



Removable Media

Internal Audit Report

2010 / 2011

Kevin McLafferty

Auditor

14 June 2011

Contents

Audit: Removable Media
Auditor: Kevin McLafferty

If viewing on-screen, please click on the links below or use the scrolling arrows

Introduction.....	Page 3
Scope.....	Page 3
Findings.....	Page 3
Conclusions.....	Page 5
Action Plan.....	Page 6



1. Introduction

- 1.1 The Council's computer network is a secure system. Officers will from time to time need to access the network from portable devices: for example USB sticks, laptops, cameras etc. These can potentially represent a serious threat to the networks security. The Council recognises that it is important that officers have access to these devices. However, they must be used in accordance with set procedures and policies. This way the risk can be mitigated.
- 1.2 In February 2010 the Council introduced a new Communications and Operations Management policy to comply with the Governments Code of Connectivity. Incorporated within this policy is a Removable Media policy that governs the use of all removable media used by the Council. In March 2007 the Council introduced software called 'Devise-lock' to restrict access to the network to authorised devices only.

2. Scope

- 2.1 The audit focused on compliance with the requirements placed on the Council by the Governments Code of Connectivity in particular;
- Inventory control.
 - Contents management.
 - Physical and virtual security of devices.
 - Training and guidance given to staff.
 - Incident reporting.

3. Findings

- 3.1 The Council has over the past 10 years for operational reasons purchased various items of removable media that allow officers to carryout their duties whilst away from the office. These include cameras, laptops, external hard drives and UBS sticks. From the onset the business need for this equipment was the driver and they were purchased at the request of the Service and distributed to officers without any formal guidance. The then Communications policy only stated 'Never introduce a disc or CD into a PC without having it virus checked by IT Services'. This resulted in most departments purchasing their own removable media without any reference to the Council's IT operations team.



- 3.2 The amount of removable media within the Council continued to expand as departments purchased cameras, USB sticks and PDA's. All of which required to be connected to the Council's secure network in order to transfer the data stored on them on the department's records. In March 2007 the Council installed 'Devise Lock'. This restricts access by removable media to the Council's secure network as it only allows pre-registered devices to communicate with the network. 'Devise Lock' is also used as the inventory of removable media, which had not existed prior to its introduction. However, a formal naming convention was not applied to 'Devise Lock' and as a consequence it has not always been possible to identify who has been issued with a particular piece of removable media.
- 3.3 In February 2010 the Council introduced its first specific removable media policy in order to comply with Government Connect requirements. All staff and Councillors are required to sign this policy. As at the date of publication there are still 14 members of staff who have yet to sign this new policy. The policy gives clear guidance on how removable media should be used, the level of security to be applied and the classification of data that can be stored on them.
- 3.4 Using the inventory from 'Devise Lock' the audit verified that the removable media identified was held by the service and the contents of the media was held in accordance with the policy. The audit found in a sample of laptops, cameras and PDA's the devices were correctly registered on 'Devise Lock' and in the case of laptops they were all encrypted. However, in the case of USB sticks the picture was different.
- 3.5 'Devise Lock' has 177 USB sticks registered on it. As mentioned in 3.2 the absence of a naming protocol has meant that it has not always been possible to identify who the USB stick was issued to. The initial audit sample found that staff could not locate the USB's that had been issued to them. Consequently the sample was expanded to include all 177 USB sticks registered on 'Devise Lock'. The audit was able to locate 107 of the USB sticks registered on 'Devise Lock'. 70 USB sticks have been lost or destroyed.
- 3.6 Of the 70 lost USB sticks no service is immune from having a missing USB key. 14 of the missing USB sticks are recorded as being issued to members of staff who have left the Council's employee. The current exit procedures does not identify if the departing employee has been issued with a USB stick. USB sticks will in future be allocated to a small number of staff, with IT operations holding and keeping a log of 20 encrypted sticks for occasional use.



- 3.7 Officers have not kept formal records of the contents of USB sticks. The sticks have typically been used to store presentations to external bodies, for home working and data transfer. It wasn't until February 2008 that staff were advised that it was not permitted to work on classified data from home using either e-mail or USB sticks to transfer the data. Staff are only permitted to work from home using the Virtual Private Network (VPN).
- 3.8 The audit reviewed the content of all USB sticks that could be located and found that there were only 3 USB sticks that held data that the Council had classified as 'Confidential' by the user, this data consisted of an April 2009 copy of the Emergency Contact Directory. The Directory contains the names and contact numbers of key officers in Chichester District Council and neighbouring authorities. Additionally it contains the names, address, telephone numbers and e-mail address of the then Parish Clerks. The contact details of the Parish Clerks would have been in the public domain at the time the document was produced. Under the Governments Code of Connectivity (aka Co-Co) data classification this document would have been classified as 'Protect'. One of the missing USB sticks is known to have contained this document.
- 3.9 Staff who have been issued with or have had access to one of the missing USB sticks have been interviewed through the course of this audit. They have all consistently stated that they did not copy any 'Personal' and/or 'Sensitive' data on the USB stick. It would be preferable if all data produced by the Council were automatically classified within the Co-Co definitions. However, in view of the costs associated with procuring a system to accomplish this, it is not being considered at the present time.
- 3.10 It is a requirement of the Council's removable media policy that all removable media is virus checked prior to it being connected to the Council's network if it has been used outside the network. Since May 2008 IT Operations has kept a record of all devices that have been virus checked. The audit checked the record of virus checking against the missing USB sticks and found that none of the missing USB sticks had ever been virus checked.

4. Conclusion

- 4.1. The Council has ensured that all its laptops are suitable protected. However, it failed to control the issue of USB sticks to officers. Controls were put in after the USB sticks had been issued, and it is



clear that officers either ignored them or were unaware of their existence. Despite the various reminders issued by the IT service.

4.2 Technology has moved on and USB sticks are no longer required by staff to work remotely as the VPN is now the only permitted method of remote working. This audit has made 3 recommendations on the future of USB sticks; these can be seen in the accompanying action plan.

4.3 Internal Audit was concerned that the loss of the 70 USB sticks needed to be reported to the Information Commissioner as a possible breach of the Data Protection Act 1998. However advice from Legal Services is that it need not be reported on the basis that the only known personal data on a missing stick was already in the public domain. The Audit failed to find any evidence that the missing USB sticks contained personal data.




4.4 The lack of clear guidance when the USB sticks were issued is the prime cause for the loss. Officers have failed to understand the importance of proper control of the devices and it is likely that they have been lost over the passage of time or in the course of the recent office moves.

4.5 The recent removable media policy and a withdrawal of all but essential USB sticks will mitigate the risk of the Council being sanctioned by the Information Commissioner.



Audit: Removable Media
Auditor: Kevin McLafferty

Ref	Recommendation	Officer	Priority	Agreed?	Comments	Implementation Date
3.2	All removable media should be recorded on 'Devise Lock' in a standard format.	Karen Parsons	Medium	Yes	Using 'Devise-Lock' to record all removable media is now standard practice within ICT Operations.	Completed
3.2	All unencrypted USB sticks are withdrawn and destroyed.	Jane Dodsworth	High	Yes	In progress exercise currently being undertaken	July 2011
3.2	The Council has a policy that only encrypted USB sticks are issued.	Jane Dodsworth	High	Yes	Removable Media Policy to be updated. To coincide with annual Code of Connection audit at the end of August.	October 2011

 **High = Fundamental System Weakness – Action is Essential.**
 **Medium = Potential Control Weakness – Action Required**
 **Low = Advised for Best Practice**