesigned Information Governance Toolkit based around assuring local implementation of the ten data security standards set out in the National Data Guardian’s *Review of Data Security, Consent and Opt-outs*. The data security standards are shown in **Appendix 2**.

14. The redesigned toolkit will include a new set of mandatory requirements and, according to HSCIC, will be more accessible and easier to use. Formal roll-out is

scheduled for April 2018.

Information risk management

15. Revised information risk assessment checklists reflecting the requirements of GDPR were circulated to service managers in April 2017. Information security and governance update sessions with service management teams have been scheduled in September and October and will include a review of progress on the completion of the risk assessments and the delivery of resulting action plans.

Information sharing

16. 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. Work is underway to implement an information sharing agreement enabling the Council to share SEND (Special Education Needs and Disability) data with Hartlepool and Stockton Clinical Commissioning Group in order to produce one dataset which will allow the development of needs assessment work required under the SEND statutory requirements.

17. The Council has a secure information sharing system (Egress Secure Workspace) that allows sensitive personal information to be shared securely and easily with external organisations. It is currently being used in eight service areas, including Legal Services, Children's Placements and the Safeguarding Board.

Information security incident management

18. Designated information security incident investigating officers have been identified in service areas and training will be scheduled to be completed by October 2018. This will improve both the consistency in the way investigations are handled and the timeliness of the delivery of improvement plans.

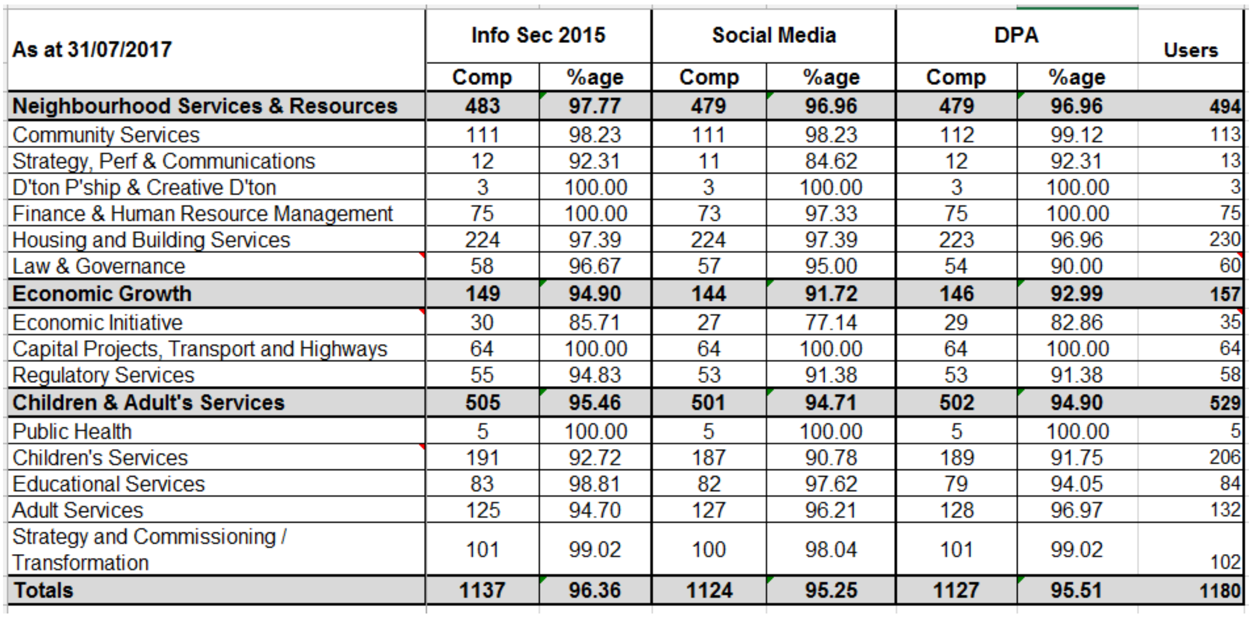
Conclusion

19. 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. However, the timely delivery of the programme remains an issue of concern given the competing demands on limited resources.

Outcome of Consultation

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

APPENDIX 1



As at 31/07/2017	Info Sec 2015		Social Media		DPA		Users
	Comp	%age	Comp	%age	Comp	%age	
Neighbourhood Services & Resources	**483**	**97.77**	**479**	**96.96**	**479**	**96.96**	**494**
Community Services	111	98.23	111	98.23	112	99.12	113
Strategy, Perf & Communications	12	92.31	11	84.62	12	92.31	13
D'ton P'ship & Creative D'ton	3	100.00	3	100.00	3	100.00	3
Finance & Human Resource Management	75	100.00	73	97.33	75	100.00	75
Housing and Building Services	224	97.39	224	97.39	223	96.96	230
Law & Governance	58	96.67	57	95.00	54	90.00	60
Economic Growth	**149**	**94.90**	**144**	**91.72**	**146**	**92.99**	**157**
Economic Initiative	30	85.71	27	77.14	29	82.86	35
Capital Projects, Transport and Highways	64	100.00	64	100.00	64	100.00	64
Regulatory Services	55	94.83	53	91.38	53	91.38	58
Children & Adult's Services	**505**	**95.46**	**501**	**94.71**	**502**	**94.90**	**529**
Public Health	5	100.00	5	100.00	5	100.00	5
Children's Services	191	92.72	187	90.78	189	91.75	206
Educational Services	83	98.81	82	97.62	79	94.05	84
Adult Services	125	94.70	127	96.21	128	96.97	132
Strategy and Commissioning / Transformation	101	99.02	100	98.04	101	99.02	102
Totals	**1137**	**96.36**	**1124**	**95.25**	**1127**	**95.51**	**1180**

APPENDIX 2

Leadership Obligation 1: People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

Data Security Standard 1: All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

Data Security Standard 2: All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3: All staff complete appropriate annual data security training and pass a mandatory test provided through the revised Information Governance Toolkit.

Leadership Obligation 2: Process: Ensure the organisation proactively prevents data security breaches and responds to incidents or near misses.

Data Security Standard 4: Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5: Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise security.

Data Security Standard 6: Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

Data Security Standard 7: A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Leadership Obligation 3: Technology: Ensure technology is secure and up-to-date

Data Security Standard 8: No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Security Standard 9: A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10: IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.