KWAZULU-NATAL PROVINCE
EDUCATION
REPUBLIC OF SOUTH AFRICA

DIRECTORATE: IT Services

Private Bag X9137, PIETERMARITZBURG, 3200

Anton Lembede Building, 247 Burger Street, Pietermaritzburg, 3201

Tel: 033 8465104 Fax: 033 8465187

To:

Deputy-Director Generals

Chief Directors

Directors

CES – Circuit Management

Principals of Public Ordinary Schools

Schools Governing Bodies

Users of KZN Department of Education ICT systems, System Administrators, Contractors, Staff, Consultants, Vendors and Service Providers.

KZN CIRCULAR 112 OF 2026

Advisory Note: KZN DoE ICT Security GUIDELINES

1. Purpose

1.1. Every person who uses a Department device, network, system, email account or data must follow ICT Security Policy Guidelines of the department.

1.2. This advice applies to all KZNDOE information systems end-users, including vendors, consultants and any third-party solutions that interact with KZN Education data must also meet these minimum requirements.

1.3. The document also seeks to encourage KZN Schools to develop or review their specific ICT Security Policy for their respective environment and ensure alignment with the minimum guidelines encapsulated in this document.

2. Access to systems and user accounts

2.1. Access must be granted only on a "need-to-know" and "need-to-use" basis, and only through a formal, approved request.

2.2. Request must follow a documented and formal process which must be approved by a designated person(s) before processing.

2.3. A unique user ID must be assigned to each employee accessing government application systems. The employee assigned with the username must be accountable for everything done under the assigned user ID.

2.4. Use multi-factor authentication wherever possible must be enabled for all government applications systems.

2.5. Any change in roles and functions, access is adjusted immediately and documented.

2.6. Any employment termination must be documented and access to application system(s) be revoked at the end of the contract term.

2.7. Workstations must be set up with basic user access. Local administrator rights are not automatic, not even for IT staff.

2.8. User Account management process must be documented and approved by the designated person(s).

2.9. User accounts must be reviewed at least quarterly, and evidence kept.

3. Passwords

3.1. Your password is confidential information: never give, tell or hint at it to anyone — including IT staff, managers, colleagues or family. At a minimum seek to achieve the following:

Rule	Requirement
Minimum length	8 characters.
Complexity	At least 3 of: upper case, lower case, numbers, special characters.
Change frequency	At least every 30 days (maximum age 1 month).
First logon	Change the issued password immediately.
Lockout	Account locks after 3 incorrect attempts.
Avoid	Personal information, well-known facts, dictionary words.

3.2. Do not write passwords down unless kept in a locked safe or an encrypted file.Do not send passwords by email or over the internet unprotected.

3.3. Do not use the "Remember Password" feature, especially on laptops.

3.4. Do not reuse your official password on personal accounts, or personal passwords on Department systems.

3.5. Password resets must follow an approved documented process and signed by designated official(s).

3.6. If you suspect your password is compromised, report it to IT Services or designated IT Administrator (for Schools) and have it change immediately.

3.7. Avoid common names when creating a password.

4. Workstations, Laptops, Server and Local Area Network Devices Operating Systems.

4.1. All devices must run on supported Operating Systems, where not possible, due care must be done to minimum any risk exposure of running unsupported operating system.

4.2. A review must be scheduled to assess whether all devices are on supported operating systems and documented.

4.3. Rename default administrator account where possible or create new unique administrator(s) account and disable the default one.

4.4. Implement disks encryption using appropriate tools i.e. Bitlocker for Windows.

5. Department Email and internet.

5.1. Ensure that you read and sign the Internet and Email Acceptable Use agreements.

5.2. **You may not use Department email or internet for:**

5.2.1. Illegal activity, harassment, defamation, intimidation, discrimination, fraud or copyright infringement.

5.2.2. Pornographic, sexually explicit, racist or offensive material.

5.2.3. Gaming, competitive commercial activity, chain letters or mass unsolicited mailings.

5.2.4. Large personal downloads or uploads, or peer-to-peer networks without management approval.

5.2.5. Hacking, impersonating others, or accessing someone else's mailbox or files.

5.2.6. Installing or downloading unlicensed or unauthorised software.

5.3. **Good practice:**

5.3.1. Keep personal use limited and reasonable.

5.3.2. Check your Department mailbox regularly — official communication is sent by email.

5.3.3. Emails to the whole Department need your manager's approval and are circulated via the IT helpdesk.

5.3.4. Send large files as a link to a shared location, not as attachments.

5.3.5. Take care with "Reply All"; never send anything you would not want made public.

5.3.6. Report offensive emails to designated person(s).

5.3.7. Your email access ends when you leave the Department.

5.3.8. **Instant messaging** - the Department has no official IM tool. Never send confidential, personal, salary, employment or supplier information over IM. Truly sensitive matters go by encrypted email or in person.

6. Malware protection and software

6.1. Only approved software may be installed. Always use the standard anti-virus software provided by KZN Education and never disable or bypass it.

6.2. Do not open attachments, files or macros from unknown or suspicious senders. Executable (.exe) attachments are blocked.

6.3. Do not click email links to unknown websites — they may hide malicious programs.

6.4. Scan portable drives before use and check downloaded files for viruses.

6.5. When deleting a suspected virus email, also empty it from your Deleted Items folder.

6.6. Do not forward virus warnings to colleagues; report them to IT Services, who will alert users if a threat is real.

6.7. Creating or spreading malicious programs is strictly prohibited.

7. Laptops, USBs and removable media

7.1. You are personally responsible for the security of any Department laptop or desktop issued to you, whether on site, at home or travelling.

7.2. **Laptops**

7.2.1. Update your endpoint protection before travelling or spending long periods out of the office.

7.2.2. At airports: never leave the laptop unattended, never check it in as luggage, and watch it through security scanners.

7.2.3. In cars: lock the car and keep the laptop out of sight.

7.2.4. Use the security (Kensington) cable where supplied, especially in open-plan offices.

7.2.5. Store work files in the designated, backed-up repository — not only on the laptop.

7.2.6. **Loss or theft:** report immediately to your respective IT and Asset Management and complete a security breach form. You may be held responsible.

7.3. **USBs and removable media.**

7.3.1. Passwords and confidential data stored temporarily on removable media must be encrypted.

7.3.2. Removable media may be quarantined and scanned before use.

7.3.3. Do not modify Department hardware or software — including USB port settings — without IT Services' approval.

7.3.4. Remove data from devices using approved procedures once it is no longer needed.

8. Handling information, POPIA and clear desk

8.1. All employees must comply with the Protection of Personal Information Act (POPIA) and handle information according to its classification.

8.2. Know the classification of the information you handle (e.g. public, confidential, secret) and mark classified documents clearly.

8.3. Only staff with the right security clearance may access classified information.

8.4. Never send confidential information in unencrypted form, by email or any other channel.

8.5. Collect personal information only for a specific, lawful purpose, with consent, and tell people how it will be used.

8.6. Do not use real personal or confidential data for system testing.

8.7. Do not discuss confidential matters in public places, meeting rooms or open areas where you may be overheard.

8.8. You will sign a confidentiality or non-disclosure agreement before receiving access to Department information.

8.9. **Clear desk and clear screen.**

8.10. Lock your workstation or log off whenever you leave it unattended.

8.11. Lock away sensitive papers and storage media when not in use, especially when leaving the office.

8.12. Collect printouts promptly; use the PIN release on printers where available.

9. Physical security and equipment

9.1. Department equipment may not leave its assigned site without approval recorded through Asset Management.

9.2. Do not use cameras or recording devices, including phone cameras, in server rooms or IT facilities unless authorised.

9.3. No eating, drinking or smoking in server rooms and IT facilities.

9.4. Do not leave equipment or media unattended in public places.

9.5. Equipment sent for repair must have sensitive data removed or the repairer cleared first.

9.6. Old IT equipment must be disposed of through the approved Asset Disposal Policy, with data securely wiped.

10. Reporting incidents

10.1. Report any security incident or suspicious activity to the IT Helpdesk immediately — early reporting limits the damage.

10.2. **Report things like:**

10.2.1. A suspected virus or infected computer.

10.2.2. A lost, stolen or damaged laptop or device.

10.2.3. A compromised or shared password.

10.2.4. Suspicious emails, unusual system activity or software malfunctions.

10.2.5. A breach or suspected breach of personal or confidential data.

10.2.6. Physical security breaches or misuse of email and internet.

10.3. **What to do:**

10.3.1. Stop using the affected device or account, and do not try to remove a virus yourself.

10.3.2. Log the incident with the IT Helpdesk or contracted provider.

10.3.3. Give the details: what happened, when, the virus name if known, and who may have received infected material.

10.3.4. Follow IT Services' instructions — an infected computer stays off the network until cleared.

11. Third parties, contractors and IT staff

11.1. Contractors, vendors and service providers are bound by the same rules as employees, plus their contract and SLA.

11.2. Sign a confidentiality or non-disclosure agreement before receiving any access.

11.3. Remote access to the internal network is through the Department's VPN only, using a third-party access request form with full justification submitted to IT Services. Allow about 2 days for approval.

11.4. Firewall changes require a change request form with justification; approval is not guaranteed.

11.5. Suppliers handling Department information will receive security awareness training and may be audited.

11.6. **IT and administrative staff** must follow change management for every system change, keep privileged accounts separate from everyday accounts, and expect administrator activity to be reviewed at least monthly.

12. Consequences of non-compliance

12.1. Any failure to follow the policy is treated as misconduct or breach of contract and assessed by severity. Consequences may include:

12.2. Temporary or permanent revocation of access to systems and ICT services.

12.3. Disciplinary action under the Department's Disciplinary and Labour Relations policies.

12.4. Punitive recourse against service providers under their SLA.

12.5. Legal action under applicable laws.

12.6. The contents of this circular must be circulated to all those affected.

MR G.N NGCOBO
HEAD OF DEPARTMENT
KZN EDUCATION

9/11/26
DATE