NORTH AYRSHIRE COUNCIL

12 January 2021

Audit and Scrutiny Committee

Title:	**Internal Audit Reports issued**
Purpose:	To inform the Committee of the findings of Internal Audit work completed during November and December 2020.
Recommendation:	That the Committee considers the outcomes from the Internal Audit work completed.

1. Executive Summary

1.1 The Council's local Code of Corporate Governance requires effective arrangements to be put in place for the objective review of risk management and internal control. Internal Audit is an important element in this framework as it reviews internal controls and offers Elected Members and officers an objective and independent appraisal of how effectively resources are being managed.

1.2 The remit of the Audit and Scrutiny Committee includes the monitoring of Internal Audit activity. The submission and consideration of regular reports assists the Committee in fulfilling this remit.

2. Background

2.1 This report provides information on Internal Audit work completed during November and December 2020. Internal control reviews have been completed in respect of the areas detailed in Appendix 1 to this report. The aim of these reviews is to provide assurance that the internal control framework within the areas examined is appropriate and operating effectively.

2.2 The findings from each audit assignment have been notified in writing to the Chief Executive, the Section 95 Officer and the relevant Executive Director and Head of Service on the completion of each assignment. Where appropriate, this has included an action plan with recommendations for improving internal control. Appendix 1 includes the report and action plan from each audit.

2.3 The findings from one audit assignment on remote access controls in the education network are detailed at Appendix 1 to this report.

2.4 Only limited assurance was obtained. There are particular concerns over unencrypted laptops being used for remote working, iPads not being properly managed, weak network password controls and Sophos anti-virus notifications not being sent to the school ICT Technicians to action.

3. Proposals

3.1 It is proposed that the Committee considers the outcomes from the Internal Audit work completed during November and December 2020.

4. Implications/Socio-economic Duty

Financial

4.1 None.

Human Resources

4.2 None.

Legal

4.3 None.

Equality/Socio-economic

4.4 None.

Environmental and Sustainability

4.5 None.

Key Priorities

4.6 The work of Internal Audit helps to support the efficient delivery of the strategic priorities within the Council Plan 2019-2024.

Community Wealth Building

4.7 None.

5. Consultation

5.1 The relevant Services are consulted on Internal Audit findings during each audit assignment.

Mark Boyd
Head of Finance

For further information please contact **Paul Doak, Senior Manager (Audit, Fraud, Safety and Insurance),** on **01294-324561**.

Background Papers
None.

REMOTE ACCESS CONTROLS AROUND THE EDUCATION NETWORK

1 Background

1.1 The Council has an Education network for teaching staff and pupils, which is separate from the Corporate network.

1.2 Direct Access is used to provide remote access to users in the schools and wireless networks have also been set up in the schools.

1.3 System Centre is used by IT Services to maintain a list of all Microsoft based devices on the Education network. The schools should also maintain an inventory record of all IT devices.

1.4 Airwatch is the mobile device management system which is used to control all NAC purchased iPads. This allows all iPads to be set up uniformly across the schools. Some are set up with staff access and some are set up with pupil access.

1.5 All laptops should be encrypted with Bitlocker encryption and installed with Sophos anti-virus protection.

2 Objectives and Scope

2.1 The main objectives of this audit were to ensure that:

- teaching staff have been provided with appropriate IT policies and procedures and ICT Technicians have corporate procedures to follow for carrying out key functions.
- only Council authenticated devices are used for Direct Access, laptops are encrypted, iPads are appropriately managed and controlled and appropriate Wi-Fi settings are in place.
- strong network password controls are in place and there are appropriate processes in place for setting up new teaching staff with relevant IT access and promptly removing leavers.
- there are proper controls around the procurement and setting up of new mobile devices and up-to-date inventories are maintained by the schools.
- all mobile devices are protected with up-to-date anti-virus software, ICT Technicians are notified, and act on these alerts and an appropriate patch management process is in place.

2.2 The scope of the audit covered remote access controls around the Education network to allow agile working. The audit was restricted to employees only and excluded pupils’ access.

3 Findings

Governance and IT Policies and Procedures

3.1 No additional remote access or agile working policies and procedures are issued to staff in the schools. Teaching staff are expected to adhere to the corporate Acceptable Computer Use Policy. Teaching staff have to manually sign up to this policy as Education do not have software to electronically issue such policies and provide an audit trail of the staff that have signed up. Education should consider purchasing compliance software such as Meta Compliance which is used for the Corporate network to sign up to such policies. **(action a)**

3.2 There is no documented formal Service Level Agreement between IT Services and Education to ensure clear roles and responsibilities are defined, agreed and allocated for the provision of IT services in the schools. **(action b)**

3.3 There are no standard procedures provided by IT Services covering key functions/tasks carried out by the ICT Technicians, to ensure a standard approach is taken across all the schools. IT Services and Education should work together to define key functions and produce standard procedures. **(action c)**

Mobile Device Authentication and Device Security Settings

3.4 Internal Audit requested a usage report on Direct Access but IT Services advised the auditing function had not been switched on. It was switched on during the course of the audit although, due to lockdown, usage reports were not provided as evidence.

3.5 The auditor compared the list of Direct Access devices for primary and secondary schools to the MBAM (Microsoft Bitlocker Administration and Monitoring) database which lists encrypted devices, and 42 (out of 1,533) direct access devices could not be found Action is being taken by IT Services to rectify these 42 to ensure all are either encrypted or disabled in Active Directory.

3.6 The auditor compared the list of all iPads on Airwatch, the mobile device management system, to the secondary schools' inventory records of the iPads they hold. There are major discrepancies in this comparison. There are 481 iPads on the schools' inventory records that are not on the Airwatch report. IT Services advised that when Airwatch was introduced all existing iPads should have been provided to IT to set them up on Airwatch. There is a risk that these iPads have not been set up on Airwatch and are therefore not being properly managed in line with Council policy. If they are not being managed, they are not being controlled via the Councils corporate policies and settings provided by Airwatch. **(action d)**

3.7 The auditor tested the use of USB data storage devices in the secondary schools. The following was noted:

- USB devices are not recorded on any of the inventory records provided by the secondary schools – this is a requirement of the ICT Acceptable Use Policy.
- There is discrepancy between the ICT Acceptable Use Policy and the IT Standards Product List regarding who can purchase encrypted USB devices. One states they should be purchased via IT Services and the other states they can be purchased directly by employees. **(action e)**
- One of the secondary schools confirmed unencrypted USB devices are being used.
- There is no technology in place to provide notification of unauthorised USBs being connected to the schools' network, so there is no current way to determine the scale of unauthorised and unencrypted USB devices being used on the schools' network. **(action f)**

Network Access Controls

3.8 Password controls for network logons are weak and are not in line with best practice. There is no requirement to use a mix of special characters, numbers, uppercase, lowercase etc or to change the password periodically or get locked out after a specified number of failed login attempts. **(action g)**

3.9 The auditor was advised by 2 of the ICT Technicians that cloning is still being used in the secondary schools when setting up a new teacher's IT access. **(action h)**

3.10 It was noted that not all the secondary schools have a robust process in place for promptly removing IT access for teaching staff that have left the school. IT Services confirmed that they have a process in place to move accounts not used for 250 days to a stale users container which disables the account. **(action i)**

Procurement and Recording of Mobile Devices

3.11 The information recorded on the IT Inventories maintained by the secondary schools varies. In all cases, the serial number is recorded but only 1 school records the computer name. **(action j)**

3.12 The auditor compared each secondary school's list of laptops to the System Centre report provided by IT Services, using the serial number to match the 2 sets of data. This comparison showed major discrepancies between the laptops as per the schools' inventory and the laptops as per the System Centre report. Some of the ICT Technicians advised that their inventory records are not up-to-date, and this is supported by these results, as not all laptops on the schools' inventory are still being used. **(action k)**

Anti-Virus Software and Patch Management Arrangements

3.13 Sophos anti-virus is installed on all school devices, but it was noted that 2 of the ICT Technicians are not receiving any notifications provided by this software, to allow them to investigate and fix the problem. Internal Audit advised IT Services to rectify this during the audit.

3.14 IT Services confirmed there is a current issue with the email alerts for Sophos which is the anti-virus software for end user devices. IT Services are working with the company to resolve this issue.

3.15 IT Services confirmed that the ICT Technicians have been added to the group "Sophos console administrators" meaning they can do anything from a Sophos perspective. **(action l)**

3.16 IT Services confirmed that there was a temporary pause on patching under the lockdown conditions and response efforts. IT Services restarted updates to Education in July and are playing catch-up now the schools are back. IT Services aim to complete the catch-up so that updates are following the normal cycle.

4 Internal Audit Opinion

4.1 Overall, limited assurance was obtained with regard to remote access controls around the Education network to allow agile working. There are particular concerns over unencrypted laptops being used for remote working, iPads not being properly managed, weak network password controls and Sophos anti-virus notifications not being sent to the ICT Technicians to action.

Definitions of Assurance Levels:

Substantial	The framework of governance, risk management and control is adequate and effective.
Reasonable	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
None	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

NB The level of assurance given is at the discretion of Internal Audit.

KEY FINDINGS AND ACTION PLAN
REMOTE ACCESS CONTROLS AROUND THE EDUCATION NETWORK

Action	a
Finding	Teaching staff have to manually sign up to the ICT Acceptable Use Policy as Education do not have software to allow teaching staff to electronically sign up to such policies which would provide a full audit trail.
Action Description	Education should consider purchasing software to allow teaching staff to electronically sign up to the ICT Acceptable Use Policy.
Risk	Staff may not have agreed to comply with the ICT Acceptable Use Policy.
Priority (1, 2, 3)	3
Paragraph Reference	3.1
Managed by	Andrew McClelland, Head of Service (Education)
Assigned to	Andrew McClelland, Head of Service (Education)
Due Date	30/04/2021
Management Comment	An electronic solution to ensuring that all staff sign up to the ICT acceptable use policy will be introduced across the Education service. This may include the purchase of additional software in conjunction with IT Services.

Action	b
Finding	There is no documented formal Service Level Agreement between IT Services and Education to ensure clear roles and responsibilities are defined, agreed and allocated.
Action Description	IT Services and Education should produce a documented formal Service Level Agreement to ensure clear roles and responsibilities are defined, agreed and allocated for the provision of IT in the schools.
Risk	The roles and responsibilities of both parties have not been defined and agreed.
Priority (1, 2, 3)	2
Paragraph Reference	3.2
Managed by	Andrew McClelland, Head of Service (Education), Fiona Walker, Head of Service (People and ICT)
Assigned to	IT Services: Brendan Quigley, Senior Manager IT; and Carolann McGill, Team Manager Customer Experience Education: Andrew McClelland Head of Service (Education); Rosslyn Lee, Digital Skills Co-ordinator
Due Date	31/03/21
Management Comment	Education and IT Services to draft and agree a "working together" document. This document will be high level and cover roles and responsibilities to ensure they are clearly defined, agreed and allocated for the provision of IT in schools. The standard procedures (action c) would be the more detailed processes that would sit behind this.

Action	c
Finding	There are no standard procedures provided by IT Services covering key functions/tasks carried out by the ICT Technicians to ensure a standard approach is taken across all the schools.
Action Description	IT Services and Education should work together to define key functions and produce standard procedures to be followed.
Risk	Key tasks are not being carried out.
Priority (1, 2, 3)	2
Paragraph Reference	3.3
Managed by	Andrew McClelland, Head of Service (Education), Fiona Walker, Head of Service (People and ICT)
Assigned to	IT Services: Brendan Quigley, Senior Manager IT; Carolann McGill, Team Manager Customer Experience; James McNeil, Team Manager IT Operations Education: Lynn Taylor, Senior Manager Education; Rosslyn Lee, Digital Skills Co-ordinator
Due Date	31/03/21
Management Comment	A working group will be set up to agree and define the key functions, produce standard procedures to be followed and ensure standard approaches are taken across all schools and that ICT Technicians align with corporate ICT policies and procedures.

Action	d
Finding	There are 481 iPads on the schools' inventory records that are not on the Airwatch report.
Action Description	The ICT Technicians should reconcile their inventory records with the Airwatch report and identify any NAC purchased iPads not on Airwatch and pass to IT to ensure they are added to this console, to allow them to be properly managed.
Risk	iPads have not been set up on Airwatch and are therefore not being properly managed in line with Council policy.
Priority (1, 2, 3)	1
Paragraph Reference	3.6
Managed by	Andrew McClelland, Head of Service (Education)
Assigned to	Lynn Taylor, Senior Manager Education
Due Date	31/01/21
Management Comment	Education to review and provide IT with details of iPads to be added to Airwatch (include as part of ICT Monthly meeting). See action c.

Action	e
Finding	There is discrepancy between the ICT Acceptable Use Policy and the IT Standards Product List regarding who can purchase encrypted USB devices. One states they should be purchased via IT Services and the other states they can be purchased directly by employees.
Action Description	IT Services should clarify which process is correct and update one of the documents accordingly.
Risk	Inconsistent advice provided to employees.
Priority (1, 2, 3)	2
Paragraph Reference	3.7

Managed by	Fiona Walker, Head of Service (People and ICT)
Assigned to	Carolann McGill, Team Manager Customer Experience; Derek Nelson, ICT & Cyber Security Architect
Due Date	28/02/2021
Management Comment	IT Services will ensure that both documents are aligned.

Action	f
Finding	USB devices are not recorded on the schools' inventory records, one of the secondary schools confirmed the use of unencrypted USB devices and there is no software to identify unauthorised USB devices being plugged in to the network.
Action Description	Education should remind the ICT Technicians to record USB devices on the IT inventory records and remind teaching staff to only use encrypted USB devices. Consideration should also be given to purchasing software that will identify unauthorised USB devices being plugged in to the network.
Risk	Unencrypted USB devices are being used to transmit sensitive data, USB devices are not properly managed and can lead to difficulty in determining if IT assets have been lost.
Priority (1, 2, 3)	1
Paragraph Reference	3.7
Managed by	Andrew McClelland, Head of Service (Education)
Assigned to	Andrew McClelland, Head of Service (Education)
Due Date	31/01/21
Management Comment	Education will update inventory records and analyse usage of USB devices. Andrew McClelland will write to schools with regard to this issue, advising to make maximum use of cloud storage and minimise the use of USBs.

Action	g
Finding	Password controls for network logons are weak and are not in line with best practice. There is no requirement to use a mix of special characters, numbers, uppercase, lowercase etc or to change the password periodically or get locked out after a specified number of failed login attempts.
Action Description	Password controls should be amended to be in line with best practice guidance.
Risk	Increased vulnerability to hacking or other forms of cyber-attack, which could lead to data breach or inability to undertake duties.
Priority (1, 2, 3)	1
Paragraph Reference	3.8
Managed by	Andrew McClelland, Head of Service (Education), Fiona Walker, Head of Service (People and ICT)
Assigned to	IT Services: James McNeil, Team Manager IT Operations Education: Rosslyn Lee, Digital Skills Co-ordinator
Due Date	30/04/21
Management Comment	IT Services will add the fine-grained password management capability to the Education Active Directory (AD). IT Services will then work with Education to plan the rollout of fine-grained password management and password complexity rules. The current Education AD solution does not support fine grained password policies i.e. different policies for different groups of

	people. This upgrade is required to facilitate distinct password policies are required for teachers, secondary students and primary students.

Action	h
Finding	The auditor was advised by 2 of the ICT Technicians that cloning is still being used when setting up a new teacher's IT access.
Action Description	Cloning should no longer be used to minimise the risk of teaching staff being given unnecessary access to potentially sensitive data.
Risk	Teaching staff are given unnecessary access to potentially sensitive data.
Priority (1, 2, 3)	2
Paragraph Reference	3.9
Managed by	Andrew McClelland, Head of Service (Education)
Assigned to	Andrew McClelland, Head of Service (Education)
Due Date	28/02/21
Management Comment	Education will ensure process of cloning is stopped within schools and that each user is newly created and access rights applied manually (to include in ICT Technician monthly meeting and produce communication guidance). Covered in action c.

Action	i
Finding	It was noted that not all the secondary schools have a robust process in place for promptly removing IT access for teaching staff that have left the school. IT Services confirmed that they have a process in place to move accounts not used for 250 days to a stale users container which disables the account.
Action Description	A robust process should be put in place to ensure that IT access is removed by the ICT Technician promptly when teaching staff leave. In addition, Education should consult with IT Services to improve the current IT Services process as 250 days is excessive.
Risk	Former employees have inappropriate access to data.
Priority (1, 2, 3)	2
Paragraph Reference	3.10
Managed by	Andrew McClelland, Head of Service (Education), Fiona Walker, Head of Service (People and ICT)
Assigned to	IT Services: James McNeil, Team Manager IT Operations Education: Lynn Taylor, Senior Manager Education
Due Date	28/02/21
Management Comment	Policy will be altered by IT Services to ensure accounts are moved to stale after 90 days. Education will introduce a robust process for removing staff IT access when they leave service. Education will produce a 'leavers' form to incorporate IT hardware/software return and to inform school Technician (this will be documented as part of the procedures at action c).

Action	j
Finding	The information recorded on the IT Inventories maintained by the schools varies. In all cases the serial number is recorded but only 1 school records the computer name.
Action Description	Schools should be reminded of the information that should be recorded on the inventory records and this should include the computer name.
Risk	Non-compliance with inventory procedures and not all relevant information is recorded.
Priority (1, 2, 3)	3
Paragraph Reference	3.11
Managed by	Andrew McClelland, Head of Service (Education)
Assigned to	Lynn Taylor, Senior Manager Education
Due Date	28/02/21
Management Comment	Education will ensure an IT Inventory is maintained by all schools using standard inventory template provided by IT. IT Services will provide inventory reports once or twice a year. The new process will be documented as part of action c.

Action	k
Finding	The auditor compared each school's list of laptops to the System Centre report provided by IT Services using the serial number to match the 2 sets of data. This comparison showed major discrepancies between the laptops as per the schools' inventory and the laptops as per the System Centre report. Some of the ICT Technicians advised that their inventory records are not up-to-date and this is supported by these results as not all laptops on the schools' inventory are still being used.
Action Description	School ICT technicians should undertake a review of the laptops on their inventory in comparison to the records held on System Centre and ensure that the inventories are up-to-date.
Risk	Lost or stolen laptops are not identified
Priority (1, 2, 3)	1
Paragraph Reference	3.12
Managed by	Andrew McClelland, Head of Service (Education)
Assigned to	Lynn Taylor, Senior Manager Education
Due Date	28/02/21
Management Comment	Education will undertake a review of laptop inventory in comparison to records on System Centre to ensure inventories are up to date. Technicians will include a process for frequently updating inventories throughout the year rather than once a year. This will be documented as part of the procedures noted at action c. IT agreed to provide the Technicians with reports from System Centre and Airwatch as starting points, to allow them to compare their records and update these as appropriate.

Action	I
Finding	IT Services confirmed that the ICT Technicians have been added to the group “Sophos console administrators” meaning they can do anything from a Sophos perspective.
Action Description	IT Services should review the ICT Technicians’ access and remove the administrator’s role if this is not required to ensure only relevant staff have this level of access.
Risk	ICT administrators could change policy that has been set corporately by IT Services without IT Services being aware of changes made.
Priority (1, 2, 3)	2
Paragraph Reference	3.15
Managed by	Fiona Walker, Head of Service (People and ICT)
Assigned to	James McNeil, Team Manager IT Operations
Due Date	28/02/2021
Management Comment	IT Services will review ICT Technician rights and ensure that only rights appropriate to the ICT Technician role are implemented i.e. “just enough admin” rights.

Priority Key used in Action Plan

1 (High)	Control weakness where there is a material impact on the achievement of the control objectives, generally requiring prompt attention.
2 (Medium)	Control weakness which needs to be rectified, but where there is no material impact on the achievement of the control objectives.
3 (Low)	Minor weakness or points for improvement.