Iphondo leMpuma Kapa: Isebe leMfundo
Provinsie van Oos Kaap: Department van Onderwys
Provense ya Kapa Botjhabela: Letapha la Thuto

OFFICE OF THE DIRECTOR: INFORMATION COMMUNICATION TECHNOLOGY (ICT)
Steve Vukile Tshwete Complex, Zone 6 Zwelitsha, 5608, Private Bag X0032, Bhisho, 5605 REPUBLIC OF SOUTH AFRICA:
Enquiries: **Mr L. Ndzube Tel: 040 608 4244. Fax :040 608 4672. Email:** lethu.ndzube@ecdoe.gov.za
Website: www.eceducation.gov.za

INTERNAL MEMORANDUM

TO : ALL DDGS, CHIEF DIRECTORS, DIRECTORS, CIRCUIT MANAGERS, PRINCIPALS AND ICT STAKEHOLDERS

FROM : DIRECTOR ICT

DATE : 07 MAY 2026

SUBJECT : END-OF-LIFE (EOL) OF LEGACY DEVICES AND ASSOCIATED ICT SECURITY RISKS

1. PURPOSE

To formally communicate the identification of legacy and End-of-Life (EOL) ICT devices within the Eastern Cape Department of Education (ECDoE) environment, to outline the associated operational, security, governance, and network risks introduced by these devices, and to request approval for the implementation of mitigation and replacement measures.

2. BACKGROUND

The ICT Directorate has identified several categories of devices currently operating within the departmental environment that have reached manufacturer End-of-Life (EOL) or End-of-Support (EOS) status. These devices no longer receive vendor security updates, firmware support, compatibility updates, or performance enhancements required to operate securely within the modern ICT environment.

The affected devices include, but are not limited to:

1. Lenovo ThinkPad L460, L470, L480, and L490 models
2. Lenovo ThinkPad T440p models
3. Devices utilising Intel Pentium processors
4. Desktop and laptop devices classified as aged or beyond the approved ICT lifecycle threshold

The continued operation of these devices presents increasing technical, operational, cybersecurity, and governance concerns for the Department.

3. RISK AND SECURITY IMPLICATIONS

The continued use of legacy and EOL devices exposes the Department to the following risks:

3.1 Information Security Risks

1. Unsupported operating systems and firmware no longer receive security patches, increasing exposure to known vulnerabilities and cyber threats.
2. Legacy devices may not support current endpoint protection, encryption standards, identity management controls, or modern security protocols.
3. Increased risk of malware infections, ransomware attacks, unauthorised access, and data compromise.

3.2 Network and Infrastructure Risks

1. Outdated hardware components may negatively impact network performance and stability.
2. Legacy devices may generate compatibility issues with modern systems, cloud services, authentication platforms, and security configurations.
3. Unsupported devices may introduce vulnerabilities into the broader departmental network environment.

3.3 Governance and Compliance Risks

1. Continued use of unsupported devices may result in non-compliance with the Department's Information Security Management System (ISMS), ICT governance framework, and audit requirements.
2. Increased likelihood of audit findings relating to asset lifecycle management, ICT controls, and information security compliance.

3.4 Operational Risks

1. Higher failure rates and reduced device reliability impact service delivery and user productivity.
2. Increased maintenance overhead and reduced vendor support availability.
3. Escalating support costs associated with maintaining obsolete technology.

4. ICT GOVERNANCE POSITION

In line with ICT lifecycle management principles and departmental governance requirements, devices classified as End-of-Life (EOL) or End-of-Support (EOS) should be formally phased out and replaced through approved procurement and asset replacement processes.

The ICT Directorate reserves the right to progressively restrict or isolate unsupported devices from accessing departmental systems and network resources where such devices present a security or operational risk.

5. RECOMMENDATIONS REQUESTED

It is recommended that approval be granted for the following:

1. Formal recognition of identified legacy devices as End-of-Life (EOL) assets within the ECDoE ICT environment.
2. Progressive decommissioning and phased removal of unsupported devices from departmental networks and systems.
3. Implementation of access control measures restricting unsupported devices from connecting to departmental ICT infrastructure.
4. Development and implementation of a departmental device replacement and refresh plan aligned to approved budget and procurement processes.
5. Enforcement of lifecycle management standards for all ICT assets to ensure continued compliance with ICT governance and security requirements.
6. Mandatory updating of asset registers to reflect lifecycle status, decommissioning actions, and replacement requirements.
7. Disposal of decommissioned devices in accordance with approved asset disposal, environmental, and PFMA compliance processes.
8. Communication of this directive to all business units, districts, schools, and ICT stakeholders for immediate awareness and compliance.

6. IMPLEMENTATION AND ENFORCEMENT

The ICT Directorate will progressively implement monitoring and enforcement measures to ensure compliance with this directive and to protect the integrity, security, and stability of the departmental ICT environment.

Implementation measures will include:

1. Identification and verification of all legacy and End-of-Life (EOL) devices within departmental environments.
2. Monitoring of device compliance against approved ICT lifecycle and security standards.
3. Progressive restriction, isolation, or removal of unsupported devices from departmental systems, networks, and cloud services where risks are identified.
4. Coordination with business units, districts, and schools regarding replacement planning and decommissioning processes.
5. Continuous reporting on compliance status, identified risks, and implementation progress through relevant ICT governance structures.

All business units, districts, schools, and officials utilising departmental ICT resources will be required to comply with this directive and cooperate with the implementation process.

Non-compliance with this directive may result in devices being denied access to departmental ICT infrastructure due to security, governance, and operational risk considerations.

7. CONCLUSION

The management of legacy and End-of-Life ICT devices is critical to maintaining a secure, stable, compliant, and efficient ICT environment within the Department. Immediate intervention is required to mitigate growing cybersecurity, operational, and governance risks associated with obsolete technology assets.

Your consideration and approval of the above recommendations will be appreciated.

RECOMMENDED BY:

08/05/2026

MR C SWARTZ **DATE**

DEPUTY DIRECTOR: INFORMATION SYSTEMS

APPROVED/ NOT APPROVED

08/05/2026

MR T.L NDZUBE **DATE**

DIRECTOR: INFORMATION COMMUNICATIONS TECHNOLOGY