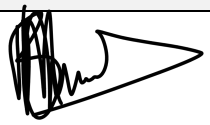
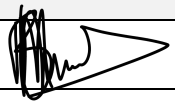
WHOLESALE & RETAIL SETA
Mobile Device Policy

Policy Reference Number	POL_IT_006
First Approved	30/05/2019
Current Version Number	V2.0
Effective Date of Current Version	
Department	Information and Communications Technology
Policy Owner	
Designation	**Signature**
Information, Communication and Technology Executive	
Policy Sponsor	
Designation	**Signature**
Chief Executive Officer (Acting CEO)	

Document Control Page											
Document Title	Mobile Device Policy										
Digital Name	POL_IT_006										
Digital Location	HO-Share (I)_QMS										
Department	Information and Communications Technology										
Creation Date & Revision Dates	V0.1: 17/04/2019; V0.2: 22/04/2019; V0.3: 29/04/2019; V0.4: 10/05/2019; V0.5: 15/05/2019: V0.6: 29/05/2019; V1.0: 30/05/2019; V1.1: 17/05/2023; V2.0: 25/05/2023;										
Current Version	**Version**:	V2.0	**Status**	Approved							
Password Protected	Indicate with X			Yes	**X**	No					
Distribution	All W&RSETA Employees										
Security Classification **Indicate with X**	Restricted	**X**	Confidential		Secret		Top Secret				

Revision	**Version No**	**Revision Date**	**Revision Details**	**Revised by (Dept/Unit)**
Revision frequency: Every 2 years	V0.1	17/04/2019	Drafting of Policy	ICT
	V0.2	22/04/2019	Inputs from CEO; refinement of policy to suit W&RSETA environment	CEO Office
	V0.3	29/04/2019	Presentation to REMCO and amendments	ICT
	V0.4	10/05/2019	Consultation and inputs from Governance and Strategy Committee	ICT
	V0.5	15/05/2019	Consultation with CIO, CEO, ACCO, Board Committee Secretary, Quality Assurance	ICT
	V0.6	29/05/2019	Editing of Policy	QMS
	V1.0	30/05/2019	Approval of Policy	Accounting Authority (AA)
	V1.1	17/05/2023	Review of Policy viz. provision for security, usage and management	ICT
	V2.0	25/05/2023	Approval of Policy	AA

TABLE OF CONTENTS

1 BACKGROUND

1.1 In line with the W&RSETA mandate of developing a skilled, capable, competent and professional workforce; W&RSETA acknowledges the need for its employees to communicate with fellow Provincial offices, partners and stakeholders.

1.2 As a result, W&RSETA requires certain employees to be reachable at all times and to be in a position to communicate through mobile phones, to enable them to carry out their duties effectively and efficiently. When these tools are used correctly, they provide an efficient way of communicating and sharing information.

1.3 The policy will provide guidelines as to the attainment and management of the benefit of a mobile phone allowance, to promote service delivery and ensure that services continue even when employees are not office-bound.

1.4 This policy seeks to provide regulatory standards on how mobile phones must be used by all employees to enhance a high-performance culture.

2 PURPOSE

The purpose of this policy is to:

2.1 Provide guidelines for the payment of mobile phone allowances for W&RSETA employees.

2.2 Efficiently and effectively manage the costs associated with the usage of mobile phones.

2.3 Outline what the W&RSETA should do to protect against threats related to the use of mobile devices.

2.4 Guide in terms of mobile devices which are allowed as tools of trade at the W&RSETA.

2.5 Articulate the governance around the user responsibility, security of network connectivity, mobile device administration and the treatment of insurance and replacements.

3 SCOPE

This policy applies to all W&RSETA employees.

3.1 This policy covers the usage of mobile phone allowances by employees where the regular use of a mobile phone and remote connectivity is necessary to meet the requirements of the job at W&RSETA, at the discretion of the CEO or his/her delegated person.

3.2 These allowances are not part of Total Cost To Company.

4 RELATED INFORMATION AND LEGAL REFERENCE

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the enterprise network.

This policy must be read in conjunction with the following supporting documents:

4.1 *Internal Documents*

a) Human Resource Policies.

4.2 *External Documents*

a) Best Practice on Corporate Mobile Phone Policies.

4.3 Legal Reference

a) Labour Relations Act, No. 66 of 1995, as amended;

b) Public Finance Management Act, No. 29 of 1999, as amended;

c) The Protection of Personal Information (POPI) Act, No. 4 of 2013.

5 ACRONYMS AND DEFINITIONS

Accounting Officer	The Chief Executive Officer (CEO) of the W&RSETA
Employee	Any person, other than an independent contractor, who works for the W&RSETA in conducting the business of the SETA in terms of the Labour Relations Act No. 66 of 1995, as amended
Employer	Wholesale and Retail Sector Education and Training Authority (W&RSETA)
ICT	Information and Communications Technology
Line Manager	The manager to which an employee(s) reports to in a specific department or division
Management	Middle or senior managers at the W&RSETA
Mobile phone	Mobile device with smart capabilities

6 POLICY FUNDAMENTALS

6.1 This policy aims to:

6.1.1 Articulate how mobile computing should be handled at the W&RSETA.

6.1.2 In relation to the above point, an employee's actual working conditions shall determine whether a person may be allocated mobile phone allowances. The level of work in the organisation may not be the determining factor.

6.1.3 Pay mobile phone allowances to employees as determined by assessing an employees' individual needs based on the job specific requirements.

6.2 The principles of this mobile phone policy are as follows:

6.2.1 An approved list of the acceptable mobile devices and platforms must be maintained by the W&RSETA ICT department.

6.2.2 Only mobile devices that run W&RSETA approved platforms must be procured. Similarly, users are only permitted to utilise a user-owned mobile computing device to connect and access W&RSETA resources if the platform on the device is approved by W&RSETA ICT department and is in line with the ICT security standards.

6.2.3 The approved W&RSETA password controls must be implemented to reduce the risk of unauthorised access to the mobile device. Users should avoid sharing their passwords between multiple services/devices. Mobile computing devices must be protected using security policies which comply with the W&RSETA standards. Users cannot change security policies. The policies are applied to both user-owned and W&RSETA-owned devices.

6.2.4 The mobile device users must take due care to ensure that mobile devices are secure at all times, on and off the W&RSETA premises. Mobile devices should not be left unattended in unsecured environments under any circumstances. Whenever possible, mobile devices are to be secured using cable locks or similar controls.

6.2.5 Whenever possible, the data stored on mobile devices should be encrypted.

6.2.6 In addition to the password controls listed in the W&RSETA User Management Standard, wherever possible, mobile computing devices are configured so that if incorrect passwords are entered 10 consecutive times, the contents of the mobile computing device (emails, applications and stored files) are erased.

6.2.7 Mobile computing devices should make use of secure protocols to enable authentication to wireless networks. Such protocols include WPA/WPA2. Strong authentication must be used to login to e-mail, applications and portals.

6.2.8 Communication over the enterprise wireless networks between the mobile device and the wireless access points or a network firewall on the enterprise wireless network must be encrypted.

6.2.9 Users are not allowed to create hotspots to access data on other mobile devices using their W&RSETA devices.

6.2.10 User-owned mobile computing devices must comply with the W&RSETA configuration standards before allowing the device to connect to or access W&RSETA information resources. Users must confirm in writing that they

comply with the W&RSETA standards before the device is granted access to W&RSETA resources.

6.2.11 Mobile device users must password lock their mobile computing devices whenever not using them.

6.2.12 Mobile device users must not store personal or business-sensitive information (credit card numbers, card PINs, password to applications, confidential reports etc.) in their mobile devices using stored e-mail messages, to-do lists, notes, etc. If they wish to save such information, they should use the built-in applications like Keychain, Password Manager, Secure folder etc.

6.2.13 Mobile device users must back-up and then wipe their mobile device before handing it over for support by external parties so that sensitive information is not inadvertently shared with unauthorised individuals.

6.2.14 Mobile device users must consider the implications on their privacy before enabling location-based services such as Facebook check-ins, Google latitude, Twitter location tagging on tweets, etc.

6.2.15 Mobile device users are urged to only install and use applications from trusted sources on their mobile computing devices. Users will be held responsible for the actions performed by all applications installed on their mobile computing devices.

6.2.16 Mobile device users are not allowed to jailbreak, root or otherwise interfere with the functioning of security systems on the mobile computing devices (e.g. iPad) that they use to access W&RSETA information resources. The restriction applies to both W&RSETA and user-owned devices.

6.2.17 Mobile device users may only use secure personal wireless networks. Such protocols include WPA/WPA2.

6.2.18 When using public access Wi-Fi networks (airports, cafés, etc), mobile device users must be aware that access to any unsecure services (e.g. websites) may compromise the information transmitted.

6.2.19 Mobile device users that have lost their mobile computing device need to immediately activate a remote location procedure. Users may initiate the process themselves or call the W&RSETA helpdesk for assistance in locating the device. If the user cannot locate the mobile device immediately, the device must be considered stolen and the relevant procedures triggered, including remote wipe.

6.2.20 Theft is of high priority, as such, mobile device users must report those cases to W&RSETA immediately and the relevant procedures must be followed. If a mobile computing device is stolen, the user must remotely erase all data on the device to protect the information stored in it and ensure compliance with the W&RSETA policies and standards. Users may initiate the process themselves or call the W&RSETA helpdesk for assistance in wiping the device. Once the wiping is complete, users must immediately contact the mobile service provider

to block the SIM card, report the theft to SAPS and blacklist the device with the mobile service provider.

6.2.21 W&RSETA shall not be responsible for insuring and replacing lost, stolen or damaged mobile phone devices or user-owned computing devices

6.2.22 Mobile devices issued by W&RSETA are insured as part of the W&RSETA comprehensive insurance and replaced if damaged or lost.

6.2.23 The W&RSETA pays mobile phone allowances to employees who regularly use a mobile phone to meet the requirements of the job, following due approval.

6.2.24 The amount of the allowance is determined by assessing an individual's needs concerning the job requirements, and is fully taxable, hence the following identified employees are eligible for a mobile phone allowance with the following limits:

ROLE BAND	MOBILE PHONE ALLOWANCE	DATA ALLOWANCE
F1	R 1 700.00	R 590.00
Chief Officers E2 – E1	R 1 300.00	R 590.00
Executive Managers D5 – D3	R 1 000.00	R 570.00
Line Managers D2 – D1 Board Secretary / CEO's PA	R 800.00	R 540.00
C4 – C3	R 400.00	R 500.00

6.2.25 W&RSETA will pay a taxable allowance, which may be amended from time to time, towards the W&RSETA related mobile phone costs incurred by the individual employee.

6.2.26 This allowance will be paid monthly through the payroll.

6.2.27 The W&RSETA expects the eligible employees to enter into mobile phone contracts with the relevant mobile service provider in their capacity and within the approved allowance limit.

6.2.28 The W&RSETA will only support one mobile phone allowance per employee; W&RSETA reserves the right to remove the employee that does not qualify or no longer qualifies for mobile phone allowances.

6.2.29 The mobile phone allowance must be used for intended purpose i.e. for the device, data and/or connectivity.

6.2.30 If the W&RSETA makes provision for bulk data (Access Point Network — APN) to its employees, the mobile phone allowance shall be used as a subsidy for the employee to obtain a compatible mobile device.

6.2.31 W&RSETA does not accept any liability for claims, charges or disputes between the service provider and the staff member.

6.2.32 Recipients of a mobile phone allowance must notify W&RSETA of the mobile phone number and must continue to maintain the mobile phone rental or air-time/pay-as-you-go contract while in receipt of the allowance.

6.2.33 If the employee exceeds the allocated limit based on the W&RSETA operational requirements, the employee will be reimbursed by the W&RSETA, subject to receipt and approval of an itemised bill by the delegated official.

7 USAGE OUTSIDE OF SOUTH AFRICA

7.1 Employees on approved business trips outside South Africa may claim for;

7.1.1 International roaming; and

7.1.2 Business calls received.

8 INSURANCE AND REPAIRS

8.1 Repairs, loss, theft or replacements are for the individual's account.

9 EXCLUSIONS

None.

10 REQUEST TO DEVIATE FROM POLICY

Requests to deviate from any provision of this policy may be made to the Accounting Authority in writing. The Chief Executive Officer has powers to grant such request in whole or in part or refuse it. Unauthorised deviations may result in disciplinary action.

Policy Approval & Sign-off

1. POLICY INFORMATION

Policy Name	
Policy Reference Number	

2. RECOMMENDATIONS/ ENDORSEMENTS

☑ Recommended ☐ Not Recommended

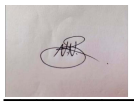
Comments……

……

……

Name of Committee ……..

Committee Chairperson Nonkululeko Bogopa……..



27 June 2023

Signature **Date**

3. APPROVAL BY W&RSETA ACCOUNTING AUTHORITY

☐ Approved ☐ Not Approved

Comments……

……

……

27/06/2023

Reggie Sibiya **Date**

W&RSETA Board Chairperson

Document Name:	POL_IT_006_Mobile Device Policy_V2.0	Next Review Date: 17/05/2025
Version Control	Created: 17/04/2019	
	Approved: 30/05/2019 (V1.0)	
	Reviewed: 17/05/2023	