North Somerset Council

Report to the Audit Committee

Date of Meeting: 25 April 2024

Subject of Report: ICT Mobile Devices

Town or Parish: All

Officer/Member Presenting: Mike Riggall, Information and ICT Security Manager

Key Decision: No

Reason:

The subject matter of this report will not result in incurring expenditure or making savings in excess of £500,000 and will not create significant impact in terms of its effects on communities within North Somerset.

Recommendations

That the Audit Committee notes the steps that have been taken to improve the management of mobile devices within ICT since the report was written in December 2022 and takes the opportunity to raise any ongoing matters of concern with the Information and ICT Security Manager.

1. Summary of Report

1.1 In its report *ICT Mobile Devices* of December 2022, the internal audit team identified a number of issues relating to the management of mobile technology within the council, resulting in three high level and four medium level recommendations to be actioned. This report discusses each of the recommendations presented in the audit report and details the steps that have subsequently been taken to address the concerns raised.

2. Policy

2.1 *Maintaining Security* is the second of the eight themes of the ICT Strategy, the aim of which states:

> The residents of North Somerset must have confidence in our ability to ensure the integrity, availability and confidentiality of the personal information we process. We therefore undertake to have robust systems and processes in place to protect information from inappropriate disclosure.

3. Details

3.1 Internal audit assessed the framework of internal control at Level 2, Limited Assurance. Specifically, the executive summary highlighted that *records are not held of lost or stolen devices and therefore we cannot provide assurance that the security*

risk of all incidents has been properly accounted for. The Council is running versions of the Windows 10 operating system which are not supported. This increases the risk of malicious actors exploiting vulnerabilities in the operating system. Further, an asset register is in place but details of mobile assets, as well as the details of the user, are not always updated.

3.2 In the interests of brevity, the full findings of the audit report will not be repeated in this update[AW1][MR2][AW3]; the reader is instead referred to the report to understand the weaknesses identified and the management actions agreed. The following paragraphs will provide detail of the activities that have taken place since December 2022 in response to the recommendations.

Operating System (H1)

3.3 **Recommendation:** *ICT services should update all devices to ensure that they are running a supported version of the operating system. This should be reviewed and actioned on a monthly basis using the ICT Exception Reports.*

3.4 The report identified that the council's estate of thin client laptops was built on a version of Windows 10 that was no longer supported by Microsoft. Whilst to use such an unsupported operating system contravenes the council's information security policy, there were two mitigating factors in this instance that were not reflected in the audit report.

3.5 The operating system identified was the host operating system of the machine, the sole purpose of which is to allow the laptop to start and connect the user of the machine to the virtual desktop they use on a daily basis. There is no flow of information between the host operating system and the virtual desktop in these circumstances and at no time was the council's internal IT estate threatened.

3.6 The council's security policy continues to allow for an NSC virtual desktop to be run from a web client or a desktop client installed on a personal computer, i.e. one not owned or managed by the organisation. In these circumstances, the council has no control over the operating system being used on that personal computer however it has other protections in place to mitigate the risks associated with compromise of the host device such as access control policies and multi-factor authentication.

3.7 The virtual desktops highlighted in the report were deployed between February and July 2020 in response to the need to mobilise the workforce to allow services to continue to be delivered during the pandemic. No means was designed to update the operating system on the host machine as the devices were not under central control.

3.8 Subsequent to the audit report, all thin client laptops have been recalled and swapped with reconfigured devices that now automatically join a secure management network when they start through which updates can be deployed, and if necessary, forced into use. The standard operating system currently in use across all machines in the estate is Windows 10 version 22H2 which will be supported by Microsoft until 14 October 2025.

3.9 The council's IT team works hard to ensure that vulnerabilities are identified and patched according to a patching policy compliant with standard frameworks such as Cyber Essentials and the Cabinet Office's PSN code of connection. This work includes a monthly patching report that scans the entire estate to identify weaknesses such as patches that have been released by vendors but have not yet been applied, and unsupported hardware, software and firmware. The latest patching

report shows that 1780 of 1787 mobile devices are currently running the latest version of Windows 10, and the outstanding 7 are pending upgrades.

3.10 **Recommendation:** *The end of version support is clearly published by Microsoft/ Apple well in advance of the end of support so a process should be put in place that ensures devices are upgraded to a supported version timely.*

3.11 The Security-as-a-Service function provided by Agilisys maintains oversight of the lifecycle of firmware, software and operating systems in use across the council and feeds into pipeline projects that are created within the Project Management Office to ensure that adequate preparations are made.

3.12 A Windows 11 upgrade programme has already been commissioned and will see the removal of Windows 10 from the estate well in advance of the end of Microsoft support in October 2025.

Asset Register (H2)

3.13 **Recommendation:** *ICT Services should ensure that an officer is assigned responsibility for the upkeep of the Asset Register.*

3.14 Subsequent to the publication of the audit report, the council has introduced the new role of ICT Asset and Information Security Officer and this post was filled on a full-time basis in October 2023. One of the responsibilities for this officer is to monitor the asset register on a regular basis to ensure that accurate information is being maintained.

3.15 **Recommendation:** *The Asset Register should be reviewed on a regular basis to ensure that all fields are populated including the user and location of the device.*

3.16 We no longer look solely within the asset register for an owner of a device as this may vary on a day-to-day basis. The information in the asset register is supplemented by that from other means of obtaining tracking information such as the Aternity monitoring system used to monitor performance of desktops across the estate that can associate a user of desktop with the hardware device on which the desktop is running.

3.17 **Recommendation:** *ICT Services should define how they will monitor and record those ICT devices that are not recognised by the MDM system (polled), such as monitors.*

3.18 We acknowledge that there is a lack of accurate asset information relating to monitors that were taken by officers to enable homeworking during the pandemic. Line managers were tasked with maintaining records of people within their teams who had taken monitors for use at home, however, inevitably, this information was not reliably captured and as a result we are currently unable to account for many monitors. Whilst this does not represent good asset management control, it must be considered in the context of the need to mobilise the workforce urgently and maintain statutory services during a time of national crisis.

3.19 As part of the office refurbishment programme, 350 new monitors have been procured for use in the Town Hall and all of these devices will appear in the asset

register together with their deployed locations and will be verified by the ICT Assets and Information Security Officer.

3.20 **Recommendation:** *The Leavers process should be amended to ensure that it covers all mobile ICT devices, including monitors.*

3.21 As recommended in the report, the leaver's form on the self-service IT portal has been updated to allow managers to identify any equipment used for homeworking such as monitors that need to be returned.

Lost and Stolen Devices (H3)

3.22 **Recommendation:** *Procedures should be written and implemented for ICT devices that are lost or stolen.*

3.23 A self-service form has now been developed through which officers should report devices which have been lost or stolen. Linked to the form are tasks and activities for IT teams to perform which will be triggered automatically such as wiping of mobile devices that are under MDM control. The service desk system provides the audit trail for the completion of these activities.

3.24 The procedure for reporting lost and stolen devices has been added to the Personal Information Security Policy which features in the newly revised security policy framework which is shortly to be issued.

3.25 **Recommendation:** *ICT should maintain a record of all lost or stolen devices together with the action taken to prevent data loss.*

3.26 As indicated in 3.23 above, the audit trail recommended is created within the Service Desk system from the activities that are triggered by the initial call raised.

Allocation of Devices (M1)

3.27 **Recommendation**: *A policy should be written to ensure that mobile devices are allocated to staff based on their job description and their role.*

3.28 The allocation of technology to individuals is largely driven by the workstyle assigned to each officer. Detailed information on this is published through the Accommodation Strategy Programme pages on the intranet.

3.29 Whilst the new ways of working describe a 'standard offer' of technology for each of the four workstyles, some variations to the offer are inevitable. Not every officer with a workstyle of *mobile worker* for example requires a mobile telephone and each service manager will therefore determine whether one is appropriate depending on the individual circumstances. The ongoing cost of mobile phone contracts are funded from service budgets and hence decisions of affordability must be considered by individual budget managers before the device can be allocated.

3.30 The recommendations of the report are fulfilled through a combination of the council's Hybrid Working Policy available on the intranet and the Asset Management Policy which has been updated to reflect the new ways of working introduced through the Accommodation Programme and confirms the approach outlined above.

Policies and Procedures (M2)

3.31 **Recommendation:** *ICT policies and procedures should be reviewed and updated to ensure that they consider:*

- staff homeworking arrangements.

- reference those ICT policies that are related.
- clearly identify the owner of the policy.
- Clearly identify the date that the policy was last reviewed.

3.32 Whilst the re-write of the council's information security policy framework is still in the process of being completed however some elements referred to in the audit report such as the remote working and hybrid working policies have been published to all members of staff.

3.33 As we continue to work through the revision of the policy framework we are ensuring that all policies are marked as being owned by the ICT Architecture Board and are routed through the board for approval and adoption as they are finalised. Review dates being set for an initial period of 12 months following introduction with a view to this being subsequently extended to two years. Policy reviews are entered onto the ICTAB forward plan.

Mobile Data Usage (M3)

3.34 **Recommendation:** *The use of council mobile data whilst at home should be clearly defined in the homeworking policy to ensure that staff that have either a mobile dongle or council issued mobile phone, use their own broadband connection, whilst at home.*

3.35 The use of council mobile data whilst working from home is clearly identified in the Hybrid Working Policy,

When working from home you will need to use your own broadband facilities and meet any increased energy costs – you won't be reimbursed for doing so.

3.36 **Recommendation:** *The council should monitor high usage (defined as over 10gb) per month to identify the reasons for the high usage. Staff that are using the data at home due to lack of broadband connectivity should be reminded that they should either return to the office or should be paying for a mobile data contract.*

3.37 Monthly mobile phone bills are analysed by the Programme Management Officer and items of excessive spend are investigated with the relevant officer, primarily with a view to ensuring that the user is on the correct mobile phone data tariff. Additionally, the Head of Support Services and the Information and ICT Security Manager both receive a notification whenever an officer reaches 80% of their monthly data allocation, and again when reaching 100%.

3.38 Whilst individual mobile data contracts have allowances, the council suffers no additional cost over the £5 per month basic charge should an individual contract exceed that allowance. The council suffers additional costs only in the circumstances where the collective monthly usage exceeds the combined data allowance of all 2024 devices, which is 2,706 GB (figures are correct as at 12 March 2024).

ICT Assets Returned to ICT (M4)

3.39 **Recommendation**: *The Leavers Form should be updated to make It clear that all ICT equipment must be returned to ICT once a user leaves.*

3.40 The leaver's form has now been updated in line with the report recommendations and contains a header which states,

> *It is NSC policy that ALL assets i.e. laptops, mobiles, iPads etc are to be returned to ICT for all leavers. IT will raise the relevant form in the Managers name for the return of all devices and these must be returned within 5 working*

days of leavers date. Managers are responsible for returning all IT equipment to Field Services. If the laptop is to be used by another user, the Field services team will need to prepare it for the new user (rebuild, ensure latest updates, add any required software)

3.41 We have processes in place to identify and isolate IT equipment that has not been seen on the network for a period of longer than 60 days. This information is becoming increasingly understood by service managers which, alongside the fact that end user IT equipment like laptops and tablets are now funded centrally, means that there is no benefit to services holding on to equipment previously assigned to officers that have left the organisation.

3.42 **Recommendation:** *As part of the off-boarding process, ICT Services should implement a process to chase unreturned devices and update the Asset Register.*

3.43 The ICT Asset and Information Security Officer will identify assets that have not been returned, follow up with line managers and HR and ensure that the asset register is update appropriately.

4. Consultation

4.1 Not applicable to this report.

5. Financial Implications

5.1 Not applicable to this report.

Costs

5.2 Not applicable to this report.

Funding

5.3 Not applicable to this report.

6. Legal Powers and Implications

6.1 Not applicable to this report.

7. Climate Change and Environmental Implications

7.1 Where assets have reached the end of their life, they are disposed of ethically and in accordance with Waste Electrical and Electronic Equipment (WEEE) regulations.

7.2 Redistribution of IT hardware creates complications for the council in terms of the costs associated with ensuring that it is free from NSC branding and, more importantly, does not contain any council information. Where equipment is otherwise suitable for being redistributed, permanent storage drives such as hard disks and SSD drives will first be removed and destroyed.

8. Risk Management

8.1 The audit report clearly identifies risks to the council and suitable mitigations have been presented [AW4]in section 3 of this report in response to the recommendations made.

8.2 At a wider level, the council maintains a separate risk register for all IT services within which cyber risks are prevalent and the risk register is reviewed on a monthly basis.

8.3 The potential for disruption that relates to cyber attack appears as a risk on the corporate risk register and is managed in accordance with the risk management strategy.

9. Equality Implications

9.1 Not applicable to this report.

10. Corporate Implications

10.1 The audit report identifies the wider corporate implications and these have been addressed throughout this document.

11. Options Considered

Not applicable to this report.

Author:

Mike Riggall, Information and ICT Security Manager

Background Papers:

Audit Report *ICT - Mobile Devices*, December 2022
ICT Strategy 2021-24
Hybrid Working Policy
Information Security Policy Framework