KWAZULU-NATAL PROVINCE
EDUCATION
REPUBLIC OF SOUTH AFRICA

DIRECTORATE: MATHS, SCIENCE, TECHNOLOGY & INFORMATION COMMUNICATION TECHNOLOGY

Private Bag X9137, PIETERMARITZBURG, 3200
Suite 328: Department of Education - Head Office
228 Pietermaritz Street| Pietermaritzburg|3200
Tel: 033 846 5538 |Fax: 033 846 5435

Enquiries: Lucky Mthetho
Email: Lucky.Mthetho@kzndoe.gov.za

STANDARD OPERATING PROCEDURE: SCHOOL-BASED ICT SECURITY, ASSET MANAGEMENT, AND RESOURCE UTILISATION

Effective Date:	15 September 2026
Review Cycle:	Five years from date of the signature
Head of Department:	Mr G. N Ngcobo

1. Purpose

This Standard Operating Procedure (SOP) defines the mandatory processes for developing institutional school-based ICT security policies, governing ICT hardware and software assets, and regulating the proper utilisation of public educational ICT resources by both educators and learners within the KwaZulu-Natal Department of Education.

2. Legislative Framework & Alignment

All institutional procedures mapped within this SOP must comply strictly with national and provincial legal frameworks, including but not limited to:

- **South African Schools Act (Act No. 84 of 1996):** Empowers School Governing Bodies (SGBs) to pass local school-level codes of conduct and institutional infrastructure management policies.
- The school management team led by the principal is further advised that after the deployment of (ICT) resources, the maintenance and management must be in line with the South African Schools Act No. 84 of 1996 relating to the following clauses:

  Section 16A (2): Functions and responsibilities of principal of public school
  The principal must—
  (a) in undertaking the professional management of a public school as contemplated in section 16 (3), carry out duties which include, but are not limited to—
  (iii) "the management of the use of learning support material and other equipment"
  (v) "the safekeeping of all school records.

  Section 37 (5): School funds and assets of public schools - "*All assets acquired by a public school on or after the commencement of this Act are the property of the school*"
- **Public Finance Management Act (Act No. 1 of 1999):** Mandates strict internal control systems, accountability metrics, and asset verification practices for all state assets deployed in learning spaces.
- **Protection of Personal Information Act (Act No. 4 of 2013):** Imposes absolute statutory care obligations to safeguard sensitive data, identity logs, and student records maintained across local school platforms.

3. Workflow for School-Based ICT Security Policy

Every public school in the province must formulate an individualised School ICT Security Policy through a formalized governance cycle. The development workflow requires four mandatory stages:

Step 1: Establishment of the School ICT Committee: The Principal must formally commission a School ICT Committee comprising an ICT coordinator, an SGB representative, and designated educators. This committee drives operational planning.

Step 2: Conduct Asset Risk Assessment & Inventory Management: The committee must audit local network configurations, physical storage facilities, user access mechanisms, and active device tallies before drafting security controls in conjunction Asset Management Committee.

Step 3: Outlining Scope of the ICT Policy: A draft policy must be generated specifying password requirements, classroom ICT resource sharing, safeguarding of ICT resources, network firewalls, data backups, access control to ICT storage/rooms & smart classroom, participation on Microsoft Schools Agreement and clear handling parameters for incidents including loss, theft, burglary, breakages etc.

Step 4: SGB Ratification & Sign-off: The final draft must be formally adopted through an SGB resolution, documented in meeting minutes, and co-signed by the Principal and the SGB Chairperson.

4. ICT Device Asset Management Procedures

4.1 Asset Tracking and Procurement Logs

All hardware items—including interactive smartboards, teacher laptops, tablets, and desktop units—must be accurately recorded against the asset register. The following processes are compulsory:

- Filing of all installation sign-off and proof of deliveries
- **Immediate Registry Capture:** Every departmentally supplied or independently purchased device must be recorded in the official school asset registry within 24 hours of delivery.
- **Labelling:** All physical hardware must be permanently marked with the institutional KZN-DoE school-based asset tracking number. This must include the serial number of each device.

4.2 Physical Storage and Structural Infrastructure

Schools must implement protective barriers to mitigate theft and environmental damage risks:

- **Re-enforced Storage Environments:** Server cabinets, media centers, and device storage rooms must be re-enforced with physical padlocks, electronic alarm systems (where possible), and functional fire extinguisher setups.
- **ICT Resources Received or Purchased:** Mobile ICT Resources must be kept inside centralized charging lockers when not in active classroom usage, logged carefully using manual sign-out registers. They can also be assigned to individual users/teachers through a formal handover procedure.

4.3 Reporting and Mitigation Framework for Losses

In the event of institutional hardware loss, damage, or theft, schools must initiate immediate compliance procedure:

Action Item	Mandatory Timeline & Output Details
SAPS Case Filing	File an official theft report with the South African Police Service (SAPS) within 24 hours of incident discovery to secure a valid Case Number.
District Escalation	Submit a written notification detailing hardware specification to the Circuit Manager and District Director within 48 hours.
Registry Update	Flag the device as 'Stolen/Lost' in the school asset ledger. Append copies of the SAPS report and insurance claims for subsequent auditing.
Head Office	The district, through the District ICT Coordinator, must further submit the information to MST & ICT Directorate within next 48 hours.

5. ICT Resource Utilisation Controls

Departmental ICT systems are provided strictly for curriculum delivery, professional educational administrative tasks, and structured learning interventions.

5.1 Rules for Educators and Administrative Personnel

- **Credential Integrity:** Educators must utilize individualized, password-protected profiles on school networks. Passwords must never be shared or left visible.
- **ICT Curriculum Integration: T**he educator to integrate ICT resource utilization during the implementation of annual teaching plan.
- **Content Moderation obligations:** Educators are strictly prohibited from utilizing department-funded networks to stream, download, or distribute non-educational multimedia content.

5.2 Rules for Learners and Classroom Activity

- **Access to ICT Lab/Smart Classroom:** Learners may only enter digital learning facilities or interact with school ICT resources under the direct supervision of an educator or ICT Coordinator.
- **Hardware Handling Protocol:** Learners are strictly barred from altering physical device cabling, installing unauthorised software applications, or bypassing local filtering rules.
- **Handling of Classroom ICT Resources:** learners are prohibited to tamper with data projects, HDMI cables, interactive smart screens and any other relevant resources deployed.
- **Cyber-Safety and Conduct:** Any instance of online bullying, accessing inappropriate materials, or malicious software tampering will trigger immediate disciplinary steps under the SGB School Code of Conduct.

6. Executive Approval and Sign-off

By authority of the Head of Department of the KwaZulu-Natal Department of Education, this Standard Operating Procedure is officially approved for immediate province-wide distribution and local institutional enforcement.

MR G. N NGCOBO
HEAD OF DEPARTMENT
KWAZULU-NATAL DEPARTMENT OF EDUCATION

28/9/26
DATE