PLYMOUTH CITY COUNCIL

Subject:	Information Asset – Annual Report
Committee:	Audit Committee
Date:	25 September 2014
Cabinet Member:	Councillor Lowry
CMT Member:	David Trussler (Interim Strategic Director for Transformation and Change)
Author:	Mike Hocking, Head of Corporate Risk and Insurance
Contact details	Tel: 01752 304967 email: mike.hocking@plymouth.gov.uk
Ref:	CRM/MJH
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.

In 2010/11 Devon Audit Practice conducted a review of information management arrangements and reported a finding of "fundamental weakness" which was reported to this Committee on 27 June 2011.

A specific breach of the Data Protection Act (DPA) occurred in November 2011and a fine of £60,000 imposed by the Information Commissioner's Office (ICO).

As a result of the above Corporate Management Team approved the formation of an Information Lead Officer's Group (ILOG) which was established in February 2012 in order to implement an action plan to enable the information asset to meet the council's service delivery goals and ensure on-going legislative compliance.

The Brilliant 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 Management – Information Governance is included as a risk in all directorate risk registers

Equality and Diversity

Has an Equality Impact Assessment been undertaken?   No, as Information Governance applies to any data or information irrespective of its subject.

Recommendations and Reasons for recommended action:

The Audit Committee is recommended to:
Note and endorse the current position with regard to the action plan 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 fulfilling 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:

Fin	Djn1415.42	Leg	DVS/21166	Mon Off		HR		Assets		IT		Strat Proc	
Originating SMT Member													
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 In 2010/11 Devon Audit Practice conducted a review of Information Management arrangements and reported a finding of "fundamental weakness" which was reported to this Committee on 27 June 2011.

1.3 A specific breach of the Data Protection Act (DPA) occurred in November 2011 and a financial penalty of £60,000 was imposed by the Information Commissioner's Office (ICO).

1.4 As a result of the above the Corporate Management Team approved the formation of an Information Lead Officers Group (ILOG) which was established in February 2012 in order to implement an action plan to improve the Council's information governance resilience in order to meet service delivery goals and ensure on-going legislative compliance.

2.0 The Council's response

2.1 The inaugural meeting of ILOG took place on 22 March 2012 and the terms of reference of the group are listed in more detail in paragraph 3.0 of this report.

2.2 An initial list of priority issues was drawn up and incorporated into an action plan which was RAG rated based on the perceived importance of each issue.

2.3 A communication action plan was also drawn up and the first of a series of staff communications was circulated in March 2012 in order to begin raising awareness.

2.4 An Information Governance risk audit was carried out via the Operational Risk Management Group.

2.5 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.

2.6 Based on the recommendations from DAP's report an action plan has been produced which identifies responsible officers and target dates for completion. The action plan is linked to the Corporate Transformation Programme and will be actioned where appropriate to a strand of the Programme.

3.0 Information Commissioners Office

3.1 The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51(7) of the DPA contains a 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 and focussed on three areas:-

- **Records management** (manual and electronic) - The processes in place for managing both manual and electronic records containing personal data.
- **Training and awareness -** The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities.
- **Subject access requests -** The procedures in operation for recognising and responding to individuals' requests for access to their personal data.

3.3 As a result of the audit 49 recommendations have been made by the ICO primarily around enhancing existing processes to facilitate compliance with the DPA.

3.4 The ICO's overall conclusion was that Plymouth City Council is currently providing "limited assurance" that processes and procedures are in place and delivering data protection compliance

3.5 Areas of good practice identified by the ICO were:-

- Adult Social Care have not created manual records since July 2012 due to scanning and shredding manual information which eases demands on physical storage, simplifies retention and reduces security risks
- Implementation of the Data Safe e-learning course
- The 'Information Access Business Processes' guidance which provides clear details of team specific processes to be used when responding to a subject access request
- Maintaining comprehensive records of subject access requests and performance response times.

3.6 The main areas for improvement were noted as:-

- The post of the data protection lead has been dissolved and the responsibilities are yet to be reassigned
- The identification and appointment of Information Asset Owners (IAOs) needs to take place corporately
- No consistent review of data protection related policies
- There is no named individual or post with overall responsibility for the provision of data protection training
- There is no compulsory specialist training for employees undertaking roles such as Data Protection Officer, Senior Information Risk Owner, Information Lead Officers, Records Manager and IAOs
- A corporate Information Asset Register to be created and used to continually risk assess information assets
- There is no quality assessment of the application of subject access redactions and exemptions or responses to third party requests, unless requested by an Information Access Officer.

3.7 An action plan has been produced and an audit delivery group has been established to co-ordinate implementation of the ICO recommendations.

3.8 One of the recommendations from the ICO audit was to reinstate the post of the data protection lead (first bullet point in 3.6). A new post of Information Governance Manager has now been created to support the delivery of the action plan.

3.9 The ICO will undertake a desk-based follow up of the audit early in 2015. This will assess progress against recommendations and will require senior sign off at Chief Executive or Board member level. Following that audit the ICO will review the Council's rating.

4.0 ILOG Terms of Reference

4.1 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 an increasing return on information holdings and improvements to service delivery.

4.2 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.

4.3 Performance will be monitored through an annual report to Audit Committee on the status of the information asset and the first of these was brought to this Committee in June 2013.

4.4 ILOs will direct work streams within their service areas in accordance with the overall governance of the information asset.

4.5 The current ILOG work plan includes promoting improvements in:

- Identifying and classifying holdings of data and information
- Trustworthiness and reliability of data
- Storage of electronic holdings, paper documents and physical artefacts
- Privacy requirements
- Information exchange and sharing
- Information availability
- Reducing duplication of data
- Determining the council's approach to the information asset and providing analysis of its efficient and effective use.
- Staff and customer awareness and compliance with responsibilities

4.6 The group will continue to oversee action plans arising from the Information Governance risk audit completed by the Operational Risk Management Group.

4.7 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 Form, Freedom of Information Representatives and the Operational Risk Management Group.

4.8 The group is also supported by the Caldicott Guardians (the AD's for social care as the responsible managers for people's social and health data).

4.9 The group meets bi-monthly.

5.0 Actions

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

- Team briefing (Jan 14)
- Action plan rolled out following DAP audit
- Information Management staffroom pages revised
- Staffroom campaign during Oct 13 followed by Data Safe Course Nov 13 for all staff
- Information management capability included in staff appraisal
- Team Plymouth communication
- Staffroom articles (Jun 13/Sep 13/Nov 13/Dec 13)
- Information Governance risk audit
- Continued promotion of incident reporting so that lessons can be learnt
- Office walk-throughs continuing across Directorates

6.0 Future actions over the next 12 months

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

- Freedom of Information compliance to continue to be improved
- Information Asset Owners to be identified and trained within each service area
- Information Asset Registers to be created
- Carry out a further Information Governance risk audit via the Operational Risk Management Group
- Follow up action plan arising out of ICO/DAP audits
- Roll out Data Safe refresher training for all staff
- Introduce revised security policy framework
- Incident / Breach definition and reporting to be improved
- Develop an Information Governance communication strategy
- Produce an Information Risk Management Policy

7.0 Summary and conclusion

7.1 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

7.2 There are practical difficulties in trying to achieve this objective against a background of re-organisation and financial constraint and it will take a considerable culture shift within the organisation to ensure all processes and staff take appropriate care when handling data and look after the interests of the people of Plymouth.

7.3 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.