Province of the
EASTERN CAPE
SOCIAL DEVELOPMENT

ICT Equipment Policy

Department of Social Development

Policy Registration 2026-08

TABLE OF CONTENTS

TABLE OF CONTENTS

TERMS AND DEFINITIONS

Terms	Definition
Apps	Software applications that are installed on the devices
Electronic Communications	Any communication transmitted via email, fax, telephone, or the internet.
Encrypted	Information that has been converted into a coded form so that only authorized people can read it.
End User	The person utilising the information.
Executive Management	Executive management, often termed upper management, constitutes the highest level of leadership (CEO, CFO, DDG, Chief directors and some Directors) responsible for defining an Department's strategy, setting long-term goals, and making high-stakes decisions.
Find My Device	Feature on a mobile device to locate lost or stolen devices.
Information Assets	Identifiable data resources, repositories, and knowledge management channels — encompassing physical paper records, digital client databases, operational software, and intellectual property — that are essential for departmental decision-making and statutory continuity.
ICT Asset	Any tangible component (such as laptops, mobile devices, servers, and network routers) or intangible asset (such as software licences and systemic data packages) within the departmental infrastructure that holds institutional value and is managed throughout its operational lifecycle.
ICT Help/Service Desk	An ICT Help/Service Desk is a support service that provides technical assistance to users who experience problems with computer systems, software, networks, or ICT equipment.
Jailbroken	Jailbreaking refers to the process of removing or bypassing limitations set by the manufacturer or operating system on a device, such as mobile device. This allows users to install unauthorised software, access system features not typically available and modify device behaviour.
One Drive	Microsoft online cloud storage service (official data storage).
Operating System	An Operating System (OS) is system software that manages computer hardware and software resources and provides common services for computer programs.
Portable Device	Any device that can easily be carried.
Rooted	A state wherein a user has gained root access (the highest level of permission) on a device running an Android operating system, thereby bypassing administrative restrictions.
Acronyms	
BYOD	Bring Your Own Device
CIO	Chief Information Officer
ECDSD	Department of Social Development
GB	Gigabyte
GITO	Government Information Technology Officer
ICT	Information and Communication Technology
IT	Information Technology

PC	Personal Computer
PDA	Personal Digital Assistant
iOS	iPhone Operating System

LEGISLATIVE FRAMEWORKS

1. Constitution of the Republic of South Africa, 1996 (formerly referred to as Act No. 108 of 1996)
2. Public Finance Management Act, 1999 (Act No. 1 of 1999)
3. Protection of Personal Information Act, 2013 (Act No. 4 of 2013)
4. Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)
5. Protection of Information Act, 1982 (Act No. 84 of 1982)
6. State Information Technology Agency Act, 1998 (Act No. 88 of 1998)
7. Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002)
8. ISO/IEC 27002:2022 (formerly ISO/IEC 17799:2005)
9. Minimum Information Security Standards (MISS), 1996
10. Guidelines for the Handling of Classified Information (SP/2/8/1)

1. PREAMBLE

This policy has been in the implementation since 2020. Upon the review process it has been discovered that most of the controls are still relevant. The rapid development and progress of computer technology and systems networks have escalated threats in respect of information systems security, requiring for the establishment of information management and security policies, standards and control measures to protect the information assets configuration and information against security risks.

The Portable Device Security Policy and ICT Equipment Policy merged into this policy. The backing up of users' data to One Drive was addressed for new developments in the ICT environment. The ECDSD shall ensure that all employees shall be allocated or have access to computing and printing facilities, enabling them to perform their jobs.

2. PURPOSE

The purpose of this policy is to ensure the proper allocation and use of ICT equipment to automate departmental users.

3. OBJECTIVES

a) To provide controls of ICT user equipment.

b) To allocate and manage ICT user equipment.

4. SCOPE OF APPLICABILITY

The scope of this policy is applicable to all employees, contract workers and individuals granted access to departmental systems.

5. PRINCIPLES AND VALUES

a) **Confidentiality:** The Departmental employees shall be ethical and maintain the legal obligation to protect sensitive information.
b) **Integrity:** Employees shall practise honesty, consistency and be ethically firm.
c) **Availability:** The Department shall ensure systems and resources remain accessible.
d) **Accountability:** Department shall ensure employees take responsibility for actions and outcomes.

6. POLICY PROVISIONS

6.1. Minimum Requirements for Allocation of User Equipment

The following requirements shall be met before equipment is allocated to users:

a) The applicant shall be those addressed on the Scope of Applicability.
b) The applicant shall be in possession of a desk that can support the equipment, that provides enough surface area and is not shared with other users.
c) The building shall have adequate number of power sockets and network points for devices allocated.

6.2. Allocation of User Equipment

One computing device and one printing device shall be issued to a user:

a) Requirements for Allocation of a Laptop

Departmental employees that require laptops to perform duties shall be allocated laptops as per their requests.

b) Requirements for Allocation of a Desktop Computer

The Departmental employees that require access to a computer to perform duties and comply with the minimum requirements shall be provided with a desktop computer.

c) Requirements for the Allocation of Printing Devices

i) Printer applications shall be considered if access to a high-capacity multi-functional device is not available.
ii) Printing devices are shared resources and shall be shared with users in the building irrespective of their section units.
iii) ECDSD shall not exceed a ratio of 1 printing device per 5 computers or laptops but shall provide at least 2 printing devices per building.
iv) Institutions are responsible for providing common space where shared printers can be housed.
v) Mobile printers shall be allocated per request and at the discretion of the CIO.
vi) Colour Laser Printers: 1 Colour laser printer shall be allocated per Directorate or District but shall be shared due to the high costs of these devices.

d) Requirements for the Allocation of Scanners

High-capacity scanners shall be provided for employees who are required to scan large quantities of documents daily as needed. Regular counter checks shall be done to ensure that these devices are not underutilised. Scanners shall be redeployed in the event that their utilisation falls below an average of 500 pages per month.

e) **Tablets** shall be allocated as requested and at the discretion of the CIO.

6.3. Bring Your Own Device (BYOD)

a) Employees shall not use their personal notebook and laptop for work, ECDSD prohibits such use of equipment.
b) Employees shall be allowed to bring their own smartphones running the supported or latest Operating System.
c) BYOD tablets including iPad and Android running minimum Operating System noted above shall be allowed.
d) Users shall not download or store confidential ECDSD information on their personal devices or external storage device unless the data can be encrypted.
e) Users unsure about what is permissible to download shall refer to the Information Security Policy or contact the legal section for advice.
f) Devices shall be password protected according to the ECDSD requirements.
g) Rooted (Android) or jailbroken (iOS) smartphones or tablets are strictly forbidden from accessing the ECDSD network.
h) Personal data on BYOD device shall be remotely wiped if:
   i) The device is lost.
   ii) The employee terminates their service of employment.
   iii) ICT detects a data or policy breach.

6.4. Physical Security Controls for Portable Devices

a) The physical security of a portable device shall be the personal responsibility of a user.
b) The user shall keep the portable device in their possession and within sight whenever possible.
c) Employees shall not leave portable devices unattended in the office.
d) The portable device shall be locked away when not in use.
e) The portable device shall be carried and stored in a padded portable computer bag.
f) Employees shall keep a note of the ECDSD asset label containing the make, model, and serial number of the portable device.

6.5. Virus Protection

a) ECDSD ICT equipment anti-virus shall be updated to prevent threat of viruses.
b) The end-user shall log on to ECDSD network for automatic update processes to run.
c) Files from various sources shall be scanned before downloading to devices.
d) Employees shall report security incidents to the ICT Help/Service Desk to minimise the damage.
e) When employees receive virus warning messages, they shall contact the ICT Help/Service Desk.
f) The user shall scan the system for viruses before sending files outside ECDSD.

6.6. Controls Against Unauthorised Access

a) Employees shall use approved encryption software on corporate portable devices.
b) The user shall be personally accountable for network and systems access under their user ID.
c) Employees shall not allow devices to be used by family and friends.
d) The devices shall be shut down or have password-protected screensaver when not in use.
e) Tablets shall have authorised security keys and shall be activated with Find My Device.
f) Jail breaking of tablets shall be forbidden and tablets shall come with authorised Apps.
g) When employees have an App that needs to be installed for work, they shall submit an approved memo to ICT for installation.

6.7. Unauthorised Software

Download and installation of unauthorised software programs shall be prohibited.

6.8. Unlicensed Software Media

a) Installation of unlicensed software on departmental workstations shall be prohibited.
b) Departmental employees shall be prosecuted for infringing software copyright.

6.9. Backups

a) Employees shall backup data on their devices.
b) Employees shall ensure their devices are synchronised with One Drive as network backup storage.
c) When users are unable to access the network, they shall be responsible for offline backups to external devices.
d) When a device is stolen, lost, damaged, or malfunctions, it shall be impossible to retrieve the data from the device.

6.10. Inappropriate Materials

a) Employees shall be prohibited from using departmental workstations or resources to view and store illicit material.
b) ECDSD shall not tolerate inappropriate material that might cause offence.
c) ICT staff shall track internet use and monitor the network and systems.

6.11. Warranty Management

a) User equipment including computers, laptops, printing devices and scanners shall be bought with a minimum of 3-year onsite warranties.
b) Tablets shall be bought with minimum of 2-year onsite warranties.
c) All networking and data centre equipment shall be bought with a minimum of 5-year onsite warranties.
d) To minimise the risk and of costs associated with hardware support, all equipment has to be replaced as soon as possible after the warranty expires.

e) A register should be kept of the warranty status of all ICT equipment, it should include but is not limited to the following information: Order No, Serial Number, Barcode, Warrant End Date etc.

f) After warranty has expired, the equipment shall be evaluated to check if it can still be usable.

6.12. Replacement Cycle for ICT equipment

Obsolete ICT equipment has rising operating costs that unnecessarily increase overheads while hampering business innovation and flexibility. In most cases, ICT equipment becomes technologically obsolete before it fails mechanically. This obsolescence manifests itself in direct and subtle ways (e.g. escalating IT support requirements and incompatibilities with current software).

The following replacement cycles shall be enforced by the department:

a) All user equipment including computers, laptops and printing devices shall be replaced after a minimum of 3 years.

b) All scanners, networking and data centre equipment shall be replaced after a minimum of 5 years.

6.13. Loss and Repairs of Damaged ICT equipment

a) When ICT equipment is lost or stolen, users shall notify the police and inform ICT and Supply Chain within 24-hours.

b) When ICT equipment is damaged, ICT shall assess damage and provide Supply Chain with information on repairs as requested.

c) When ICT equipment is lost, stolen, dropped or knocked due negligence, users shall be liable.

7. APPROVING AUTHORITY

The Member of the Executive Council has the responsibility to approve the ICT Equipment Policy.

8. ACCOUNTABILITIES AND RESPONSIBILITIES

8.1. The Chief Information Officer

The CIO shall implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.

8.2. Supply Chain Management

The Supply Chain Management Asset Unit shall take sole responsibility for departmental assets allocated on their jurisdiction.

8.3. ICT Operations

The ICT Operation shall be responsible for the maintenance of ICT equipment.

8.4. District Management / Asset Management

a) Asset Management and ICT shall allocate assets based on priority lists to ensure equitable, needs based distribution according to asset register.

b) ICT Governance shall be responsible for running awareness sessions on ICT policies and cyber security.

8.5. The Head of the Department

The Head of Department of the ECDSD in conjunction with the ICT Head shall implement, enforce and monitor the controls in accordance with the requirements outlined by management.

8.6. The Member of the Executive Council

The member of the Executive Council shall be responsible for the approval of this policy.

9. EFFECTIVE DATE OF THE POLICY

This policy shall be implemented from its effective date approval.

10. MONITORING MECHANISMS

The CIO and senior management shall be required to ensure ICT Operational Committee, ICT Steering Committee and Risk committee exist to monitor and measure compliance with this policy.

11. ENFORCEMENT

a) Failure to comply with this policy shall result in disciplinary action, which shall include termination of employment.
b) Any conduct that interferes with the normal and proper operation of the departments ICT systems, shall constitute violation of approved ICT Equipment Policy.
c) The Department executive management reserves the right to revoke the privileges of users.

12. POLICY REVIEW

The policy shall be reviewed after three years (3) and whenever there are new developments or legislation change.

13. POLICY RECOMMENDATIONS AND APPROVAL

RECOMMENDED/NOT RECOMMENDED

MR M. MACHEMBA
HEAD OF DEPARTMENT
EASTERN CAPE DEPARTMENT OF SOCIAL DEVELOPMENT
DATE: 08/05/2026

APPROVED/NOT APPROVED

MS B. FANTA
MEMBER OF THE EXECUTIVE COUNCIL
EASTERN CAPE DEPARTMENT OF SOCIAL DEVELOPMENT
DATE: 18/08/2026

Annexure A

Process flow diagram

This is to be developed in our SOPs and shall be maintained on an annual basis.