Audit and Governance Committee 11 February 2015

Report of the Head of Internal Audit

Information Security Update Report

Summary

1 This report provides members with an update on the adequacy and effectiveness of the council's information security arrangements.

Background

2 The council recognises that information is a key business asset and that accurate and reliable information is important to support the provision of good quality services and the discharge of statutory obligations. Information governance (IG) plays a key role in ensuring that information is properly valued, used and protected.

3 The Data Protection Act requires organisations to take appropriate security measures to prevent personal data being accidently or deliberately lost, stolen, corrupted or otherwise compromised. In particular, organisations should:

- design and organise their security to fit the nature of the personal data that they hold and the harm that may result from a security breach;
- be clear about who in the organisation is responsible for ensuring information security;
- make sure they have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

4 A number of high profile cases in recent years have highlighted the consequences of personal information being accidently disclosed and hence the need for effective information security measures. Since April 2010, the Information Commissioner's Office (ICO) has had the power to fine organisations up to £500,000 for serious data breaches or losses. A significant number of organisations including many public sector bodies have been fined since then. Recent data security incidents include:

- Kent Police were fined £100,000 in March 2014 after highly sensitive and confidential information, including copies of police interview tapes, were left in a basement at the former site of a police station;

- The Ministry of Justice was fined £180,000 in August 2014 for serious failings in the way prisons in England and Wales had been handling people's information.

In addition, a number of councils and NHS bodies have been required to sign undertakings following data security incidents, as follows:

- Gwynedd Council signed an undertaking in October 2014 following two breaches of the Data Protection Act;

- South Western Ambulance Service NHS Trust signed an undertaking in October 2014. This followed an investigation into an incident involving the sharing of patient data with a local Clinical Commissioning Group (CCG) when there was no proper legal basis to do so. There were also security concerns surrounding the manner in which the data was stored on discs when being distributed to the CCG;

- Basildon and Thurrock University Hospitals NHS Foundation Trust signed an undertaking in October 2014. This follows an investigation into two reported incidents involving disclosures of personal data to third parties in error;

- The Council of the Isle of Scilly signed an undertaking in September 2014. This follows an investigation into two separate incidents. The first related to confidential information which was part of a disciplinary hearing being

sent unredacted to third parties. The second incident involved the disclosure of sensitive personal data which formed part of an internal investigation against a high profile figure which ended up in public circulation.

5 The council recognises the financial, service and reputational risks associated with the control of personal data, particularly in electronic form. In 2011, the council was required to sign an undertaking following the accidental disclosure of sensitive personal data as a result of documents taken from a shared printer not being checked properly before being copied for distribution. The council has also experienced two serious data security incidents in the last two years. Both incidents were reported to the ICO. The ICO investigated the breaches but decided to take no further enforcement action. Whilst progress has been made to strengthen corporate information governance arrangements, information security is an area where concerns remain. As a result, it was included as a significant governance issue in the council's 2014 Annual Governance Statement.

Information Security Arrangements

6 The council has established a policy and control framework to safeguard information and mitigate the risk of data security incidents occurring. The current framework includes:

- Strategic overview by the Corporate Information Governance Group (CIGG) and the council's Senior Information Risk Owner (SIRO);
- A comprehensive information governance policy framework;
- Appropriate technical IT controls which restrict access to the council's network and data, and provide ongoing monitoring to detect possible threats or vulnerabilities;
- Appropriate physical controls which prevent unauthorised access to West Offices and other council buildings;
- The preparation of information asset registers within each service area to help with the identification of key risks;

- A programme of ongoing information security compliance checks undertaken by ICT and Internal Audit;

- Ongoing staff training and measures to raise awareness of information risks and threats;

- A procedure for reporting and investigating data security incidents so that remedial action can be taken and lessons learnt.

Recent Developments

7 As reported to the last meeting, the corporate information governance framework is continuing to be developed. In respect of information security the following changes have taken place:

- A revised approach to quarterly data breach reporting has been adopted;

- A draft data sharing protocol has been developed in conjunction with North Yorkshire County Council, North Yorkshire Police, the York Teaching Hospital Foundation Trust and North Yorkshire Fire and Rescue Service. The protocol is an overarching framework designed to ensure information is shared lawfully, appropriately and in compliance with best practice;

- Work is ongoing to demonstrate compliance with the Health and Social Care Information Centre (HSCIC) IG Toolkit;

- An audit of information security is in progress and will be completed shortly. The audit has included a review of governance arrangements, data sharing, mobile working, physical security and incident management.

8 In addition, ICT have successfully secured the council's Public Sector Network (PSN) code of connection accreditation late last year through its programme of security and risk mitigation based activities / projects. These included but were not restricted to the following, and were part of the 'must have in place' list that formed part of last year's PSN controls for the council and other public sector organisations:

- The introduction of an approved Mobile Device Management (MDM) system to facilitate more control of the council's mobile devices. The system also enables ICT to remotely remove any data should a device be lost or stolen;

- ICT have moved all schools e-mail to Outlook Web Access (OWA) which has a more robust authentication access process. This has also been added to the access process for all CYC staff or members who access e-mail via OWA;

- ICT and their network partner, Pinacl Solutions, have installed a new 'walled garden' between the council's data / systems and the outside world to help improve the defence against e-based attacks and attempts to penetrate into the network/ICT infrastructure;

- The introduction of new remote connection systems that help improve the council's ICT defences. The new systems also facilitate various other improvements including; a higher level of control; device scanning and segregation of the different types of network traffic that require varying degrees of security and access rules / controls to be applied;

- The introduction of a system called iComply that will help increase staff awareness of information security and other policies – both corporate and directorate. The new system maintains records of completion and can also confirm understanding of the new or amended policies.

Data Security Incidents

9 Data security incidents are recorded and reported to CIGG. Where necessary action plans are developed to address the causes and hence reduce the risk of any recurrence. Serious incidents will be investigated by Internal Audit and the results reported to the SIRO. In the 9 month period to 31 December 2014, 28 data security incidents were reported. One of these cases was subsequently found to relate to a third party rather than the council. The reported incidents include:

- five cases where personal data was sent by post to the wrong recipient;

- seven cases where e-mails containing personal data were sent to the wrong recipient (including other council employees);

- eight cases where documents / files containing personal data were incorrectly disclosed;

- one case where sensitive personal data was e-mailed to the correct recipient but the method of transmission was not sufficiently secure;

- two cases where e-mail accounts were not properly amended / closed when members of staff transferred to new roles;

- one case where an e-mail to multiple recipients was not sent using the blind copy function;

- one case where a mobile device containing personal data was lost in a public place.

Data Security Compliance Audits

10 Two data security compliance audits have also been completed in 2014/15 to date. The audits involved unannounced checks of areas within West Offices and other council establishments to determine whether personal data and other information assets were properly secured. The first audit was undertaken in September 2014 and the report was finalised in December. The audit found that the council is generally well protected against the accidental disclosure of personal or confidential data as the majority of documents are stored in cupboards within physically secure areas. However, some of this storage is still being left unlocked when unattended. In addition, some open storage, such as bookcases, is still being used at Hazel Court for the storage of personal, sensitive and confidential data. Compliance with the council's clear desk policy is also much improved but still not complete. In addition, a number of security weaknesses were observed. The internal auditors therefore concluded that an acceptable control environment was in operation but there were a number of improvements that needed to be made. The overall opinion of the control environment was that it provided 'reasonable assurance'. Further details on the findings will be reported to this committee in April.

11 A second audit was undertaken in December 2014 and a draft report has been circulated to CIGG members for comments. This audit has found an overall improvement in data security compliance. A small number of specific issues have been reported to the SIRO and will be followed up. A third audit is planned in the next few weeks.

Consultation

12 Not relevant for the purpose of the report.

Options

13 Not relevant for the purpose of the report.

Analysis

14 Not relevant for the purpose of the report.

Council Plan

15 The council's information governance framework offers assurance to its customers, employees, contractors, partners and other stakeholders that all information, including confidential and personal information, is dealt with in accordance with legislation and regulations, and its confidentiality, integrity and availability is appropriately protected.

Implications

16 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

17 The council may face financial and reputational risks if the information it holds is not managed and protected effectively. For example, the ICO can levy fines up to £500k for serious data security breaches. The failure to identify and manage information risks may diminish the council's overall effectiveness.

Recommendation

18 Members are asked to:

a) note the progress made to maintain and develop the council's information security arrangements.

Reason

To enable members to consider the effectiveness of the council's information security arrangements and the steps being taken to address the issue identified in the last Annual Governance Statement.

Contact Details

Author:	**Chief Officer Responsible for the report:**
Max Thomas Head of Internal Audit Veritau Limited 01904 552940	Ian Floyd Director of CBSS Telephone: 01904 551100

Report Approved	✓	**Date**	27/01/15

Specialist Implications Officers: Not applicable

Wards Affected: Not applicable **All** ✓

For further information please contact the author of the report

Background Papers: None

Annexes: None