PLYMOUTH CITY COUNCIL

Subject:	Information Governance – Annual Report
Committee:	Audit Committee
Date:	30 June 2016
Cabinet Member:	Councillor Ian Darcy
CMT Member:	Lesa Annear (Director for Transformation & Change)
Author:	John Finch, Information Governance Manager
Contact details	Tel: 01752 307294 email: john.finch@plymouth.gov.uk
Ref:	N/A
Key Decision:	No
Part:	I

Purpose of the report:

This report provides a summary of the work that has been undertaken by the Information Lead Officers Group (ILOG) to improve information governance principles across all directorates in order to improve the Council's information asset. The report covers:-

- ILOG Terms of Reference
- Information Commissioners Office
- Devon Audit Partnership
- Information breach management
- Actions During 2016/17
- Future Actions

The Co-operative Council Corporate Plan 2013/14-2016/17:

Information Governance is included in risk registers that include links to the Corporate Plan objectives – monitoring of control action for risks therefore contributes to the delivery of the Council's core objectives.

Implications for Medium Term Financial Plan and Resource Implications: Including finance, human, IT and land

None arising specifically from this report but control measures identified in risk registers could have financial or resource implications.

Other Implications: e.g. Child Poverty, Community Safety, Health and Safety and Risk Management:

Risk and Opportunity Management – Information Governance is included as a risk in all directorate risk registers.

Equality and Diversity

Has an Equality Impact Assessment been undertaken? Not required.

Recommendations and Reasons for recommended action:

The Audit Committee is recommended to note and endorse the current position with regard to the action of the Information Lead Officers Group.

Alternative options considered and rejected:

Effective Information Governance processes are essential in helping to ensure compliance with legislative requirements such as the Data Protection Act and fulfulling the Council's duty of care to its customers. For this reason alternative options are not applicable.

Published work / information:

Background papers:

Title	Part I	Part II	Exemption Paragraph Number						
			1	2	3	4	5	6	7

Sign off: Councillor Darcy

Fin	djn16 17.10	Leg	dvs2 5893	Mon Off		HR		Assets		IT		Strat Proc	
Originating SMT Member , Asst Director for Finance													
Has the Cabinet Member(s) agreed the contents of the report? Yes													

1.0 Introduction

1.1 This report provides a summary of the work that has been undertaken by the Information Lead Officers Group (ILOG) to improve information governance principles across all directorates in order to protect the council's information asset.

1.2 The position with regard to the work of ILOG was last reported to this Committee on 25 June 2015 and this report now provides a summary of the progress of the group since then.

2.0 ILOG Terms of Reference

2.1 The ILOG comprises of Information Lead Officers (ILOs) for each directorate who provide the means for achieving a co-ordinated information governance framework that will develop improvements to service delivery.

2.2 The Information Lead Officers will be responsible for reporting directly to their management teams in order to secure buy-in and commitment to initiatives instigated by the ILOG.

2.3 Activities will be implemented through Information Asset Owners (IAOs) – those staff responsible for information holdings, or individual systems or applications within a service area and specialist working groups such as the Management of Information Security Forum, Freedom of Information Representatives and the Operational Risk Management Group.

2.4 The group is also supported by the Information Governance Manager, Corporate Records Manager, the Customer Relations Team and the Caldicott Guardians (the AD's for social care as the responsible managers for People's social and health data).

2.5. The group meets bi-monthly.

3.0 Information Commissioners Office

3.1 The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998. Section 51(7) of the DPA contains provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of good practice, with the agreement of the data controller. This is done through a consensual audit.

3.2 In July 2013 the Council agreed to a consensual audit by the ICO Good Practice Department and this took place at the end of April 2014. The results of this audit were presented to this Committee on 24 March 2016.

3.3 80% of the 49 recommendations have now been completed, with projects initiated within the Transformation programme which will result in 90% completion once they have been delivered.

4.0 Devon Audit Partnership

4.1 Devon Audit Partnership (DAP) also carried out an independent review of our information governance arrangements and the results of this were presented to this committee in March 2014.

4.2 It was agreed with DAP to put the action plan produced as a result of their audit on hold whilst the ICO action plan was being worked through as a priority.

4.3 Actions are now being revisited and worked through by the Information Governance Manager and ILOG.

5.0 Information breach management

5.1 One data breach was reported to the ICO. The Council managed to avoid receiving any monetary penalties for the breach as the ICO noted that the council acted promptly to try to prevent any damage being suffered and took into account the remedial measures adopted by the council.

5.2 The lessons learned from all breaches, and detailed statistical analysis continue to shared with many teams within the Council, to reduce the recurrence of breaches and ensure that in the event of an escalation to the ICO, there will be a reduced chance of a financial penalty.

5.3 There is an increased risk of information breaches due to cyber-attacks, which have increased worldwide, causing some major data breaches. The Council is aware of this increased risk and is preparing a Cyber emergency response team to reduce this impact.

6.0 Actions during 2015/16

6.1 Actions arising out of the group during the past 12 months include:-

- Information management project initiated in Transformation
- Records manager appointed
- Document storage project started
- Information Security @ the Council training launched
- Continued Information Governance Manager attendance at DMTs/Team meetings to raise awareness of issues
- Information Governance Manager attendance at Councillor meetings to raise awareness of issues
- Improved breach management processes, with a focus on greater reporting and escalation, and guidance provided to commissioned services.

7.0 Future actions over the next 12 months

7.1 ILOG's action plan over the next 12 months include:-

- Complete remaining ICO audit actions
- Complete DAP recommendations
- Implement full Cyber emergency response team

- Develop a plan to ensure the any changes in the Data Protection Act can be absorbed with minimum impact.

7.2 The Information Management project has 3 major work streams, which include:

- Information Governance Work Stream
    - Ensure all information assets are fully managed
    - Provide a set of clear and concise Information Governance policies
    - Address quality assurance issues for end user computing solutions:
    - Provide a mechanism for publishing Freedom of Information Requests to the Public
- Information Security Compliance Work Stream
    - Define and deliver a method for ensuring that Information Security work can be quickly prioritised, scheduled and resourced by the business and our IT provider.
    - Review and implement appropriate Identity and Access Management tools and processes
- Document / Records Management Work Stream
    - Records Management Policy and Design
    - Development of information architecture
    - Electronic Document and Records Management Systems
    - Rollout the Physical Document Storage solution, processes and standards across the business

8.0 Summary and conclusion

8.1 Good information governance provides people with confidence that their personal information is being handled properly, protects the vulnerable, enables the delivery of services and ensures that transparency requirements are met.

8.2 Where information security incidents do occur, procedures have been put in place to ensure a thorough investigation takes place, and the impact is reduced for anyone affected.

8.3 The landscape of increased cyber-attacks is something that the Council is preparing for, and will have strong procedures in place with which to reduce the impact of an attack.

8.4 Over the next 12 months ILOG will continue to focus on educating members, staff and partners about the potential pitfalls and how each of us can reduce the risk of not meeting statutory requirements, against a background of re-organisation and financial constraint.