



SUB-DIRECTORATE: SECURITY SERVICES

90 Long Street, Kimberley, Northern Cape, South Africa, 8300, Tel: (053) 807 7300,

E-mail: sthibela@ncpg.gov.za , web: www.agrinc.gov.za

Date:	07 July 2025	File:	H2.10.3
To	Acting Head of Department: ADV TI Binase	From	Security Services
CIRCULAR: GUIDELINES FOR THE HANDLING, PROTECTION AND AUTHORISED USE OF DEPARTMENT-ISSUED LAPTOPS			

This circular guide is aimed at all staff members to understand their responsibilities regarding the secure use, handling, protection and authorisation of departmental laptops. These devices often contain sensitive or confidential information critical to the operations of the department.

Below guidelines outlines preventative measures for secure laptop handling, for both on and off departmental premises, introduces a formal permission protocol for remote use and establishes clear consequences for negligence or misuse.

1. Proper Handling of Laptops — Office and Offsite

All officials entrusted with department-issued laptops must take personal responsibility for the secure handling of the device:

Within Office Premise

- a) Laptops must be stored in lockable drawers when not in use.
- b) Devices must be password-protected, encrypted and accessible only by the designated official.
- c) Officials must lock screens when stepping away, even briefly.

When Transported Outside the Office

- a) Officials are permitted to carry laptops only between the office and their place of residence for approved work-from-home purposes.
- b) Laptops must not be taken on personal errands, including shopping, dining out, or visits to public venues.
- c) Use of public Wi-Fi is strictly prohibited; officials must connect via secure, password-protected networks only.
- d) Laptops should be carried in appropriate, protective laptop bags and never left unattended in vehicles.

2. Permission for Remote Use

Officials who require their laptop for home use must:

- a) Submit a written motivation to their supervisor, stating the purpose, work to be performed, and estimated duration if not permanently allocated.
- b) Sign an undertaking of responsibility for the device while offsite.

- c) Secure written approval from the relevant director or delegated authority before removing the device from departmental premises.

3. Consequences of Negligence

Any official who:

- a) Removes a laptop from departmental premises without approval,
- b) Take a departmental laptop to an unauthorized location,
- c) Failed to follow the approved transport route from office to home,
- d) Or shown negligence that results in loss, theft, or damage

...will be held **personally liable**. Such incidents will be formally investigated and may lead to disciplinary action, recovery of costs and suspension of ICT asset privileges.

This circular seeks to promote operational discipline, reduce preventable losses, and enhance digital asset accountability across the department. Cooperation of all staff is essential in maintaining the integrity of our digital infrastructure and ensuring that public resources are protected.


.....
ADV TI BINASE
ACTING HEAD OF DEPARTMENT


.....
DATE