Enterprise Mobility and Bring-Your-Own-Device Policy

Policy Type	Corporate
Function	Information Management
Policy Owner	Manager Client Services
Policy Contact	ICT Coordinator
Effective Date	23 November 2021

Purpose

To provide a framework for the governance of enterprise mobility and BYOD within Council ensuring they are managed in accordance with relevant legislation, policies, and standards.

Scope

This policy applies to:

- Council-owned mobile devices.
- personally owned mobile devices (BYOD) used for work purposes.
- eligible council employees, contractors, and Councillors.

Exceptions

Nil.

Objectives

The objectives of this policy are to ensure that:

- enterprise mobility and BYOD resources are fit for purpose; and are used appropriately and efficiently to assist Council to deliver quality, value for money services.
- enterprise mobility and BYOD do not create or increase risk to Council, employees, Councillors, contractors or third parties.
- management and use of enterprise mobility and BYOD comply with relevant legislation, policies, and standards.
- enterprise mobility and BYOD are managed with sound consistent governance across Council.

Policy Statement

Council recognises the potential financial and productivity benefits of enterprise mobility in delivering quality, value for money services to our customers and community.

This policy seeks to ensure a consistent approach to the management and use of enterprise mobility and BYOD to ensure it is fit for purpose; to ensure it is used appropriately and efficiently; and to protect Council's information and ICT assets.

Enterprise Mobility

The Council offers eligible officers the ability to access approved Council systems and resources via an authorised mobile device. Eligibility is defined by an officer's job function and must be approved by the officer's supervisor and manager.

The approved business systems and resources may include:

- email.
- contacts.
- calendar.
- tasks.
- other compatible business systems.

Council's enterprise mobility is enabled through Mobile Device Management (MDM) software (App) to be installed on each mobile device.

BYOD

Eligible officers who are approved to use enterprise mobility may choose to do so via an approved[1] personally owned mobile device, which is also referred to as a Bring-Your-Own-Device (BYOD).

Access to the Council's enterprise mobility service via BYOD is an optional service which eligible officers may apply for and is subject to the approval process in the *Approval Process and Access Provisioning* section below.

Remuneration and Support

Council will not meet any costs associated with purchasing and running BYODs unless determined by employment contract or Council resolution. This includes telecommunications service provider charges, device repairs and other operating costs.

The eligible officer agrees to indemnify the Council in respect of any claim arising from loss or damage to the mobile device, except for any loss or damage caused or contributed to by the acts, omissions, or negligence of another Council staff member. Any claim for loss or damage will be considered following the completion of an *Incident Report* and full investigation.

Council's ICT Section will provide support solely for the MDM application deployed as part of the enterprise mobility service.

Approval Process and Access Provisioning

Use of BYODs with the Council's enterprise mobility service must be approved by the eligible officer's manager.

A signed *BYOD User Declaration* (see *Appendix A - BYOD User Declaration*) must be submitted to the Council to request the device be added to the enterprise mobility access list and to allow installation of the MDM application. This is referred to as the provisioning process.

Device Wipe

The Council will wipe all Council information from a BYOD if any of the following events occur:

- a breach of this policy or the *BYOD User Declaration*.
- the BYOD is reported as being lost or stolen.
- ten (10) incorrect password attempts to access the secure container.
- the eligible officer no longer requires access to the Council's enterprise mobility service. For example, when an officer leaves the Council, changes roles, takes extended leave or becomes unfit for duty, or the eligible officer replaces their mobile device).

The Council does not accept any liability for loss or damage to any personal data stored on a BYOD during the wiping process.

[1] Refer to the *Approved Mobile Devices* section in this document

Approved Mobile Devices

The devices approved for Council's enterprise mobility and BYOD use will be determined by the ICT Steering Committee in line with Council' information security obligations.

Approved devices are currently limited to the following:

- Android Smartphones and Tablets.
- Apple iPhones and iPads

The device's operating system (OS) must be maintained at a version supported by the developer. ***Note:*** *At the time of writing this policy the supported operating systems are version 8 (Oreo) or higher*[2] *for Android Smartphones and Tablets, iOS 12 or higher*[3] *for iPhones and iPadOS 13 or higher*[4] *for iPads.*

Appropriate Use and Security Settings

The user of the Council's enterprise mobility service must comply with the following standards:

- use must be in accordance with Council's policies and operational standards. Specifically, the *Information Security Policy*.
- mobile devices are configured to require a PIN to start up and access the device. The PIN must have a minimum length of four (4) numbers.
- mobile devices must be configured to lock the screen of the device after five (5) minutes of inactivity and instantly with the power button to ensure that it remains in a secured state when not being actively used.
- the mobile device's operating system should be updated as soon as is practical after receiving notification of an update or immediately upon receipt of such a request from Council's ICT Section.
- Council data must not be stored on a mobile device outside of the secure container or secure storage enabled via the MDM application.
- reasonable efforts must be taken to protect mobile devices from theft, damage, unauthorised access, and modification.
- reasonable efforts must be taken to prevent unauthorised viewing of Council information accessible via the mobile device.
- the user must notify their Supervisor and the ICT Coordinator within a maximum of 24 hours if a provisioned mobile device is lost or stolen.
- accept and install MDM policy updates whenever they are pushed to the mobile devices.
- the configuration of a mobile device must not be modified to circumvent any security measures imposed by the device's manufacturer, the device's operating system developer, or implemented as part of the Council's enterprise mobility service. This includes 'jailbreaking' the device.

[2] Android version history (https://en.wikipedia.org/wiki/Android_version_history)
[3] Apple iPhone User Guide (https://support.apple.com/en-au/guide/iphone/welcome/ios)
[4] Apple iPad User Guide (https://support.apple.com/en-au/guide/ipad/welcome/ipados)

Risk Management

The policy supports Council's strong commitment to transparency, accountability, and adherence to the governance framework.

The policy mitigates the risk of inappropriate use of enterprise mobility and BYOD within Council.

Legislation

Information Privacy Act 2009

Local Government Act 2009

Public Records Act 2002

Definitions and Abbreviations

BYOD acronym for Bring-Your-Own-Device and refers to employees using their personal mobile devices for work.

Council means Burdekin Shire Council.

Eligible Officers refers to any Council employee, contractor, or Councillor with an identified and approved business requirement for enterprise mobility to fulfil their duties.

Enterprise Mobility refers to the use of a variety of applications and mobile devices, such as smartphones and tablets, for business purposes to allow employees to perform some or all their duties from anywhere at any time.

Jailbreaking a jargon expression or term used for the process of exploiting security vulnerabilities on a mobile device to bypass restrictions put in place by the manufacturer or operating system developer to access additional functionality and install unapproved software. Jailbreaking can be in violation of the end user license-agreement for the device and can provide an opening for malware and hackers. Also known as 'rooting' on Android devices.

MDM acronym for Mobile Device Management and refers to security software used to monitor, manage, and secure mobile devices that are deployed across the organisation.

Mobile Device refers to a range of computing devices small enough for a person to hold and operate in their hand. Examples include Smart Phones and tablets.

PIN acronym for Protected Identification Number and refers to a set of personal numbers used to prove positive identification.

Push refers to a system in which data is "pushed" to a user's device rather than "pulled" by the user. In other words, the data transfer is initiated by the server rather than the client.

Related Documents

Reference Number	Document Title
Document Set ID 1068863	Code of Conduct for Workers
ICT-POL-0004	Information Security Policy
ICT-OSD-0009	Mobile Phone Usage Operational Standard
ICT-OSD-0012	User Access Operational Standard

Document History and Version Control

Title of Document	Enterprise Mobility and Bring-Your-Own-Device Policy
Document Reference Number	ICT-POL-0003 Rev 2
Review Schedule	36 months
Council Meeting Date	23 November 2021
Council Resolution Number	1677062

Appendix A - BYOD User Declaration

I have read, understood and agree to use the Council's enterprise mobility service via my BYOD in accordance with the Council's *Enterprise Mobility and BYOD Policy* and the Council's *Code of Conduct for Workers*.

I acknowledge that:

- Council is not accountable for any costs associated with purchasing and running my BYOD unless determined by employment contract or Council resolution.
- I indemnify the Council in respect of any claim arising from loss or damage to my mobile device, except for any loss or damage caused or contributed to by the acts, omissions, or negligence of another Council staff member.
- Council may wipe all Council information from my BYOD in accordance with the Council's *Enterprise Mobility and BYOD Policy* and I indemnify Council of any liability for loss or damage to any personal data stored on my BYOD during the wiping process.
- I am accountable for all actions undertaken using my BYOD to access the Council's enterprise mobility service.
- I understand that my use of the Council's enterprise mobility service is also bound by the terms and conditions defined in the Council's *Code of Conduct for Workers*.

-- --

Employee's Signature Manager's Signature

-- --

Employee's Name Manager's Name

-- --

Position Title Date

Date

Mobile Phone Number:	
Device Make and Model:	
Current Software Version:	
Device Unique Identifiers (Office Use Only)	