ICT Bring Your Own Device (BYOD) Policy

Date Approved	Version	Resolution Number
25 April 2018	1	018/OCM/18

The Information Technology Manager

Senqu Local Municipality

19 Murray Street

Lady Grey

Telephone (051) 603 1300

Facsimile (051) 603 0445

Resolution 018/OCM/18	Approved 25 April 2018

ICT Bring Your Own Device Policy

As a government institution, Senqu Municipality needs to keep up with and utilise the advantages offered by new technology. Any new technology also brings about new risks that need to be managed and mitigated by means of relevant Policies.

Full Title	Senqu Municipality's ICT Bring Your Own Device (BYOD) Policy
Short Title	ICT Bring Your Own Device Policy
Author(s)	Mr O. Matiso, Ms M. Oertel
Version	1

Resolution 018/OCM/18	**Approved 25 April 2018**

TABLE OF CONTENTS

1. Version Control

Description of Changes	Version No	Author(s)	Completion Date
Original draft	0.1	Mr O Matiso Ms M Oertel	04/04/2018

2. Definitions

Term	Meaning
BYOD	Bring Your Own Device – This is when a user makes use of his/her privately owned device to access work emails, systems and data.
IT	Information Technology
ICT	Information and Communication Technology
Municipality, the	Senqu Municipality
EC	Eastern Cape
IM	Information Management

Resolution 018/OCM/18	Approved 25 April 2018

3. Introduction

The Municipality recognises the benefits that can be achieved by allowing staff to use their own electronic devices when working, whether that is at the office, home or while travelling. Such devices include laptops, smart phones and tablets, and the practice is commonly known as 'Bring Your Own Device' or BYOD. The Municipality is committed to supporting staff in this practice to ensure that as few technical restrictions as reasonably possible are imposed on accessing information from Municipal servers via own devices.

The use of such devices to create and process municipal information and data creates issues that need to be addressed, particularly in the area of information security.

The Municipality must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empower staff to ensure protection of their own personal information.

4. Purpose

This policy establishes the Municipal guidelines for employee use of personally owned electronic devices for work-related purposes.

5. Scope/Audience

Employees of the Municipality may have the opportunity to use their personal electronic devices for work purposes when authorized in writing, in advance, by the employee and management. Personal electronic devices include personally owned cell phones, smart phones, tablets, laptops and computers.

The use of personal devices is limited to certain employees and may be limited based on compatibility of technology.

6. Information Security Policies

All relevant municipal policies still apply to staff using their own devices to access the Senqu Cloud. Staff should note, in particular, the Municipality's I.T Security related policies. Several of these are directly relevant to staff adopting BYOD.

- Network Access policy
- Privacy policy
- Portable Computing Policy
- Password Policy
- Acceptable Use policy
- Electronic Mail Policy

7. Responsibilities of Staff Members

Individuals who make use of BYOD must take responsibility for their own device and how they use it.

They must take all reasonable steps to:

- Familiarise themselves with their device and its security features so that they can ensure the safety of the Municipality's information (as well as their own information)
- Invoke the relevant security features
- Have a working and regularly updated anti-virus on their personal mobile devices
- Maintain the device themselves ensuring it is regularly patched and upgraded
- Ensure that the device is not used for any purpose that would be at odds with Municipal Policies on the use of Computing Facilities and Resources
- Prevent theft and loss of data
- Keep information confidential where appropriate
- Maintain the integrity of data and information
- Take responsibility for any software they download onto their device

While Municipality's IT staff will always endeavour to assist colleagues wherever possible, the Municipality cannot take responsibility for supporting devices it does not provide.

Staff using BYOD must:

Set up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device.

Set up remote wipe facilities if available and implement a remote wipe if they lose the device.

Encrypt documents or devices as necessary.

8. Access to the Senqu Network

The user needs to apply by completing the necessary Security Access form for BYOD devices and the set-up will be done by the IT Section to ensure that the particular device is recognised.

The relevant Cloudware App will be installed and the Senqu Network may only be accessed via this app, using the employee's own Senqu userid and password.

Users may not hold any Senqu information that is sensitive, personal, confidential or of commercial value on personally owned devices.

This implies that:

- Information belonging to the Municipality may not be copied to, emailed to or backed up on to own devices.
- Employees may not email, transfer or copy municipal-related data to unsecure parties.
- Employees must report any security breach or loss of any own device that was registered on the Municipal database immediately to IT Helpdesk in accordance with the Information Security Policy.

The own device may only be used as a means to securely access services that the Municipality offers over the internet, via the Cloud application.

Due to security issues, personal devices may not be synchronized with other devices in employees' homes.

Be aware of any Data Protection issues and ensure personal data is handled appropriately.

Particular care must be taken if a device is disposed of/sold/transferred to a third party in which case it must first be cleared by Senqu IT and de-registered from the network.

Making any modifications to the device hardware or software beyond authorized and routine installation updates is prohibited unless done by IT.

Non-exempt employees may not use their personal devices for work purposes outside of their normal work schedule without authorization in advance from management.

Employees may not use their personal devices for work purposes during periods of unpaid leave without authorization from management.

The Municipality reserves the right to deactivate the Cloudware application and access on the employee's personal device during periods of unpaid leave.

Family and friends should not use personal devices that are used for work purposes.

Management reserves the right to review or retain personal and Municipality-related data on personal devices or to release the data to government agencies or third parties during an investigation or litigation

IT is not responsible for any repairs of maintenance of any privately owned device.

9. Monitoring and Access

The Municipality will not routinely monitor personal devices. However, it does reserve the right to:

- Prevent access to a particular device from either the wired or wireless networks or both
- Prevent access to a particular system
- Take all necessary and appropriate steps to retrieve information owned by the Municipality
- At any time, monitor and preserve any communications that use the Municipality's networks in any way, including data, Internet use and network traffic, to determine proper use.

No employee may knowingly disable any network software or system identified as a monitoring tool.

In an effort to secure sensitive Municipal data, employees may be required to have "remote-wipe" software installed on their personal devices by the IT department prior to using the devices for work purposes. This software allows for data on the personal device to be erased remotely in the event of the device being lost or stolen. Wiping data from the personal device will affect other applications.

The Municipality will not be responsible for loss or damage of personal applications or data resulting from the wiping of data after a device has been reported as lost or stolen.

Termination of Employment

Upon resignation or termination of employment, or at any time on request, the employee may be asked to produce the personal device for inspection. Any Municipal data or Cloudware links to the Municipality found on personal devices will be removed by IT upon termination of employment.

10. Policy Violation

Violations of this policy may result in disciplinary action, up to and including dismissal for employees, a termination of employment relations in the case of contractors or consultants, dismissal for interns, or suspension.

11. Policy Review

This policy is subject to annual review or whenever it is deemed necessary by the Municipality, to ensure that it is aligned to prevailing resolutions, regulations and market conditions.

12. Publishing the policy

The policy shall be made available and accessible to all employees in electronic format.

13. Senqu Municipality Approval and Sign-Off

The IT Manager accepts responsibility for this Policy. The Municipal Manager will take overall accountability for this Policy.

APPROVAL OF THE POLICY

Date of Approval by Council: 25 July 2018

Resolution Number: **018/OCM/18**

_____ _____

MM YAWA **DATE**

MUNICIPAL MANAGER

Resolution 018/OCM/18	**Approved 25 April 2018**