Audit and Governance Committee 17 April 2013

Report of the Senior Information Risk Owner

Information Governance Strategy

Summary

1 The purpose of the report is to inform Members about the Information Governance Strategy developed by the council's Corporate Information Governance Group (CIGG) and progress in implementing the strategy discussed by the committee on 13 February 2012.

Background

2 Information is a key asset which enables the council to deliver high quality services. However, there are responsibilities in maintaining such information and significant risks if proper standards and procedures are not adhered to. This paper summarises the responsibilities and risks, and progress in implementing the strategy the council has adopted to ensure robust information governance arrangements are developed.

Responsibilities & Risks

3 Recent years have seen an increased volume of legislation affecting public sector use and maintenance of information, including the Freedom of Information Act and the Data Protection Act. Current government initiatives are also aimed at encouraging public access to data held by public bodies and this is likely to increase the exposure of the council if its information governance systems fail to meet required standards.

Data Breaches

4 Thus far the largest fine levied by the Information Commissioner has been against Brighton and Sussex

University Hospital NHS Trust who were fined £325,000 for loss of patient data. In the last year several local authorities have been fined by the Information Commissioner following breaches of the Data Protection Act. Some of the high profile cases include:

- Telford and Wrekin Council - £90,000 fine for the disclosure of confidential and sensitive personal data relating to four vulnerable children.
- The London Borough of Barnet – fined £70,000 as a result of losing paper records containing highly sensitive and confidential information, including the names, addresses, dates of birth and details of the sexual activities of 15 vulnerable children or young people. The loss occurred when a social worker took the paper records home to work on them out of hours. The social worker's home was burgled and a laptop bag, containing the records and an encrypted computer, was stolen.
- Scottish Borders Council - £250,000 fine after former employees' pension records were found in an over-filled paper recycle bank in a supermarket car park. The Council employed an outside company to digitise the records, but failed to seek appropriate guarantees on how the personal data would be kept secure.
- Stoke-on-Trent City Council - £120,000 fine following an incident in which unencrypted sensitive information about a child protection legal case was emailed to the wrong person. This followed a similar breach in 2010.
- Plymouth City Council - £60,000 fine when the details of a child neglect case were sent to the wrong recipient..
- Leeds City Council - £95,000 fine when sensitive personal details about a child in care was sent to the wrong person, revealing details of a criminal offence, school attendance and information about the child's relationship with their mother.
- Devon County Council - £90,000 fine when a social worker used a previous report as a template for an adoption panel report they were writing, but a copy of the old report was sent out instead of the new one. The mistake revealed personal data of 22 people, including details of alleged criminal offences, extended family details, religion and mental and physical health.

- London Borough of Lewisham - £70,000 fine when, a social worker left sensitive documents in a plastic shopping bag on a train, after taking them home to work on. The files, which were later, recovered from the rail company's lost property office, included GP and police reports and allegations of sexual abuse and neglect.

5 In April 2011, City of York Council was required to sign an undertaking by the Information Commissioner following the inappropriate disclosure of an individual's personal data. This occurred as a result of information being erroneously included with documentation sent to an unrelated third party. While this breach did not result in a fine, it is likely that any further serious breach would.

6 Members will also be aware of the recent press reports concerning the loss of a number of files containing completed housing application forms. This incident is currently under investigation and CYC has reported the matter to the Information Commissioner's Office, who have initiated their own investigation.

7 Based on fines levied by the Information Commissioner so far, there is a pattern of escalating levels of fines, particularly where further breaches are identified following the signing of an undertaking. The maximum level of fine which the Information Commissioner can impose is currently £500,000, however if current EU proposals are implemented, this could rise to 5% of turnover.

Strategy

8 A copy of the information governance strategy agreed by the committee last year is attached at Annex 1. The strategy is based on a framework for information governance developed by the Cabinet Office. The framework defines five levels of maturity for information governance arrangements. Achievement at level one should be sufficient to ensure the council meets legal requirements. An action plan has been drawn up to ensure the council improves procedures where necessary to meet this level. It is intended to build on this over a number of years to meet higher levels of the framework. Details of initial actions required are set out in table 1 below.

Table 1: Action to meet level 1 of Information Maturity Model

Action	Current Position
Review the role of the Corporate Information Governance Group (CIGG) and re-launch	Revised terms of reference drafted and agreed by CIGG and the SIRO
Members of CIGG to attend training	Most members attended the joint training session with NYCC members in late 2011. Refresher training is planned for 2013.
New starters to CYC to have induction training covering Data Security	Specific training is currently covered as part of Directorate induction. Generic data security training in draft.
Promote data security awareness across the council using both Directorate communications and Colin	A regular series of Shout communications has been timetables and Shouts appear regularly on Colin Ongoing discussions are being held with key information asset owners to raise awareness and tailor the DP message to the needs to individual business areas. CYC has recently purchased the Metacompliance software to deliver training. This is currently being populated with training material.
Business Continuity Plans to be reviewed following the move to the new HQ	Encrypted laptops are being introduced and ICT are developing new BCPs for the new offices.

Action	Current Position
Review data sharing policy	Individual Directorates have their own arrangements. Veritau's Information Governance Team (IGT) are in ongoing discussions with key information asset owners to ensure data sharing policies are effective.
Complete Information Asset Registers for each Directorate	In progress. IGT is working with Directorates to identify and record their information assets.
Develop a document retention and destruction policy	This is being developed as part of the records management policy recently agreed by CIGG
Data security policies to be developed to guide home workers and staff hot desking	This is currently being developed by ICT and IGT in relation both to home workers and bring your own device initiative.

Consultation

9 Not relevant for the purpose of the report.

Options

10 Not relevant for the purpose of the report.

Analysis

11 Not relevant for the purpose of the report.

Council Plan

12 This report contributes to the council's overall aims and priorities by helping to ensure probity, integrity and honesty in everything it does.

Implications

13 There are no implications to this report in relation to:

- **Finance**
- **Human Resources (HR)**
- **Equalities**
- **Legal**
- **Crime and Disorder**
- **Information Technology (IT)**
- **Property**

Risk Management Assessment

14 The council will fail to properly comply with the undertakings given to the Information Commissioner in April 2011 and will be exposed to the risk of a significant financial penalty should a further data security breach occur. In addition, a further breach of sensitive data could undermine public faith in the council's ability to deliver services to the public.

Recommendation

15 Members are asked to;

- note the strategy adopted to improve information governance arrangements within the council, and the action being taken to achieve level 1 of the Information Assurance Model.

  Reason

  As part of the committee's responsibility to consider reports dealing with governance matters.

Contact Details

Author:

Roman Pronyszyn
Audit and Information Assurance Manager
Veritau Limited
01609 532284

Chief Officer Responsible for the report:

Ian Floyd
Senior Information Risk Owner
Telephone: 01904

Report Approved	√	**Date**

Specialist Implications Officers

Not applicable

Wards Affected: Not applicable **All** ✓

For further information please contact the author of the report