Internal Audit Report

IS Data Handling (Members)
2012/13
Report ref: C3/5

Report Issued	Draft: 17/05/13 Final: 16/08/13

No
Level of
Assurance

Contents

Auditor:

J. Fearn

Distribution:

Name	Job Title
G. Thistlethwaite	ICT Shared Services Manager
P. Shevlin	Chief Executive
P. Ellis	Director of Services

1 Background

1.1 This audit is being undertaken as part of the shared annual audit plan for 2012/13. The subject is particularly topical at present, given the recently publicised instances of monetary penalties being served on Local Authorities by the Information Commissioner for serious breaches of the Data Protection Act; £70k for the loss of an unencrypted laptop continuing personal information and £140k for the disclosure of sensitive personal information to the wrong recipients being just two examples. The Local Government Data Handling Guidelines have been used as a basis for this audit.

1.2 Internal Audit is an assurance function that provides an independent and objective opinion to the Council on the control environment by evaluating its effectiveness in achieving the Council's objectives. Internal Audit objectively examines, evaluates and reports on the adequacy of the control environment as a contribution to the proper, economic, efficient and effective use of resources.

1.3 The following key control objectives (KCOs) are applicable to the audit:

- The culture developed by the Authority ensures that information is properly valued and protected by Members
- Security of information is ensured through the physical security of systems and surroundings
- Proper information handling standards are in place.

2 Audit Scope

2.1 The testing strategy is outlined below which entailed documentation review and discussion with staff.

KCO	Test
The culture developed by the Authority ensures that information is properly valued and protected by Members	Ensure all Members have received appropriate training upon appointment and understanding is periodically monitored.
Security of information is ensured through the physical security of systems and surroundings	Determine appropriate security is in place, personal / sensitive information is securely destroyed when no longer needed, and establish the use of encryption.
Proper information handling standards are in place	Ensure Members are aware of appropriate transfer methods. Ensure Members are included on the notification to the Information Commissioner's Office (ICO) as able to receive personal information from the Authority

3 Audit Opinion

3.1 A summary of Internal Audit's opinion levels and their definitions is provided below:

Level	Definition
Significant Level of Assurance	The system of internal control is designed to support the Council's corporate and service objectives and controls are consistently applied in all the areas reviewed.
Good Level of Assurance	There is generally a sound system of control designed to support the Council's corporate and service objectives. However, some improvements to the design or application of controls is required.
Partial Level of Assurance	Weaknesses are identified in the design or inconsistent application of controls which put the achievement of some of the Council's corporate and service objectives at risk in the areas reviewed.
No Level of Assurance	There are weaknesses in control, or consistent non-compliance which places corporate and service objectives at risk in the areas reviewed.

3.2 This audit has been given a No Level of Assurance. None of the key controls are considered to be met with 5 recommendations being made overall; all graded at priority one. Errors made in the way personal /sensitive information is handled can not only harm individuals but also the reputation of the Authority and potentially incur a substantial fine from the Information Commissioner.

3.3 It was previously recommended in the last Data Handling audit, which excluded Members and was awarded a partial level of assurance, that Management should consider and implement the most appropriate way in which to periodically monitor user understanding , however, the Auditor was informed of a lack of available resource to enable such ongoing monitoring. More recently, Internal Audit have been informed that the way in which to approach this issue is currently being considered. No corresponding recommendation is therefore being made in this report given the circumstances although this situation can only be highlighted as a risk.

3.4 The recommendations made in section 4 below have been discussed with the ICT Manager who confirmed awareness of the issues and is seeking to implement actions which will best address them in the near future.

4 Detailed Findings & Action Plan

The audit findings are detailed in this section on an exception basis only for the attention of management, therefore KCO's with adequate controls are not included.

Recommendations are prioritised as follows:

Priority 1 - These relate to significant gaps in the Internal Control Framework
Priority 2 - These relate to minor gaps in the Internal Control Framework or significant issues of non-compliance with key controls
Priority 3 - These relate to minor issues of non-compliance with controls.

Ref	Findings	Risk	Recommendations and Management Response	Officer Responsible and Implementation Date
KCO1: The culture developed by the Authority ensures that information is properly valued and protected by Members				
1.	Members have not received data protection and information security training, although this issue was raised at CLT in March 2012. At the time of writing, quotes had been received for data protection training and procurement of such was subject to available funding.	Potential breach of data protection legislation for failing to meet data handling obligations, should funding to train Members be unavailable, which could risk substantially harming the Council as well as individuals.	**R1: (Priority 1)** Funding should be found to allow Management to instigate appropriate training for all existing Members and ensure that any newly appointed Members in the future receive the same. **Management Response:** Agreed.	ICT Shared Services Manager 15/12/13

Ref	Findings	Risk	Recommendations and Management Response	Officer Responsible and Implementation Date
KC02: Security of information is ensured through the physical security of systems and surroundings				
2.	Members do not have access to the Acceptable Use Policy or the Data Protection Breach Policy which outline information security responsibilities. However, both refer more to employees than Members, the latter who, at present, do not have Craven email accounts and, with one exception, do not have Council issued laptops ie. the facility and equipment to which the acceptable usage of the policy applies. Neither are Members required to sign the Acceptable Use Policy, in the way that employees do, to indicate their agreement and to abide by the Policy's conditions.	Potential inadvertent breach of the Data Protection Act (DPA) due to Members being unable to reference their obligations in the absence of any documented guidance.	**R2: (Priority 1)** Rules surrounding information security responsibilities should be produced and documented for Members, given the way in which they currently operate, and their agreement to abide by conditions obtained. Any future operational changes should be appropriately reflected in these rules via their update. **Management Response:** Agreed	ICT Shared Services Manager 15/12/13

Ref	Findings	Risk	Recommendations and Management Response	Officer Responsible and Implementation Date
3.	With the exception of the Leader, all Members use their own IT equipment, as opposed to any issued by the Authority, together with non CDC email accounts and additionally do not have access to the Council's network. Information transmitted to Members from the Council in general tends to be through the post although can on occasions be emailed to such private email addresses necessitating leaving the Council's network. Information concerning official business held in private email accounts is subject to the Freedom of Information Act (FOI) and therefore where it is believed an account may hold information which falls within the scope of an FOI request, this will necessitate an account search. It is understood through review of a report by the ICT Manager earlier during 2012 that a number of proposals were put to CLT to address the risks that this situation poses.	Potential harm to stored data through Member use of non-Council encrypted equipment potentially without appropriate anti-virus software. Breach of data protection legislation in the event of unencrypted equipment containing personal and/or sensitive data being lost or stolen leading to a potential fine Potentially unrecoverable data due to non-inclusion in the backup process through not being linked to the network	**R3: (Priority 1)** The means of enabling Members to use appropriately encrypted equipment should be pursued. **Management Response:** Agreed	ICT Shared Services Manager 15/12/13
4.	There has been no Member training nor any issued instructions as to correct storage and/or disposal of personal/sensitive information. Users of Council issued electronic media contact IS directly to advise of potential disposal, after which items are securely held in storage prior to collection by a third party who wipes hard drives and issues a certificate to CDC confirming appropriate destruction. Given that Members, with the exception of the Leader, use their own IT equipment, disposal would not be carried out in the same secure way.	Non compliance with the DPA and potential ICO issued fine for data loss caused by inappropriate storage and /or data reconstruction caused by inappropriate disposal of personal / sensitive information	**R4: (Priority 1)** Training and documentation provided to Members should include guidance on the proper storage and disposal of any personal and / or sensitive information **Management Response:** Agreed	ICT Shared Services Manager 15/12/13

Ref	Findings	Risk	Recommendations and Management Response	Officer Responsible and Implementation Date
KCO3: Proper information handling standards are in place				
5	The ICT Manager's report to CLT during 2012 put forward options for consideration which would improve security and data handling including transitioning Members to downloading from a secure area on the Council's network, creating CDC email accounts for Council business and the provision of laptops and/or Blackberrys	Non compliance with the DPA and potential ICO issued fine for failing to adequately protect data	**R5:(Priority 1)** Management should progress the options previously reported to CLT so as to ensure that personal and/or sensitive information is handled securely **Management Response:** Agreed	ICT Shared Services Manager 15/12/13

The agreed actions will be subject to a follow up review to establish whether they have been implemented as part of the quarterly performance monitoring clinic.

Any queries or requests for further information regarding this report should be directed to Internal Audit on 706360 or on 01423 556116. Internal Audit would like to thank the officers involved for their assistance during this audit.