

---

# NORTH AYRSHIRE COUNCIL

1 June 2021

## Audit and Scrutiny Committee

---

**Title:** Remote Access Controls - Education Network – Internal Audit Progress Update

**Purpose:** To provide an update on:

- Internal Audit Report Management Action Plan, and
- Update on the Digital Strategy Review.

**Recommendation:** It is recommended that the Committee notes the progress made in the execution of the Internal Audit Management Action Plan and the progress made on the Digital Strategy Review.

---

### 1. Executive Summary

- 1.1 The remit of Internal Audit includes the monitoring of internal controls of how effectively resources are being managed. An internal audit began in January 2020 in relation to the Remote Access Controls around the Education Network. The audit was delayed due to the pandemic and the report was issued in November 2020. It was presented to the Audit & Scrutiny Committee on 12 January 2021. The Committee noted progress and requested a further update on the execution of the management actions detailed in the Audit report. The Internal Audit Report is attached at Appendix 1.
- 1.2 Since the beginning of the year, a Senior Manager, Education has been appointed to lead a Digital Strategy Review in Education. An ICT Technician Coordinator has also been appointed to have an overview of all systems and procedures across schools.
- 1.3 A workstream of the Digital Strategy Board has been set up which is led by the Senior Manager, Digital Strategy. The group has senior officer representation from both education and ICT services and also includes the auditor who carried out the internal audit.
- 1.4 The priority for the group was to address the actions raised in the internal audit. However, the work of the group will continue to focus on developing new and improved processes and systems that align with the output of the wider digital review. The group will focus on ensuring compliance with security protocols and will involve input from ICT technicians in secondary schools and ICT Services, who provide the ICT technician service across primary schools.

1.5 The internal audit reported a total of 12 management actions to be addressed. Nine of these actions are now closed, with the remaining 3 in progress with a plan and closure date agreed.

## 2. Background

2.1 The Digital Strategy Review will focus on the following key areas:

- Developing the skills and confidence of educators in the appropriate and effective use of digital technology to support learning and teaching.
- Improving access to digital technology for all learners.
- Ensuring that digital technology is a central consideration in all areas of curriculum and assessment delivery.
- Empowering leaders of change to drive innovation and investment in digital technology for teaching and learning.
- Further development of the ICT Working Group priorities to support schools.

2.2 The purpose of the Board will be to ensure progress across all of the areas identified above with the clear objective to develop an innovative, forward looking Digital Strategy.

2.3 The workstream group was set up at the end of January 2021 and an update on each of the actions and progress made are outlined below:

<b>Action a)</b>	<b>Status:</b>	<b>Closed</b>
------------------	----------------	---------------

Audit Action: Education should consider purchasing compliance software such as Meta Compliance which is used for the Corporate network to sign up to such policies as Accessible Computer Use Policy.

Current position: Meta Compliance has been purchased and will be utilised to enable school-based staff to sign up to the Accessible Computer Use Policy, as well as other relevant policies. It will be an effective communication tool for important ICT security information and updates.

<b>Action b)</b>	<b>Status:</b>	<b>Closed</b>
------------------	----------------	---------------

Audit Action: There is no documented formal Service Level Agreement between Education and ICT Services.

Current position: Education and ICT have worked collaboratively to produce a Working Together Agreement which been signed off by Heads of Service across both services. (Appendix 3)

<b>Action c)</b>	<b>Status:</b>	<b>Closed</b>
------------------	----------------	---------------

Audit Action: There are no standard procedures provided by ICT Services covering key functions/tasks carried out by the ICT Technicians, to ensure a standard approach is taken across all the schools.

Current Position: A set of standard procedures have been developed and communicated to all schools and ICT Technicians, which are attached at Appendix 2. These include:

- Process for New Start Employees
- Setting-up a New Device
- Inventory
- Process for employees who leave the organisation
- Disposal of Equipment
- Anti-virus Software Procedure
- USB Pen Drives Procedure

**Action d)** **Status:** **Open**

Audit Action: The ICT Technicians should reconcile their inventory records with the Airwatch report and identify any NAC purchased iPads not on Airwatch and pass to ICT to ensure they are added to this console to allow them to be properly managed.

Current position: The completion of this action has been delayed due to the focus on ensuring staff, children and young people had suitable and effective access to ICT whilst working from home and home schooling.

The group have revised the completion date of this action to 31 May 2021. This will allow staff, children and young people to return iPads to the ICT Technicians now that schools have returned. A communication has been sent to Head Teachers requesting that all iPads be returned to the ICT Technicians by 14<sup>th</sup> May in order that they can be included on Airwatch where appropriate and added to the inventory.

**Action e)** **Status:** **Closed**

Audit Action: 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 ICT Services and the other states they can be purchased directly by employees.

Current position: The ICT Acceptable Use Policy has been updated to reflect the IT Standards Product List information. The updated ICT Acceptable Use Policy can be accessed on Connects.

**Action f)** **Status:** **Closed**

Audit Action: Education should remind the ICT Technicians to record USB devices on the 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.

Current position: A communication was sent to Head Teachers and ICT Technicians on 24 February 2021 providing information on the use of USB devices. The Use of USB Pen Drives Procedure has also been developed and is included in the procedures pack sent to Head Teachers and ICT Technicians.

<b>Action g)</b>	<b>Status:</b>	<b>Open</b>
------------------	----------------	-------------

Audit Action: Password controls for network logins 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.

Current position: The group have made the decision to delay this action until August 2021 due to the recent return of schools and the school holiday period coming up at the end of June. The change of login settings will take place w/c 23 August 2021 and will be completed over a five-week period.

<b>Action h)</b>	<b>Status:</b>	<b>Closed</b>
------------------	----------------	---------------

Audit Action: The Audit highlighted that cloning was still taking place when setting up new teachers' ICT access. The action advised that cloning should no longer be used to minimise the risk of teaching staff being given unnecessary access to potentially sensitive data.

Current position: A guidance document has been created with instructions on how to create each new user and has been circulated to all Head Teachers and ICT Technicians. A receipt and adherence confirmation has been returned by each Head Teacher. A procedure is also included in the pack sent to Head Teacher and ICT Technicians.

<b>Action i)</b>	<b>Status:</b>	<b>Closed</b>
------------------	----------------	---------------

Audit Action: The audit highlighted 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. Therefore, 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 process as 250 days is excessive.

Current position: A Leavers procedure has been developed and includes a Leavers Form to ensure the return of ICT equipment prior to staff leaving. The procedure has been sent to all Head Teachers and ICT Technicians as part of the procedure pack. ICT have revised the process for disabling accounts not being used from 250 days to 90 days and advised Head Teachers and ICT Technicians as part of a communication sent on 04 December 2020.

<b>Action j)</b>	<b>Status:</b>	<b>Closed</b>
------------------	----------------	---------------

Audit Action: The information recorded on the ICT Inventories maintained by the schools varies. In all cases the serial number is recorded but only 1 school recorded the computer name. Schools should be reminded of the information that should be recorded on the inventory records and this should include the computer name.

Current position: A new standard inventory template has been developed and circulated to all Head Teachers and ICT Technicians and an Inventory Procedure is also included in the procedures pack sent to all Head Teachers and ICT Technicians.

<b>Action k)</b>	<b>Status:</b>	<b>Open</b>
------------------	----------------	-------------

Audit Action: 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.

Current position: It has not been possible to fully update inventory records and compare inventory records with System Centre information due to the impact of Covid-19 and the return of schools. The Working Group have discussed and agreed to delay this work until a more appropriate time due to the high level of workload for ICT Technicians at this time.

A System Centre Report will be provided to each secondary school w/c 07 June 2021. ICT Technicians will be requested to carry out a full inventory during the school holiday period and undertake a reconciliation and to report any anomalies addressed. This process has to be complete by 31 July 2021.

<b>Action l)</b>	<b>Status:</b>	<b>Closed</b>
------------------	----------------	---------------

Audit Action: ICT Services confirmed that the ICT Technicians have been added to the group "Sophos console administrators" which means they can do anything from a Sophos perspective. ICT Services should review ICT Technicians access and remove the administrator role if this is not required to ensure only relevant staff have this level of access.

Current position: Changes have been made to the current rights to ensure minimal access. Head Teachers and ICT Technicians were advised by email communication sent on 04 December 2020.

### **Update on Additional Action Raised at Audit & Scrutiny in January 2021**

At the Audit and Scrutiny Committee meeting held on 12 January 2021, members requested information on the comparison of device numbers in the last year.

ICT Services provided a report on the number of PC's, iPads and laptops currently in schools. However, upon investigation there appears to be a difference in the number of devices actually in schools.

The group have discussed this action and have agreed to run a more up-to-date report once the inventory records identified in Action k) is updated by the end of July.

It is proposed that the group will provide a report once the school inventories have been updated and any discrepancies as outlined above have been resolved. This will enable a report to be provided which reflects accurately the number of devices across schools. This information can be shared with the Committee at that time.

## **3. Proposals**

- 3.1 It is proposed that Audit and Scrutiny Committee note the progress made to date in the execution of the management actions contained in the Audit report and note plans for the Digital Strategy Review.

- 3.2 It is proposed that information on numbers of devices across schools will be provided after the inventory reconciliation has been carried out by ICT Technicians.

#### **4. Implications/Socio-economic Duty**

##### **Financial**

- 4.1 The Education service has spent £883,998 on digital devices and connectivity to support home learning for pupils during 2020-21. This was part-funded by a Scottish Government Grant of £551k. A total of £276,600 has also been spent on digital devices to support staff throughout the pandemic.

The Council is also investing £1.234m in 2021/22 and £0.752m in subsequent years in digital technology within schools.

##### **Human Resources**

- 4.2 None

##### **Legal**

- 4.3 The working group have addressed actions and developed procedures in line with data protection policy.

##### **Equality/Socio-economic**

- 4.4 None

##### **Environmental and Sustainability**

- 4.5 None

##### **Key Priorities**

- 4.6 None

##### **Community Wealth Building**

- 4.7 None

#### **5. Consultation**

- 5.1 Consultation has taken place with Head Teachers, ICT Technicians, ICT Services and Internal Audit.

Audrey Sutton  
**Executive Director (Communities and Education)**

For further information please contact **Susan Lauder, ICT Strategic Lead**, on **01294 552626**.

### **Background Papers**

Appendix 1 – Internal Audit Report

Appendix 2 – ICT Procedures in Schools Document

Appendix 3 – Working Together Agreement

# INTERNAL AUDIT REPORT

## REMOTE ACCESS CONTROLS AROUND THE EDUCATION NETWORK

<b>Assurance Level:</b>	<b>Limited</b>
<b>Version:</b>	Final
<b>Date:</b>	October 2020
<b>Author:</b>	Yvonne Trundle
<b>File Ref:</b>	2020-PA-023
<b>Classification:</b>	Official - Protect
<b>Budget Days:</b>	20 days
<b>Actual Days:</b>	22 days



**North Ayrshire Council**  
Comhairle Siorrachd Àir a Tuath



## 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:**

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

DRAFT

## KEY FINDINGS AND ACTION PLAN

### REMOTE ACCESS CONTROLS AROUND THE EDUCATION NETWORK

<b>Action</b>	a
<b>Finding</b>	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.
<b>Action Description</b>	Education should consider purchasing software to allow teaching staff to electronically sign up to the ICT Acceptable Use Policy.
<b>Risk</b>	Staff may not have agreed to comply with the ICT Acceptable Use Policy.
<b>Priority (1, 2, 3)</b>	3
<b>Paragraph Reference</b>	3.1
<b>Managed by</b>	Andrew McClelland, Head of Service (Education)
<b>Assigned to</b>	Andrew McClelland
<b>Due Date</b>	31/03/21
<b>Management Comment</b>	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.

<b>Action</b>	b
<b>Finding</b>	There is no documented formal Service Level Agreement between IT Services and Education to ensure clear roles and responsibilities are defined, agreed and allocated.
<b>Action Description</b>	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.
<b>Risk</b>	The roles and responsibilities of both parties have not been defined and agreed.
<b>Priority (1, 2, 3)</b>	2
<b>Paragraph Reference</b>	3.2
<b>Managed by</b>	Andrew McClelland, Head of Service (Education), Fiona Walker, Head of Service (People and ICT)
<b>Assigned to</b>	People and ICT: 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
<b>Due Date</b>	28/2/21
<b>Management Comment</b>	IT Services and Education to work together to draft an ICT Services SLA between IT Services and Education. Note there are significant differences in the Services provided by IT Services to Secondaries and Primaries. Education Comment: Education will set up a meeting with IT i.e. Carolann McGill, Michele Lavery to draft SLA, taking into account Primary and Secondary requirements.

<b>Action</b>	c
<b>Finding</b>	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.

<b>Action Description</b>	IT Services and Education should work together to define key functions and produce standard procedures to be followed.
<b>Risk</b>	Key tasks are not being carried out.
<b>Priority (1, 2, 3)</b>	2
<b>Paragraph Reference</b>	3.3
<b>Managed by</b>	Andrew McClelland, Head of Service (Education), Fiona Walker, Head of Service (People and ICT)
<b>Assigned to</b>	People and ICT: 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
<b>Due Date</b>	31/03/21
<b>Management Comment</b>	IT Services will set up monthly meetings with Education / ICT Technicians. The remit will be to <ul style="list-style-type: none"> <li>Identify key functions/tasks carried out by the ICT Technicians</li> <li>Agree standard procedures for the above functions and tasks</li> <li>Ensure standard approaches are taken across all schools and that ICT Technicians align with corporate ICT policies and procedure</li> </ul> <p>Education comment: A working group will be set up to address this action and will include ICT Co-ordinator, Quality Improvement Officer (ICT), Carolann McGill, Michele Laverty, James McNeil, Rosslyn Lee, Lynn Taylor, Alison Mair. Actions D, G, H, I, J, K and L will also be addressed by the working group. However, any preliminary actions possible prior to January 2021 will be carried out as detailed on agreed Action Plan (enclosed).</p>

<b>Action</b>	d
<b>Finding</b>	There are 481 iPads on the schools' inventory records that are not on the Airwatch report.
<b>Action Description</b>	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.
<b>Risk</b>	iPads have not been set up on Airwatch and are therefore not being properly managed in line with Council policy.
<b>Priority (1, 2, 3)</b>	1
<b>Paragraph Reference</b>	3.6
<b>Managed by</b>	Andrew McClelland, Head of Service (Education)
<b>Assigned to</b>	Lynn Taylor
<b>Due Date</b>	31/01/21
<b>Management Comment</b>	Education 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.

<b>Action</b>	e
---------------	---

<b>Finding</b>	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.
<b>Action Description</b>	IT Services should clarify which process is correct and update one of the documents accordingly.
<b>Risk</b>	Inconsistent advice provided to employees.
<b>Priority (1, 2, 3)</b>	2
<b>Paragraph Reference</b>	3.7
<b>Managed by</b>	Fiona Walker, Head of Service (People and ICT)
<b>Assigned to</b>	People and ICT: Carolann McGill, Team Manager Customer Experience; Derek Nelson, ICT & Cyber Security Architect
<b>Due Date</b>	28/02/21
<b>Management Comment</b>	IT Services will ensure that both documents are aligned. Education comment: confirm no action required by Education.

<b>Action</b>	f
<b>Finding</b>	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.
<b>Action Description</b>	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.
<b>Risk</b>	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.
<b>Priority (1, 2, 3)</b>	1
<b>Paragraph Reference</b>	3.7
<b>Managed by</b>	Andrew McClelland, Head of Service (Education)
<b>Assigned to</b>	Andrew McClelland
<b>Due Date</b>	31/01/21
<b>Management Comment</b>	Education comment: Update inventory records - Take to ICT Monthly meeting and analyse usage of USB devices, See Action C. A.McClelland will write to Schools with regard to this issue, advising to make maximum use of cloud storage and minimise the use of USBs.

<b>Action</b>	g
<b>Finding</b>	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.
<b>Action Description</b>	Password controls should be amended to be in line with best practice guidance.

<b>Risk</b>	Increased vulnerability to hacking or other forms of cyber-attack, which could lead to data breach or inability to undertake duties.
<b>Priority (1, 2, 3)</b>	1
<b>Paragraph Reference</b>	3.8
<b>Managed by</b>	Andrew McClelland, Head of Service (Education), Fiona Walker, Head of Service (People and ICT)
<b>Assigned to</b>	People and ICT: James McNeil, Team Manager IT Operations Education: Rosslyn Lee, Digital Skills Co-ordinator
<b>Due Date</b>	30/04/21
<b>Management Comment</b>	<p>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.</p> <p>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.</p> <p>Education Comment: Education will work with IT to roll out fine-grained password management and password complexity rules. This will allow staff to have a different password policy from pupils as many would not be able to cope with more complicated passwords. Agree a roll out with IT and School Technicians, See Action C.</p>

<b>Action</b>	h
<b>Finding</b>	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.
<b>Action Description</b>	Cloning should no longer be used to minimise the risk of teaching staff being given unnecessary access to potentially sensitive data.
<b>Risk</b>	Teaching staff are given unnecessary access to potentially sensitive data.
<b>Priority (1, 2, 3)</b>	2
<b>Paragraph Reference</b>	3.9
<b>Managed by</b>	Andrew McClelland, Head of Service (Education)
<b>Assigned to</b>	Andrew McClelland
<b>Due Date</b>	28/02/21
<b>Management Comment</b>	Education 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.

<b>Action</b>	i
<b>Finding</b>	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.



<b>Action Description</b>	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.
<b>Risk</b>	Former employees have inappropriate access to data.
<b>Priority (1, 2, 3)</b>	2
<b>Paragraph Reference</b>	3.10
<b>Managed by</b>	Andrew McClelland, Head of Service (Education), Fiona Walker, Head of Service (People and ICT)
<b>Assigned to</b>	People and ICT: James McNeil, Team Manager IT Operations Education: Lynn Taylor, Senior Manager Education
<b>Due Date</b>	28/02/21
<b>Management Comment</b>	Policy will be altered by IT Services to ensure accounts are moved to stale after 90 days. Education comment: 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. (to include in ICT Technician monthly meeting covered in Action C).

<b>Action</b>	j
<b>Finding</b>	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.
<b>Action Description</b>	Schools should be reminded of the information that should be recorded on the inventory records and this should include the computer name.
<b>Risk</b>	Non-compliance with inventory procedures and not all relevant information is recorded.
<b>Priority (1, 2, 3)</b>	3
<b>Paragraph Reference</b>	3.11
<b>Managed by</b>	Andrew McClelland, Head of Service (Education)
<b>Assigned to</b>	Lynn Taylor, Senior Manager Education
<b>Due Date</b>	28/02/21
<b>Management Comment</b>	Education comment: Education will ensure an IT Inventory is maintained by all schools using standard inventory template provided by IT. IT advised that they could possibly set up automated emails with relevant reports for the technicians but this would be discussed and agreed as part of the regular meetings. (to include in ICT Technician monthly meeting covered in Action C).

<b>Action</b>	k
<b>Finding</b>	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.
<b>Action Description</b>	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.
<b>Risk</b>	Lost or stolen laptops are not identified
<b>Priority (1, 2, 3)</b>	1
<b>Paragraph Reference</b>	3.12
<b>Managed by</b>	Andrew McClelland, Head of Service (Education)
<b>Assigned to</b>	Lynn Taylor, Senior Manager Education
<b>Due Date</b>	28/02/21
<b>Management Comment</b>	<p>Education 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. (to include in ICT Technician monthly meeting covered in Action C).</p> <p>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.</p>

<b>Action</b>	I
<b>Finding</b>	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.
<b>Action Description</b>	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.
<b>Risk</b>	ICT administrators could change policy that has been set corporately by IT Services without IT Services being aware of changes made.
<b>Priority (1, 2, 3)</b>	2
<b>Paragraph Reference</b>	3.15
<b>Managed by</b>	Fiona Walker, Head of Service (People and ICT)
<b>Assigned to</b>	James McNeil, Team Manager IT Operations
<b>Due Date</b>	31/01/21
<b>Management Comment</b>	<p>IT Services will review ICT Technician rights and ensure that only rights appropriate to the ICT Technician role are implement i.e. "just enough admin" rights.</p> <p>Education comment: agree appropriate rights with IT Services (to include in ICT Technician monthly meeting covered in Action C).</p>

### Priority Key used in Action Plan

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

DRAFT

## Communities and Education Directorate



# ICT Guidance for Schools

## Procedures Index

- **New Start Procedure**
- **Setting up a New Device**
- **Inventory Procedure**
- **Leavers Procedure**
- **Disposal Procedure**
- **Anti-virus Software Procedure**
- **USB Pen Drives Procedure**

## Secondary Schools – ICT Guidance

### NEW START PROCEDURE

## Creating New Active Directory User Accounts from Scratch

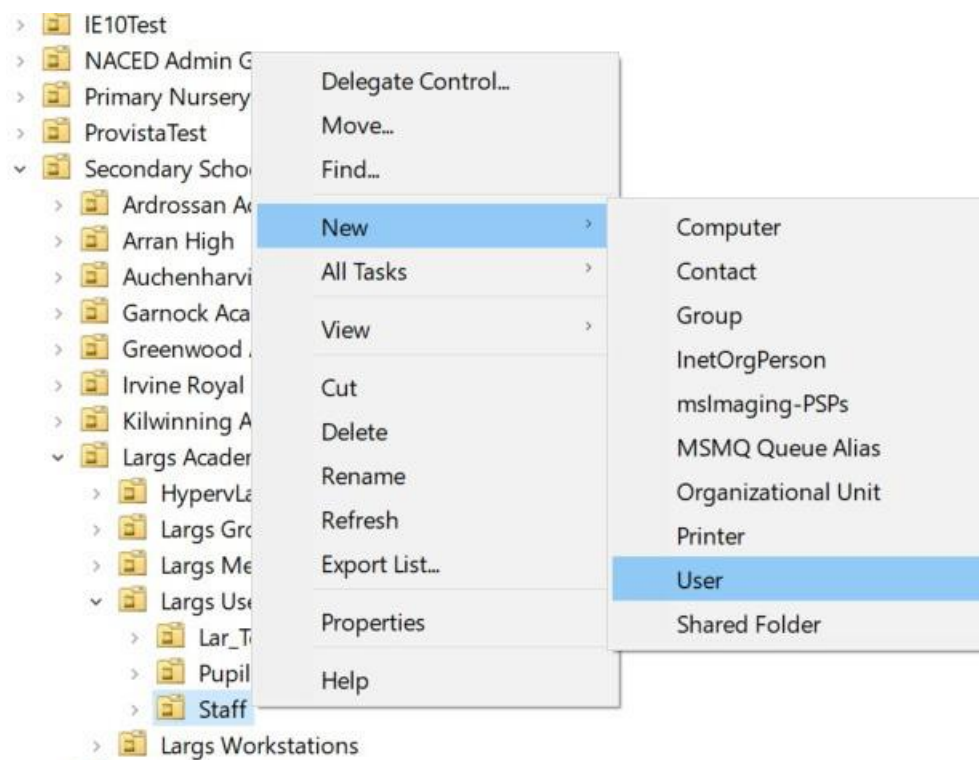
Until recently, normal practice has been when a new member of staff starts, we would have cloned the account of an existing person in the same department. This was a quick and easy way to ensure that they had access to the same resources as their colleagues. However, this risks inadvertently giving the new person permissions that they should not have.

One of the conclusions of the recent ICT audit was that, due to security risks, the process of cloning user accounts must end. Corporate ICT have already stopped the practice of cloning and instead every user is created from scratch and given membership of groups appropriate to their job. Therefore, a new user must be created for all new staff, with immediate effect.

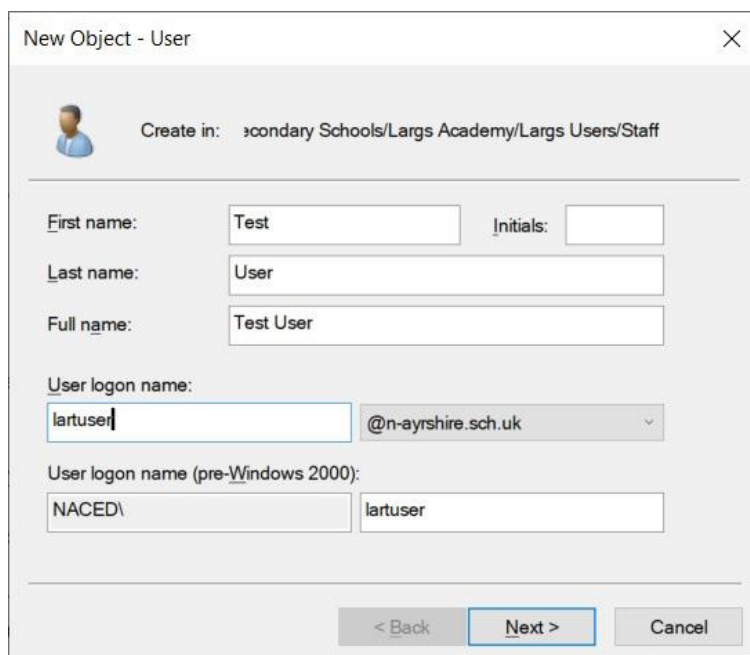
The appropriate Faculty Head/Line Manager will inform the ICT Technician when a new employee joins the school and the following process should be adhered to.

To create a new user, follow these steps:

Navigate to the OU in AD where the user should be, appropriate to your own school, in this case **Secondary Schools, Largs Academy, Largs Users, Staff**. Right-click, point to **New**, and then click **User**.

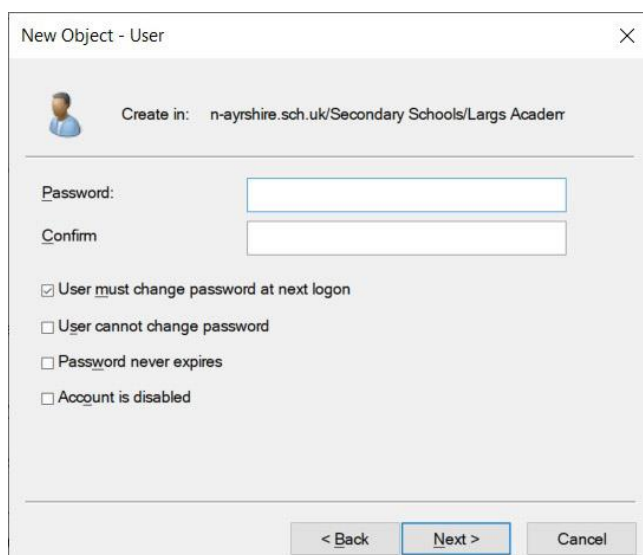


Type the first name, last name, and user logon name of the new user, and then click **Next**.



The screenshot shows a dialog box titled "New Object - User". At the top, it says "Create in: ionalary Schools/Largs Academy/Largs Users/Staff". Below this, there are several input fields: "First name:" with the value "Test", "Initials:" with an empty field, "Last name:" with the value "User", and "Full name:" with the value "Test User". Underneath, "User logon name:" has the value "lartuser" and a dropdown menu showing "@n-ayrshire.sch.uk". Below that, "User logon name (pre-Windows 2000):" has two fields with the values "NACED\" and "lartuser". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Type a temporary password, confirm the password, and then click to select **“User must change password at next logon”**

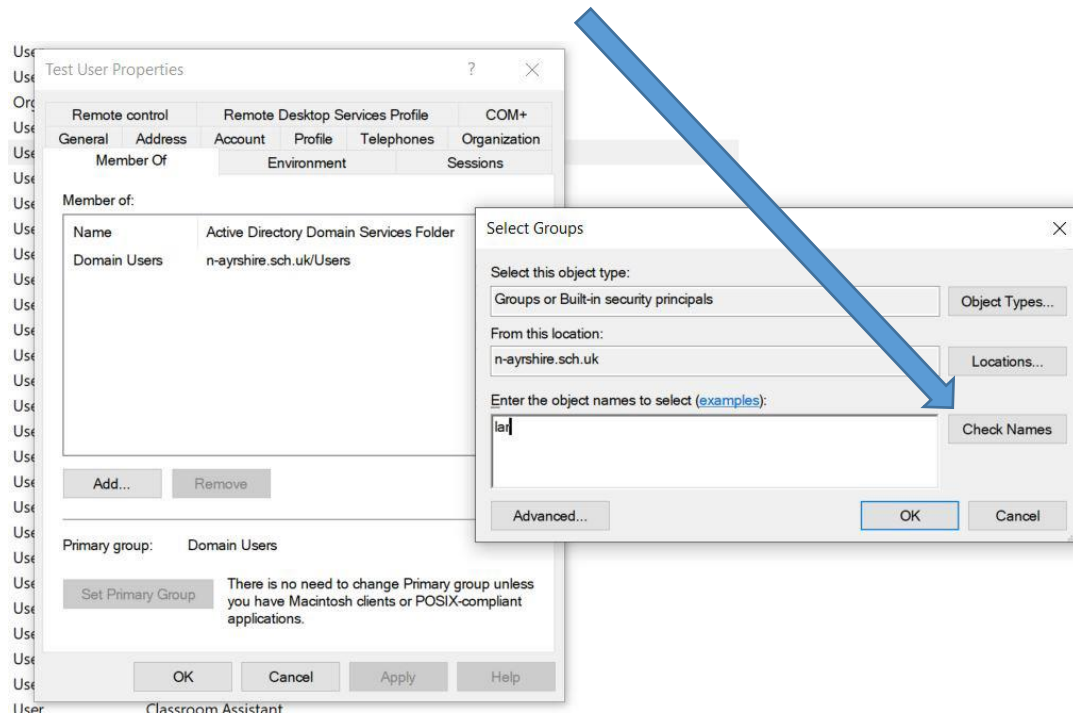


The screenshot shows the same dialog box, but now it's asking for a password. It has two input fields: "Password:" and "Confirm". Below these are four checkboxes:  "User must change password at next logon",  "User cannot change password",  "Password never expires", and  "Account is disabled". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

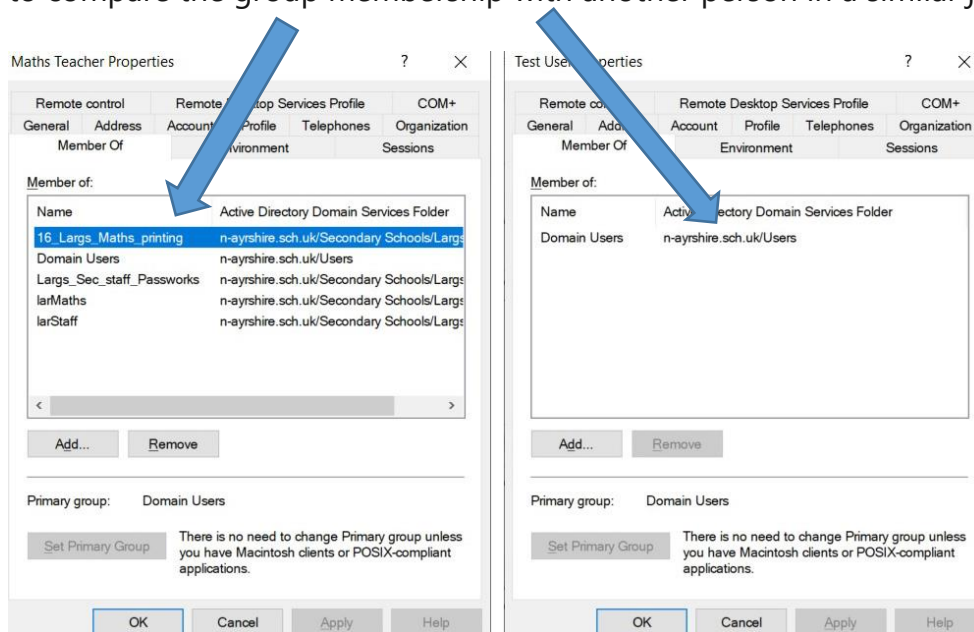
Click **Next**.

After you create the new user,

Right click the user and select **Properties**. Click the **Member Of** tab, and then click **Add**. In the **Select Groups** dialog box, specify a group, and then click **OK** to add the groups that you want to the list. This can be made easier by typing the first few characters of the group name and clicking **“Check Names”**



Repeat the selection process for each group that the user needs to be in. It should help to compare the group membership with another person in a similar job.



In the General tab you should add a description. (If your school uses Safecom for printing, you will have to specify the printing group here).

Test User Properties

Member Of: Remote control  
Environment: Remote Desktop Services Profile  
Sessions: COM+

General | Address | Account | Profile | Telephones | Organization

Test User

First name: Test Initials:

Last name: User

Display name: Test User

Description:

Office:

Telephone number:  Other...

E-mail:

Web page:  Other...

OK Cancel Apply Help

If your school uses the scan to email function, you should add their email address here.

In the Profile Tab you will have to manually enter the appropriate Logon script for your school and manually enter the path to the user's H: drive

Test User Properties

Member Of: Remote control  
Environment: Remote Desktop Services Profile  
Sessions: COM+

General | Address | Account | Profile | Telephones | Organization

User profile

Profile path:

Logon script: larSTAFF

Home folder

Local path:

Connect: H: To: \\nacedlar1\staff\TUser



## Secondary Schools – ICT Guidance

### SETTING UP A NEW DEVICE



## Ordering a new device

All new IT equipment must be ordered by logging in to the [IT Services Customer Portal](#), clicking **Submit a Request** on the top menu, then choosing the **Order New IT Equipment** option.

## Laptop – how to set up the encryption and direct access

All staff laptops must be encrypted to protect the data when outside of school.

- Navigate to \\nacedsrv1\mbam
- Copy the files **MbamClientSetup.exe** and **mbam.reg** to the desktop
- Run **MbamClientSetup.exe**
- Run **mbam.reg**
- Wait for a window to appear asking you to set a PIN
- Set a temporary PIN
- Encryption will begin shortly afterward
- The user must change the PIN to one of their choice after they have logged on, by clicking the **Change Encryption PIN** icon on their desktop

All staff are able to work from home using Microsoft direct Access. To enable Direct Access, simply add the laptop to the MBAM\_Computers group in Active Directory. Only encrypted laptops should be given Direct Access.

## iPad – how to set up on Airwatch

When purchasing a new iPad, it should come already configured for Airwatch. However, should any be sent to the school in error, you must log a job on the [IT Services Customer Portal](#) to have them added to Airwatch.

## Standard Build Procedure

A standardised procedure should be followed when setting up a new device, where possible.

An **example** standard build is outlined below and may be used for such departments as English, Social Subjects, Library use etc.

Install Windows 10 Education (Latest version available. Currently 20H2. MAK version)	
Check Windows activation	
Set language and regional settings to UK	
Pre-stage computer name in Active Directory, in the appropriate OU	
Rename the computer and join n-ayrshire.sch.uk domain	
Log in to domain	
Install Sophos from \\SERVERNAME\sophosinstall	
Install latest Cumulative Update <a href="https://www.catalog.update.microsoft.com/home.aspx">https://www.catalog.update.microsoft.com/home.aspx</a>	
Install latest drivers for your device and Windows version <a href="http://ftp.hp.com/pub/caps-softpaq/cmit/HP_Driverpack_Matrix_x64.html">http://ftp.hp.com/pub/caps-softpaq/cmit/HP_Driverpack_Matrix_x64.html</a>	
Install Microsoft Office 2019 with accessibility tools and activate (Some schools may use earlier versions of Office)	

Install the Chrome browser (Edge will be installed as part of the Windows installation)	
Install Adobe Reader	
Install Java 8 (Check the current required version for SEEMiS)	
Install VLC Player	
Adjust Power Settings if required (e.g. devices not to sleep until after 1 period)	
Install Scottish Voice Heather	
Install Scottish Voice Stuart	
Install any printers required (Procedure varies between schools)	
Install 7zip	
Install .net3.5 (Can be installed from Windows media)	
Install SEEMiS and manually set up shortcuts	<b>Staff devices only</b>
Install Active Inspire Suite (Only licenced if you have a qualifying Promethean panel)	<b>Staff devices only</b>
Install any additional software that your school has a site licence for (e.g. LanSchool)	
Add any standard shortcuts required to public desktop (e.g. if your school has an intranet homepage)	
*If required, run gpedit.msc	
Set standard Start Layout	
Set standard wallpaper and lock screen	
<b>Before continuing you should test everything thoroughly then capture an image prior to encryption. Encrypted hard drives shouldn't be cloned.</b>	
Encrypt	<b>Staff devices only</b>
Add to MBAM_Computers group to enable home working	<b>Staff devices only</b>

\*To set standard Start Layout run gpedit.msc

Computer Configuration, Administrative Templates, Start Menu and Taskbar, Start Layout – Set to C:\Start.xml (To export, start Windows Power Shell and run command “**Export-StartLayout –Path G:\Start.xml**” Copy xml file to C:)

**Please note that this is a suggested basic build. There will be various items of subject specific software and configurations required throughout the school. It is not an exhaustive list.**

## Non-Standard Build

Where there is a requirement for additional software to be installed for school departments such as Music, Computing, Design Technology etc. ICT Technicians should liaise with the appropriate Faculty Head/Line Manager to install the appropriate software, which complies with NAC policies and procedures.

## Secondary Schools – ICT Guidance

### INVENTORY PROCEDURE



## Standard Inventory Template

The enclosed standard inventory template should be used for all types of devices used within a secondary school i.e. laptops, iPads, USBs etc.

It is important that the inventory information is kept up to date on an ongoing basis i.e. as and when additions and disposals take place and NOT left to year-end. This is an audit requirement and as such copies of inventories can be requested at any point throughout the year.

Sufficient information should be recorded to enable items to be easily identified i.e. monitor, dock etc. Where IT equipment is recorded in this way, the serial number, computer name and make of the processing unit must be recorded.



Schools Inventory  
Template 2021.xlsx

## NAC Inventory Procedure

The NAC Inventory Procedure is enclosed for your information and adherence.



NAC Inventory  
Procedures.pdf

## Annual Audit

An Annual Audit should be carried out at school level and the inventory report authorised by the Head Teacher or a designated member of the School Management Team. The inventory report should be sent to headquarters for sign off by the ICT Strategic Lead for Education.

An annual audit should take place between June and July each year, a date at the end of July will be advised for the completed audit report to be sent to headquarters.

However, it is important that inventory records are kept up-to-date as Internal Audit can request copies of inventory documents at any time throughout the school year and financial year.

## Secondary Schools – ICT Guidance

### LEAVERS PROCEDURE



A Leavers Form has been developed which should be completed prior to a member of staff leaving the Service. Ideally within 1-2 days of the official leaving date.

- The Head Teacher should inform relevant school staff once a leaving date has been confirmed for a member of staff i.e. Education Business Officer, School Office Staff, ICT Technician, Janitor.
- A Leavers Form should be initiated and populated with the employee name and leaving date and sent to the ICT Technician to complete the appropriate sections. The ICT Technician should also inform Corporate ICT in relation to the computer login and also the Corporate 0365 account.
- The Leavers Form should then be passed to Janitorial staff to complete their appropriate sections.
- Once the form has been completed, it should be passed to the Head Teacher for authorisation.
- The Leavers Form should be held within the school for audit purposes.



Insert School Name



# Staff Leavers Form

This form should be completed as close as possible to the leaving date.

<b>Name of Staff Member:</b>	
<b>Leaving Date:</b>	

Laptop/ iPad model and serial number

Make/ Model	Serial Number
HP EliteBook G4	

Please **initial** the appropriate box or mark as N/A.

Item of Equipment	Returned	Disabled	Deleted	Designation <i>(delete as appropriate)</i>	Date
Laptop/ iPad				ICT Technician/Line Manager (Primary)	
Charger				ICT Technician/Line Manager (Primary)	
Computer Login				ICT Technician/ EBO/ IT Services (Primary)	
Mobile phone/ Radio				ICT Technician	
Keys				Janitor	
ID badge/ Door entry fob				Janitor	
SEEMiS work record				EBO	
Corporate O365 Account				EBO/ IT Services	

When a user is removed from SEEMIS their Glow login should automatically close.

<b>Head Teacher's signature:</b>	
<b>Date:</b>	

## Secondary Schools – ICT Guidance

### DISPOSAL PROCEDURE

## NAC Disposal Procedure

The NAC Disposal Procedure should be followed by secondary schools for the disposal of IT Equipment.

The procedure is attached for your information and is also referred to in the NAC Inventory Procedure.



NAC

ict-disposal-guideline:

## Procedure for uplift of IT Equipment

1. Browse to the [IT Customer Portal](#) and log a new Service Request for Equipment Collection.
2. If you have 5 or less items, please complete the form on the page and submit the request.
3. If you have more than 5 items, please download the [ICT Disposal request form \(xlsx, 18kb\)](#) and upload it to the case and submit the request.

A member of staff must be made available to oversee the collection. It is his/her responsibility to check the correct equipment has been collected, and to sign the waste transfer note from the driver.

Store equipment neatly. The serial numbers from each device will be checked by the driver at your location before being loaded onto the van. To help reduce delays, stack like items together and place keyboards, cables and mice in a box or bag.

All paperwork in relation to disposal of IT equipment should be retained in the school for audit purposes.

## Secondary Schools – ICT Guidance

### ANTI-VIRUS SOFTWARE



## New devices and Anti-Virus Software

When a new device has been set up by the ICT Technician the anti-virus software should automatically be installed as soon as the new device is joined to the network. However, it is good practice to manually install. The location of the installation files will typically be \\SERVERNAME\sophosinstall

Notifications from Sophos will automatically come up on screen in relation to any viruses detected. This could include such notifications as 'potentially unwanted applications' (PUA's). These on the main are not dangerous. However, other notifications could be highlighted which require action to be taken, therefore, it is important to ensure that the anti-virus software has been installed.

Please find further information in the ICT and Cyber Security Policy enclosed.



ICT and Cyber  
Security Policy.pdf

## Secondary Schools – ICT Guidance

### USB PEN DRIVES PROCEDURE



### USB Pen Drives Policy

It is NAC policy that **only encrypted USB pen drives (AES hardware encryption)** should be used in schools and they should be included in the school inventory. The audit highlighted that there are many unencrypted devices being used in schools and many have not been properly recorded.

The use of USB pen drives should be minimised where possible. All staff have access to OneDrive and Google Drive, therefore, documents not classed as personal or sensitive should be stored in one of these Cloud locations.

Encrypted USB pen drives may continue be used to store personal/sensitive information and all devices must be recorded on the school's inventory as per North Ayrshire Council policy.

#### **In summary:**

- **Only encrypted USB pen drives can be used in schools – AES hardware encryption.**
- **Encrypted USB pen drives may continue to be used to store personal/sensitive information.**
- **Devices must be recorded on the school's inventory.**

#### **Note:**

Anyone currently using an unencrypted pen drive should have this replaced with an encrypted one immediately and ensure the unencrypted device is erased and disposed of safely.





# Working Together Agreement – between Education and IT Services – May 2021

This agreement is between the Education Service and IT Services who provide IT support to our Schools. 'Schools' refers to all education establishments which include Early Years Centres and Bases.

## Duration

*The working together agreement will run from 01 May 2021 – 31 May 2022, the agreement will be reviewed annually thereafter.*

## Intent

This Working Together Agreement has been developed in collaboration between IT Services and Education. The agreement aims to provide the best value and highest quality support to schools, and enable schools to maintain reliable and suitable ICT for learning and teaching through:

- A coordinated programme of support, maintenance, and repair with a focus of prevention of future incidents.
- Support and advice for school staff to enable a speedy resolution of basic technical issues.

- Effective communication and systems for monitoring and reporting, with clear accountability and actively managed channels for feedback.
- Through a formal working group IT Services and Education will address and discuss any issues, developments, and work towards consistency in all IT related services. Formal procedures created via this group will be added to this document via a link.

*Note: Throughout the document - IT Technician refers to Corporate IT and ICT Technician refers to Education school-based Technicians.*

#### **Key Responsibilities of IT Services:**

- Provide remote support for hardware and software issues through the Helpdesk facility, including IT infrastructure, such as network and servers.
- Provide on-site support visits where required, examples provided in Section 3, and provide written reports recorded on the Information Technology System Management (ITSM) Customer Portal.
- Provide support on large projects, outwith term-time, to minimise impact on schools.
- Provide same day support for major IT related emergencies within schools.

#### **Key Responsibilities of Schools:**

- To adhere to the process on the [IT Customer Portal](#) for logging and repair of IT equipment in primary schools, including ensuring that appropriate arrangements are in place for IT Technicians visiting to repair equipment. Further details are outlined in the [IT Services – visits to schools'](#) section below.
- To ensure secondary schools staff contact their ICT Technician in the first instance for any IT related support. Should the issue require escalation to IT Services, the ICT Technician will log a job.
- To ensure all ICT Technicians within Secondary Schools adhere to the procedures agreed as follows:
  - New Start Procedure
  - Setting up a New Device
  - Inventory Procedures and Annual Audits
  - Leavers Procedure
  - Disposal Procedure
  - Anti-virus Procedure
  - USB Pen Drives Procedure



ICT Procedures in  
Schools.pdf

The procedures have been circulated to all ICT Technicians and will be kept in a central resource file for ease of access. Additional procedures will be added as and when agreed and a notification will be sent to Head Teachers and ICT Technicians.

## Service to be provided to our schools

The **IT Helpdesk facility** is available to all schools to provide remote support of all hardware and software issues. The service is provided to resolve the majority of issues, through directed advice or live remote assistance. The facility can be accessed Monday to Thursday, 08:00am to 4.45pm and Friday 08:00 to 16:30 the number to call is 01294 324290. Alternatively, contact can be made through the online [IT Customer Portal](#) .

A Job Ticket will be generated for the school under the name of the person who has called. A reference number will be given to allow easy tracking and follow up for both the client and technical staff.

For issues that cannot be resolved on the phone or require escalation an appointment will be made to visit the school to resolve.

**Reporting and monitoring** - a written summary of work carried out on each visit is recorded on our IT Customer Portal. Access is available to nominated education contacts within the school who have raised tickets. IT Services monitor the service to schools and their technician's processes through the Information Technology System Management (ITSM) system for any breaches of milestones and ensure updates are showing on tickets raised.

**IT Services** scheduled onsite support visits support a planned programme of implementation of hardware/software, maintenance and repair that provides a dependable presence at the school. Work carried out during the technical visits can include, but is not limited to, the following:

- Maintenance of curriculum and admin systems
- Support of peripheral devices e.g. printers
- Resolution of user issues and functionality
- Installation of new hardware and software
- Management of network, security, and protection
- Liaising with external suppliers to resolve specific technical issues

IT Services visits will be made by appointment. This will be negotiated in advance and applies to term time only. An individual visit may be rearranged either by the Schools or IT Services, providing both parties agree. If a visit cannot be honoured due to unforeseen circumstances, the appointment will be re-scheduled and every effort will be made to communicate this with the school as soon as possible.

**Out of Term visits** may be arranged for large projects to eliminate impact to the school. Head Teachers will be fully informed in advance in order for preparations to be made. Access for these visits will be arranged via an Education Service contact (key holder) who can support the opening of schools during these times.

**Major Emergencies and ad-hoc callouts** may be required on occasions where an onsite presence is required due to unforeseen circumstances. In all cases IT Services will follow up almost immediately with some remote support. Failing a resolution, an IT Technician will be arranged to visit the school on the day the incident is reported. Unfortunately, IT Services cannot offer emergency visits beyond 4.45pm, if reported on or after this time, an IT Technician would be scheduled for an early next day visit (9am).

## Exclusions and best endeavours

**IT Services** will endeavour to resolve all issues encountered, However, due to the nature of some issues they may be excluded from support under the following categories:

- Beyond economic repair (where cost of repair exceeds cost of replacement)
- Out of support devices which should have been securely disposed of
- Printers not procured via the Council's required framework
- Health and Safety implications in relation to resolving issues such as carrying heavy equipment or climbing ladders.
- Mechanical failure (for systems with moving parts such as printers)
- Personal devices
- Pupil Home Devices such as Chromebooks or Ipad
- Non-standard software not previously encountered. New software and exceptions must be discussed with IT Services on a case-by-case basis.
- Peripheral Devices such as projectors, and classroom interactive and panel boards. Issues with these devices must be reported direct to the vendor by emailing AVMI on [helpdesk.scotland@kinly.com](mailto:helpdesk.scotland@kinly.com)

## IT Services - visits to Schools

To enable IT Services to provide the services outlined in this agreement to our schools and to the best possible standards, the school must ensure the following criteria are met:

- Ensure a single or primary point of contact for IT reporting of issues is identified.
- Ensure devices are placed in the school's red box clearly marked with the ticket reference (Primary Schools only).
- Liaise with the IT Technician at both the beginning and end of the visit for updates and feedback on support and ongoing issues.
- Ensure appropriate arrangements have been made to enable the IT Technician to carry out tasks as requested (e.g. access to PC or software, suitable space to perform fixes complete with power and network access).
- Log technical tasks and jobs. This is vital to ensuring the IT Technician can prioritise workload and minimise the number of interruptions whilst working on other issues.

- Ensure access to physically restricted equipment is possible prior to a school visit.

## Continuous Improvement

Continuous improvement is critical to our schools, the working group which has been set up will collaborate regularly to make technology work better for our teachers and pupils enabling their creativity and enhancing their learning.

## Health and Safety

It is the school's responsibility to ensure the IT Technician is briefed on the school's health and safety procedures and that the visiting IT Technicians adhere to the school's signing in and signing out procedures. IT Technicians are not expected to lift significant technical equipment or to climb or crawl to access systems. It has also been agreed that a member of staff in our ASN schools and Bases should accompany the IT Technician throughout the visit to ensure children and young people do not feel anxious.

### **Note:**

Enquiries for device pricing or procurement of Technology MUST be requested from IT Services and not Education Services through the online Customer Portal or by calling 01294 324290.