# Bolsover, Chesterfield and North East Derbyshire District Councils'

# Internal Audit Consortium

# Internal Audit Report

| | |
|---|---|
| **Authority:** | **Chesterfield Borough Council** |
| **Subject:** | **Laptops and Other Removable Media** |
| **Date of Issue:** | **23rd January 2019** |
| **Level of Assurance** | **Limited Assurance** |
| **Report Distribution:** | **Customers, Commissioning and Change Manager**<br>**Head of ICT Improvement** |

Bolsover District Council

CHESTERFIELD BOROUGH COUNCIL

North East Derbyshire District Council

# INTERNAL AUDIT REPORT

# ICT

# Laptops and Other Removable Media

## Introduction

An internal audit review has recently been completed to evaluate the processes relating to Chesterfield Borough Council's (CBC) Laptops and Other Removable Media provisions.

## Scope and Objectives

The objectives of the audit were to ensure that adequate controls are in place to prevent loss of media, loss of information, introduction of malware and reputational damage.

The areas examined as part of the audit were: -

- The Policies and procedures in place
- Equipment / Inventory checks
- Government connect requirements
- Internet Usage Monitoring
- Virus Protection
- Connection to network
- Insurance
- Encryption and Security
- 4G MiFi Devices
- Smart Phones
- Elections Tablets

PCs, laptops and other removable media used by Council Members are to be reviewed as part of the 2019/20 audit plan.

## Conclusion

The overall assessment of the internal controls operating in relation to the administration of the Council's Laptops and Other Removable Media based on the areas reviewed was **Limited Assurance** (Certain important controls are either not in place or not operating effectively. There is a risk that the system may not achieve its objectives. Some key risks were not well managed). The findings together with recommendations to address any issues identified are highlighted in the following report.

Acknowledgement

The Auditor would like to thank the ICT, Elections, Business transformation and Information assurance Officers for their assistance and patience during this audit.

## Findings and Recommendations

Policies and procedures

1. The policies in place related to laptops and other removable media are the Acceptable Use of Information and ICT Policy, updated on the 01/05/2018, Information Security Policy, updated on the 01/05/2018 and the Information Security Guidance, last updated on the 31/05/2018. All the policies are available to staff members via Aspire.
2. The Acknowledgement form which is signed to accept that ICT policies of Chesterfield Borough Council was not up to date at the start of the audit, ICT have now up dated this form.

Equipment / Inventory checks

3. On the eighteenth of October 2018 ICT returned from being outsourced to Avarto back in-house, the procurement procedure is now being reviewed to bring it in line with this change. Previously the process was that CBC would inform ICT of their requirements and IT would purchase the item/s required.
4. The procurement thresholds and the procedure at each threshold, is available to ICT staff via the intranet.
5. A sample of twenty employees who had been issued laptops and tablets were selected to ensure they were current employees. Three employees from the sample were no longer working with Chesterfield Borough Council. The details of the three employees were passed to ICT and checking showed that user accounts had been deactivated. It was a reoccurring theme during the audit that the primary database for laptops and other removable media was not being updated.

| | **Recommendation** |
|---|---|
| **R1** | It is essential that the primary database held in ICT which records the distribution of laptops and other removable media devices owned by Chesterfield Borough Council is being updated in an efficient and precise manner.<br>***(Priority: Medium)*** |

6. Testing was undertaken on a sample of fifteen laptops and five tablets to ensure appropriate forms had been completed when the equipment was issued to the user.
7. It was identified that two laptops (CBCHP-FLEXI88 AW & CBCHP-FLEXI315 SM) and two tablets (TAB-02 & TAB-04) from the sample did not have the appropriate forms completed and filed. A further seven laptops and two tablets had forms on file that did not match the registered user on the primary excel database held in ICT.
8. Further investigation identified that another nineteen laptops had been issued for which no signed ICT form was in the file, this included laptop numbers CBCHP-FLEXI288, CBCHP-FLEXI293 and CBCHP-FLEXI302.

| | Recommendation |
|---|---|
| **R2** | All laptops and tablets issued should have an ICT Equipment form completed and filed in ICT. ICT Equipment transferred to a different user should have a new form completed<br>***(Priority: Medium)*** |

9. A sample of fifty-four leavers from 01/04/2018 to 23/11/2018 was reviewed to confirm if they had been assigned a Laptop, iPad or Tablet on the primary database held in IT.
10. Four leavers were confirmed on the primary database marked as still employed, a review of the accounts for these employees confirmed that they had been disabled. The primary database is not being updated when laptops are transferred to new users or accounts are disabled for leavers. **See Recommendation R1**.
11. ICT informed the auditor that the process at the moment for laptops when an employee leaves is, that the laptop stays with the department and is marked on the database with the leavers name and '*post is to be filled*'. When the post is filled the new user is added and the leaver is removed.
12. It was identified during the review through discussions with ICT that the equipment issued is not always returned and at times is returned faulty, ICT only find out about this after the user has left CBC. Laptops are being held by the departments for long period's rather than being returned to ICT when an employee leaves, in one instance even when the post is not being recruited to (Senior Admin Assistant Insurance).

| | Recommendation |
|---|---|
| **R3** | A policy needs to be established to give clear guidance to management with regards to returning laptops/removable media equipment to IT when an employee leaves their post and ensuring IT are made aware if equipment is transferred to a different user.<br>***(Priority: Medium)*** |

13. The review identified that there is no requirement to keep any record of laptops/tablets that are lost or stolen however ICT had been informed regarding lost or stolen items in each incident. Internal audit is not being informed of the loss in accordance with the current Information Security Guidance. In one incidence the Information Assurance Manager was also not informed of a lost Tablet. Where a laptop has been lost or suspected stolen it should be reported to the police to improve the chances of recovery through websites such as 'checkmend' which are used by pawn brokers to ensure goods they are purchasing are not reported lost or stolen. Reporting incidents to the police would place the information regarding the item on the website so it can be traced if it is being sold.

| | Recommendation |
|---|---|
| **R4** | The Information Security Guidance should be followed to report lost/stolen media to Internal Audit and the Information Assurance Manager. Lost or stolen devices should be reported to the police to increase the chance of recovery and records should be kept regarding the incident including time, date, incident description and police incident number.<br>***(Priority: Medium)*** |

14. Audit was informed that laptops hold profiles for each user that has logged into the laptop. These profiles are not deleted however access to these is restricted to users with admin rights. Removable media devices are only wiped if requested by the manager and returned removable media is held in a secure lockable cabinet.

| | Recommendation |
|---|---|
| **R5** | The user profiles held on the laptops should be deleted when a user is no longer employed by Chesterfield Borough Council.<br>***(Priority: Low)*** |

15. ICT have a recurring call on the Service Desk for running a free tool which identifies any devices which have not been in contact with the corporate domain in 90 days. They then look through the devices to determine which devices are actually no longer in use as not all can be removed as they are stand-alone units, presentation pc's or devices which have not been turned on as staff might be on long term sick leave etc. Those then confirmed as no longer required get deleted from Active Directory as well as any other system we have referring to a device computer name. This stops anyone trying to use the device or prompts them to contact ICT to start using it.

Government connect requirements

16. It was established that since the ICT Network Security audit (December 2017), PSN compliance has been achieved for the period January 2018 to January 2019.
17. The ICT health check was completed shortly after PSN compliance was approved. It was confirmed that the council also achieved cyber essentials plus certification for the first time in April 2018. The cyber essentials plus certification will be due for renewal in April 2019.

Internet Usage Monitoring

18. Smoothwall web filter is in use at CBC, as a physical device that acts as gateway between the internet and our PCs and the internet to protect them against malicious software and code. Smoothwall blocks certain sites and can be programed with generic rules these can be amended by ICT so access is granted to some users as required.
19. Monitoring is only undertaken if required/requested for example during investigations. Log files are created and stored and can be checked back if required.

Virus Protection

20. Discussions with ICT revealed that there is no report on Sophos system to check if all devices are connecting to and updating the virus protection software. The ICT Support Officer reviews this through the Sophos console itself, however this has not been undertaken recently due to staff shortages on the service desk. There is no recurring service desk task set up for this, however IT are happy to have a task set up with a frequency of every three months.

| | **Recommendation** |
|---|---|
| **R6** | As Agreed ICT will setup a recurring service desk task to check if Sophos is updating appropriately, this will be undertaken on a monthly basis. ***(Priority: Low)*** |

21. The laptops used by audit staff were checked and the virus protection software was up-to-date.

Connection to network

22. Remote Access to the network requires 2 factor authentication as well as requiring specific network certificates (can only be provided by ICT) before access to CBCs Virtual Private Network is granted.

Insurance

23. The review identified that the insurance schedule was not up-to-date, equipment that had been purchased after the insurance renewal date had not been added to the schedule.

| | **Recommendation** |
|---|---|
| **R7** | ICT should insure that the Insurance section are informed regarding new purchases so that the insurance schedule can be updated to guarantee adequate cover is in place for laptops owned by Chesterfield Borough Council. ***(Priority: Medium)*** |

Encryption and Security

24. The information security guidance policy under the removable media guidance section states that '*sensitive information should be encrypted on removable media'*. Only ICT approved memory sticks can be used to connect to the network.
25. During the review it was identified that the use of memory sticks is very low as most staff are now using laptops to logon to the servers and don't need to transfer data however memory sticks are available in ICT for any staff who need them. If a memory stick that is not ICT approved is used it would be blocked and the user asked to get in touch with ICT.
26. When a user wishes to use data from an external CD or USB memory stick the policy states that user is required to contact ICT to ensure the media is safe to use. This is checked by using a "*Sheep Dip*" terminal which is not connected to the network. When

any media gets tested it is logged within ICT records. Examination of the "*sheep dip*" record shows that 12 tests have been completed since April 2018.

27. It was confirmed during the previous ICT Security audit that encryption on all of the councils laptops has been completed using the Bitlocker application. Encryption ensures all data stored within device is not accessible without entering a username and password.
28. Mobile devices issued by ICT such as Smart phones, iPads and tablets do not directly connect to the network. Only to the E-Mail server. These devices are managed by an application called MobileIron, which in case of loss/theft, can remotely erase all data and lock the devices.

29. The ICT Service Lead informed audit that laptops do not have permanent markings, showing that they belong to CBC. Testing showed the laptops used in audit do not have permanent marking showing that they belong to CBC.
30. The tablets used by the elections section do not have any permanent marking and the IPads issued by CBC do not have permanent markings also the USB's held in IT just have a tag and are not permanently marked as CBC.

| | **Recommendation** |
|---|---|
| **R8** | A review of having permanent markings (Asset Tags) on laptops and other removable media should be carried out to determine if it would be beneficial. ***(Priority: Low)*** |

31. The information security Guidance policy is available on CBC intranet and has a section on removable media which includes laptops, memory sticks and other removable media. The safe use of laptops for home working refers to physical safety issue around laptops.

4G MiFi Devices

32. During the review ICT were asked regarding the issuing and monitoring of 4G MiFi Devices held by CBC. ICT informed the auditor that Business Transformation are responsible for 4G MiFi Devices, however when asked, Business Transformation informed the auditor that ICT are responsible for 4G MiFi Devices.

| | **Recommendation** |
|---|---|
| **R9** | ICT and Business Transformation need to agree who is responsible for the issuing and monitoring of 4G MiFi Devices in use at Chesterfield Borough Council. ***(Priority: Medium)*** |

Smart Phones

33. Through discussions with the Business Transformation Officer it was identified that Mobile phones and Tablets are sometimes purchased before a valid purchase order is in place.
34. Upon reviewing the reports from billing manager for November 2018 it was identified that four employees no longer employed by CBC are still allocated devices & these devices

are being used. For example employee number 1131023 Employment end date 03/09/18 and employee number 1255033 Employment end date 26/10/2018.

| | Recommendations |
|---|---|
| **R10** | Orders for mobile phones and tablets should only be placed once a purchase order has been raised.<br>***(Priority: Medium)*** |
| **R11** | The primary record of SIM/phone allocation should be kept up-to-date to ensure former CBC employees are not shown to have SIM/Phone allocated to them after their leave date.<br>***(Priority: Medium)*** |

35. Smart phones and tablets that are returned to business transformation for disposal are sent the ICT to be 'Wiped' before being disposed. During the audit it was identified that the provider of disposal services for phones and tablets is selected by business transformation and no records are kept of the equipment that has been disposed.

| | Recommendation |
|---|---|
| **R12** | The disposal of equipment should be completed through ICT including the selection of disposal service provider and all items disposed should be recorded as such including valid receipts from disposal companies where applicable<br>***(Priority: Medium)*** |

36. Testing was undertaken on a sample of fifty mobile phone numbers that had not been active in September 2018 for calls and data to confirm if they had been active in the following two months October and November. 25 SIMs from the sample of 50 had no activity recorded for calls and/or data for the three month successive period.

| | Recommendations |
|---|---|
| **R13** | Testing showed that a number of devices had not been active over a three month consecutive period. A monitoring process needs to be devised which detects SIMs/phones which are not being used so that CBC are not paying for a service that is not used/required.<br>***(Priority: Medium)*** |
| **R14** | With the EE contract due for renewal in February 2019 consideration should be given to reviewing current practices and policies and assessing whether ICT are best placed to monitor and manage the devices and contract.<br>***(Priority: Low)*** |

Elections Tablets

37. The Elections department purchased 21 Samsung Galaxy Tab S2 9.7'' tablets including SOTI MDM (Mobile Device Management) software licence over a two year period in April 2018. This also included 1GB of data per month and training for the elections staff so they

could then train the staff who would undertake the canvassing the total amount spent was £32,197.00.

38. Testing for password access identified that the biometric password function available on the tablets is currently not being used. The passwords in place to access both the tablets and the App used when canvassing are very generic and weak.
39. Review of the internet access on the tablets identified that no restrictions are in place. Testing confirmed that restricted web pages can be accessed, for example alcohol and gambling sites are not blocked.
40. Through discussions with ICT it was identified that, ICT were not involved in the complete process when the tablets were purchased. The delivery of the tablets was made to the elections department and therefore ICT could not test the equipment was working in line with CBC policy.

| | **Recommendations** |
|---|---|
| **R15** | With ICT services returning in-house in should be ensured that future purchases of ICT equipment made by departments are either made through the ICT department or ICT are involved with the purchase including testing devices are in line with the ICT policy before they go live.<br>***Priority: Medium)*** |
| **R16** | Passwords to login to the tablets and the App are very weak and need to be reviewed. The option of using the biometric password function available on the tablet needs to be considered.<br>***(Priority: Medium)*** |
| **R17** | Internet access on the tablet needs to be reviewed to ensure restricted web pages cannot be accessed. The option of having the tablet in 'Kiosk Mode' should be explored with the supplier.<br>***(Priority: Medium)*** |

41. Through discussion with the elections officers it was identified that an acknowledgment form is not signed by the canvasser being issued with the tablet.
42. During the audit it was identified that there is no insurance cover in place for the elections tablets and that the elections tablets are not on the CBC ICT Assets insurance policy.

| | **Recommendations** |
|---|---|
| **R18** | It is recommended that an acknowledgment form is signed by the canvasser being issued with the tablet.<br>***(Priority: Low)*** |
| **R19** | Quotes should be obtained for insurance cover in case a tablet is lost, stolen or broken to see if it is cost effective to have such cover in place. The option of adding the tablets to the overall Chesterfield Borough Council ICT Assets insurance policy should be reviewed and pursued if viable.<br>***(Priority: Medium)*** |

## Internal Audit Consortium Opinion Definitions

| Assurance Level | Definition |
|---|---|
| **Substantial Assurance** | There is a sound system of controls in place, designed to achieve the system objectives. Controls are being consistently applied and risks well managed. |
| **Reasonable Assurance** | The majority of controls are in place and operating effectively, although some control improvements are required. The system should achieve its objectives. Risks are generally well managed. |
| **Limited Assurance** | Certain important controls are either not in place or not operating effectively. There is a risk that the system may not achieve its objectives. Some key risks were not well managed. |
| **Inadequate Assurance** | There are fundamental control weaknesses, leaving the system/service open to material errors or abuse and exposes the Council to significant risk. There is little assurance of achieving the desired objectives. |

## Internal Audit Report – Implementation Schedule

| Report Title: | Laptops and Other Removable Media | Report Date: | 23rd January 2019 |
|---|---|---|---|
| | | Response Due By Date: | 13th February 2019 |

| Recommendations | | Priority (High, Medium, Low) | Agreed | To be Implemented By: | | Disagreed | Further Discussion Required | Comments |
|---|---|---|---|---|---|---|---|---|
| | | | | Officer | Date | | | |
| **R1** | It is essential that the primary database held in ICT which records the distribution of laptops and other removable media devices owned by Chesterfield Borough Council is being updated in an efficient and precise manner. | **Medium** | ✓ | Fred Cornelius | 31.12.19 | | | ICT are planning the deployment of a new Cloud based Asset management tool called Snow |
| **R2** | All laptops and tablets issued should have an ICT Equipment form completed and filed in ICT. ICT Equipment transferred to a different user should have a new form completed | **Medium** | | Fred Cornelius | 31.12.19 | ✓ | | ICT are planning the deployment of a new ITSM tool, this new process will present the opportunity to replace paper based forms with digital (online) forms via a Service Catalogue |
| **R3** | A policy needs to be established to give clear guidance to management with regards to returning laptops/removable media equipment to IT when an employee leaves their post and ensuring IT are made aware if equipment is transferred to a different user. | **Medium** | ✓ | Jon Alsop | 01.06.19 | | | The new process will be brought to CMT board by ICT in May |

| Recommendations | | Priority (High, Medium, Low) | Agreed | To be Implemented By: | | Disagreed | Further Discussion Required | Comments |
|---|---|---|---|---|---|---|---|---|
| | | | | Officer | Date | | | |
| **R4** | The Information Security Guidance should be followed to report lost/stolen media to Internal Audit and the Information Assurance Manager. Lost or stolen devices should be reported to the police to increase the chance of recovery and records should be kept regarding the incident including time, date, incident description and police incident number. | **Medium** | ✓ | Jon Alsop | 01.03.19 | | | |
| **R5** | The user profiles held on the laptops should be deleted when a user is no longer employed by Chesterfield Borough Council. | **Low** | ✓ | Service Desk | 31.12.19 | | | The planned roll out of a new Windows10 image, plus Office 365 will ensure this process is adhered to. |
| **R6** | As Agreed ICT will setup a recurring service desk task to check if Sophos is updating appropriately, this will be undertaken on a monthly basis | **Low** | ✓ | Service Desk | 28.02.19 | | | This will become a reported KPI in at the ICT Operations Board |
| **R7** | ICT should insure that the insurance section are informed regarding new purchases so that the insurance schedule can be updated to guarantee adequate cover is in place for laptops owned by Chesterfield Borough Council. | **Medium** | ✓ | Fred Cornelius | 01.06.19 | | | |
| **R8** | A review of having permanent markings on laptops and other removable media should be carried | **Low** | ✓ | Jon Alsop | 01.03.19 | | | Investigate the cost of attaching an asset tag to CBC devices |

| Recommendations | | Priority (High, Medium, Low) | Agreed | To be Implemented By: | | Disagreed | Further Discussion Required | Comments |
|---|---|---|---|---|---|---|---|---|
| | | | | Officer | Date | | | |
| | out to determine if it would be beneficial. | | | | | | | |
| **R9** | ICT and Business Transformation need to agree who is responsible for the issuing and monitoring of 4G MiFi Devices in use at Chesterfield Borough Council. | **Medium** | ✓ | David Wing | 31.03.19 | | | |
| **R10** | Orders for mobile phones and tablets should only be placed once a purchase order has been raised. | **Medium** | ✓ | David Wing | 31.03.19 | | | |
| **R11** | The primary record of SIM/phone allocation should be kept up-to-date to ensure former CBC employees are not shown to have SIM/Phone allocated to them after their leave date. | **Medium** | ✓ | David Wing | 31.03.19 | | | |
| **R12** | The disposal of equipment should be completed through ICT including the selection of disposal service provider and all items disposed should be recorded as such including valid receipts from disposal companies where applicable | **Medium** | ✓ | Fred Cornelius | 28.02.19 | | | |
| **R13** | Testing showed that a number of devices had not been active over a three month consecutive period. A monitoring process needs to be devised which detects SIMs/phones which are not being | **Medium** | ✓ | EE Account manager | 28.02.19 | | | Our EE contract is set to expire as a result David Wing will be holding conversations about the opportunity for renewal and attendance of our EE account manager at Monthly Service Reviews |

| Recommendations | | Priority (High, Medium, Low) | Agreed | To be Implemented By: | | Disagreed | Further Discussion Required | Comments |
|---|---|---|---|---|---|---|---|---|
| | | | | Officer | Date | | | |
| | used so that CBC are not paying for a service that is not used/required. | | | | | | | |
| **R14** | With the EE contract due for renewal in February 2019 consideration should be given to reviewing current practices and policies and assessing weather ICT are best placed to monitor and manage the devices and contract. | **Low** | ✓ | | Complete | | | Already agreed that the process will revert back to ICT |
| **R15** | With ICT services returning in-house in should be ensured that future purchases of ICT equipment made by departments are either made through the ICT department or ICT are involved with the purchase including testing devices are in line with CBC ICT policy before they go live. | **Medium** | ✓ | | Complete | | | Already agreed that the process will revert back to ICT |
| **R16** | Passwords to login to the tablets and the App are very weak and need to be reviewed. The option of using the biometric password function available on the tablet needs to be considered. | **Medium** | ✓ | Jon Alsop | 01.05.19 | | | The Elections tablets have been reconfigured with a stronger PIN and investigations into setting login to biometric are being tested |
| **R17** | Internet access on the tablet needs to be reviewed to ensure restricted web pages cannot be accessed. The option of having the tablet in | **Medium** | ✓ | Jon Alsop | 01.05.19 | | | Jon Alsop has configured a tablet in kiosk mode, this prevents access to anything other than essential apps. It does however prevent the user |

| Recommendations | | Priority (High, Medium, Low) | Agreed | To be Implemented By: | | Disagreed | Further Discussion Required | Comments |
|---|---|---|---|---|---|---|---|---|
| | | | | Officer | Date | | | |
| | 'Kiosk Mode' should be explored with the supplier. | | | | | | | changing PIN codes and finger prints so more testing is required. |
| **R18** | It is recommended that an acknowledgment form is signed by the canvasser being issued with the tablet. | **Low** | ✓ | Jon Alsop | 01.05.19 | | | The Elections team issue the devices. Jon Alsop will speak to Julie Briggs to ensure that a robust process if followed. |
| **R19** | Quotes should be obtained for insurance cover in case a tablet is lost, stolen or broken to see if it is cost effective to have such cover in place. The option of adding the tablets to the overall Chesterfield Borough Council ICT Assets insurance policy should be reviewed and pursued if viable. | **Medium** | ✓ | Julie Briggs | 31.03.19 | | | Jon Alsop to liaise with Julie Brigss (during meeting above). |

Please tick the appropriate response (✓) and give comments for all recommendations not agreed.

| | | | |
|---|---|---|---|
| Signed Head of Service: | David Wing | Date: | 08 02 2019 |