**Audit and Governance Committee** 13 February 2012

Report of the Assistant Director, Financial Services

# 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 proposed action to strengthen information governance arrangements.

## 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 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 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:

- Midlothian Council fined £140,000 for disclosing sensitive personal data relating to children and their carers to the wrong recipients on five separate occasions.

- Powys County Council fined £130,000 for a serious breach of the Data Protection Act after the details of a child protection case were sent to the wrong recipient.

- North Somerset Council fined £60,000 when a council employee sent five emails, two of which contained highly sensitive and confidential information about a child's serious case review, to the wrong NHS employee.

- Worcestershire County Council fined £80,000 for an incident where a member of staff emailed highly sensitive personal information about a large number of vulnerable people to 23 unintended recipients.

- Surrey County Council fined £120,000 after sensitive personal information was emailed to the wrong recipients on three separate occasions.

- Ealing Council fined £80,000 following the loss of an unencrypted laptop which contained personal information. Ealing Council breached the Data Protection Act by issuing an unencrypted laptop to a member of staff in breach of its own policies.

- Hounslow Council fined £70,000 following the loss of an unencrypted laptop which contained personal information. Hounslow Council breached the Act by failing to have a written contract in place with Ealing Council. Hounslow Council also did not monitor Ealing Council's procedures for operating the service securely.

5 In April last year, 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 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**

7 A copy of the information governance strategy 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 | Under review by the CIGG |
| Members of CIGG to attend training | Most members attended the joint training session with NYCC members in late 2011. |
| New starters to CYC to have induction training covering Data Security | Specific training is currently covered as part of Directorate induction/.<br>Generic data security training in draft. |

| Action | Current Position |
|---|---|
| Promote data security awareness across the council using both Directorate communications and Colin | To be rolled out through Colin and a series of “shout” communications being drafted. |
| Business Continuity Plans to be reviewed following the move to the new HQ | Encrypted laptops are being introduced and ICT will develop new BCPs in the period leading up to the move |
| Review data sharing policy | Individual Directorates have their own arrangements. Veritau’s Information Governance Team (IGT) will discuss individual arrangements and develop a benchmark |
| Complete Information Asset Registers for each Directorate | In progress. IGT to work with Directorates to identify and record their information assets. |
| Develop a document retention and destruction policy | Retention requirements will be identified as part of the Information Asset review. |
| Data security policies to be developed to guide home workers and staff hot desking | Currently under review |

## Consultation

8 Not relevant for the purpose of the report.

## Options

9 Not relevant for the purpose of the report.

## Analysis

10 Not relevant for the purpose of the report.

## Council Plan

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

## Implications

12 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

13 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

14 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:**

Keith Best
Assistant Director, Financial Services
Telephone: 01904 551745


| **Report Approved** | ✓ | **Date** | 31/01/12 |
|---|---|---|---|

**Specialist Implications Officers**

Not applicable

**Wards Affected:** Not applicable **All** ✓

**For further information please contact the author of the report**

**Background Papers**

None

**Annexes**

Annex 1 – Information Governance High level Strategy