

# ONCHAN DISTRICT COMMISSIONERS

# Mobile Device Policy

Policy Date: October 2025 Review Date: October 2028

# Policy and Procedures Mobile Device Policy

#### **Contents**

<b>PUR</b>	RPOSE	3
	OPE	
1.		
2.		
3.	Usage and Responsibilities of Employees	
4.	Loss or Damage of a Mobile Device or SIM Card	
5.	Driving	
6.	Return of Mobile Devices and SIM Cards	
7.	Allocation	
8.	Incoming/Outgoing Communications	
9.	Confidentiality	
10.	Risk Management	
11.	Compliance with Policy	

#### Policy Review - History:

Please be aware that a hard copy of this document may not be the latest available version, which is available in the Authority's document management system, and which supersedes all previous versions.

Those to whom this policy applies are responsible for familiarising themselves periodically with the latest version and for complying with policy requirements at all times.

Effective from:	Replaces:	Originator:	Page X of Y	
23 <sup>rd</sup> August 2021	2005	Chief Executive/Clerk		
Board Ratification:				

History or Most Recent Policy Changes – MUST BE COMPLETED					
Version:	Date:	Change:			
2		Updated Approved by ODC 23/08/21			
3	02/10/25	Updated Approved by ODC 06/10/25			

#### **PURPOSE**

The Authority recognises that the use of mobile devices is an essential part of many employees' roles.

This policy explains how and why Onchan District Commissioners ("the Authority") provides mobile devices and SIM cards, and the expectations and responsibilities of employees who are issued with them.

#### SCOPE

This policy defines:

- Eligibility for allocation of a mobile device and SIM card.
- Types of mobile devices and tariffs.
- Usage and responsibilities of employees.
- Loss or damage of a mobile device or SIM card.
- Driving.
- Return of mobile devices and SIM cards.
- Allocation.
- Incoming/outgoing communications.
- Confidentiality.
- · Risk management.
- · Compliance with policy.

#### 1. Eligibility

The Authority will only provide a mobile device and/or SIM card where there is a clear business need.

# 2. <u>Mobile Devices and Tariffs</u>

The type of mobile device and tariff will be chosen by the Authority based on cost and business needs, not personal preference.

If required, exceptions may be made for employees with a disability.

#### 3. <u>Usage and Responsibilities of Employees</u>

Mobile devices and SIM cards provided by the Authority are to be used strictly for work related purposes.

#### Employees must:

 Take reasonable care of a device or SIM card, and report any loss, theft, or damage immediately to a line manager.

# Policy and Procedures Mobile Device Policy

- Protect it with a password or biometric lock.
- Keep it charged, switched on, and available during working hours.

# Employees must not:

- Use a mobile device or SIM card to make personal calls, texts, or emails.
- Download or install unapproved applications or software.
- Stream music, films, or other personal content.
- Move the SIM card to another device.
- Share confidential information outside of the Authority, or store the Authority's data outside of approved applications.
- Use outside of working hours unless a business need has been identified and approved by a line manager.
- Use off-Island unless a business need has been identified and approved by a line manager.

Failure to comply with the above may result in disciplinary action being taken against an employee.

Audits of mobile devices and invoices may be conducted. Any discrepancies or misuse may result in disciplinary action and reimbursement of any costs owed to the Authority.

### 4. Loss or Damage of a Mobile Device or SIM Card

If a mobile device or SIM card is lost or damaged, it must be reported to a line manager as soon as possible.

The Chief Executive/Clerk, the Deputy Clerk, or the Chief Finance Officer must also be informed so the account can be deactivated if required.

If a mobile device or SIM card is lost or damaged through negligence, an employee may be asked to pay for a replacement.

#### 5. Driving

It is illegal to use a mobile device when driving. An employee must stop a vehicle at a safe location before using any mobile device.

Employees are responsible for any fine or other penalty incurred for any breach of the law whilst driving.

#### 6. Return of Mobile Devices and SIM Cards

Mobile devices and SIM cards remain the property of the Authority at all times and must be surrendered when an employee leaves the employment of the Authority or on demand by the Chief Executive/Clerk or the Deputy Clerk.

Failure to return a mobile device or SIM card may lead to charges being deducted from an employee to cover rental or recovery costs.

#### 7. Allocation

Mobile devices and SIM cards cannot be reallocated between employees unless authorised by the Chief Executive/Clerk, the Deputy Clerk, or the Chief Finance Officer.

#### 8. <u>Incoming/Outgoing Communications</u>

Any incoming or outgoing communication is potentially the first point of contact between the Authority and members of the public.

When communicating, employees must aim to be polite, informative, and helpful.

#### 9. Confidentiality

All information relating to the Authority's business is confidential. Employees must treat any electronic information with the utmost care.

#### 10. Risk Management

Employees have a right to work in a safe environment free from aggressive or threatening behaviour.

Particular care must be taken by employees when communicating on a mobile device, as all expressions of fact, intention, and opinion may bind an employee and/or the Authority, and can be produced in court.

#### 11. Compliance with Policy

Failure to comply with this policy may result in disciplinary action being taken against an employee.