Use of Starlink Services in Community Centres for Disaster Management

Policy Type	Adminstrative Policy	Version:	1.0
Responsible Officer	Senior Executive Support Officer	Date Approved:	18/11/2026
Review Officer:	Chief Executive Officer	Review Due:	18/10/2028
Author:	Senior Executive Support Officer	Commencement:	18/11/2026

1. PURPOSE

This policy establishes the requirements for the deployment, operation, maintenance, and governance of Starlink satellite internet services within community centres to support disaster management, emergency response, business continuity, and community resilience.

The objective of this policy is to ensure that community centres can maintain essential communications and connectivity during emergencies, particularly when conventional telecommunications infrastructure is disrupted, degraded or unavailable.

2. SCOPE

This policy applies to all employees, contractors, volunteers, emergency services personnel, and other authorised persons involved in the deployment, operation, management or use of Starlink satellite internet services at community centres.

This policy also applies to the general public who access the WiFi within community centres activated for disaster response.

All persons within scope are responsible for using Starlink services appropriately, safely and in accordance with relevant organisational policies, procedures and directions.

3. POLICY STATEMENT

The organisation recognises that reliable communications are critical to effective disaster management and emergency response. This includes, but is not limited to:

- Cyclones
- Floods
- Bushfires
- Severe storms
- Telecommunications outages
- Public health emergencies
- Other declared disasters or emergency events

Starlink services may be deployed at designated community centres to provide resilient communications capability where conventional telecommunications services are unavailable, disrupted or degraded.

Starlink services shall be used to support authorised emergency management activities, including emergency communications, public information dissemination, coordination of relief activities, business continuity and community welfare services.

Access to and use of Starlink services shall be managed in accordance with this policy and any applicable emergency management, information security, and privacy requirements.

4. REPORTING

The organisation shall maintain appropriate records of Starlink activation and use for disaster management and emergency response purposes.

Significant service disruptions, failures, unauthorised use, security or privacy incidents, or damage affecting Starlink services shall be reported through established organisational reporting processes.

Following significant emergency activations, the responsible business area shall review the effectiveness of the service and identify any lessons learned or improvements required.

5. ROLES AND RESPONSIBILITIES

Role	Key responsibilities
Chief Executive Officer (CEO)	• Provides overall governance and accountability for the policy • Ensures appropriate organisational support and resources.
Disaster Management Officer	• Coordinates the deployment, activation and use of Starlink services for disaster and emergency management purposes • Coordinates with community centre managers and relevant stakeholders • Monitors use and effectiveness • Coordinates post-event reviews
IT Team	• Provides technical advice or assistance when requested, including troubleshooting connectivity or technical issues
Community Centre Managers	• Support the local deployment and use of Starlink • Ensure authorised access • Coordinate local use during emergencies • Report issues or incidents to the Disaster Management Officer
Employees and Volunteers	• Use Starlink services appropriately and in accordance with this policy and any directions provided during an emergency • Report issues or inappropriate use
Authorised Users	• Use Starlink for approved purposes, prioritise critical communications when directed • Report any service or security issues
Other public users	• Use Starlink services appropriately and in accordance with this policy and any directions provided during an emergency • All users will be deemed to accept the terms and conditions defined in Council's *Public Internet Terms and Conditions*, as published on Council's website • Report issues or inappropriate use

6. CYBERSECURITY, PRIVACY AND CONFIDENTIALITY

Starlink services must be used in accordance with the organisation's cybersecurity, privacy, confidentiality, acceptable-use and information management requirements.

Access must be limited to authorised users, and sensitive, confidential and personal information must be appropriately protected. Users must not disclose, access or transmit information inappropriately when using Starlink services.

Personal information collected during disaster operations shall only be used for authorised emergency management purposes.

Any suspected cybersecurity incident, privacy breach, unauthorised access or misuse must be reported through established organisational processes.

Records created or received through the use of Starlink for disaster management purposes must be managed in accordance with the organisation's records and information management requirements.

7. EQUIPMENT MANAGEMENT

Starlink equipment must be stored, transported and used in a manner that protects it from damage, loss or unauthorised use. Community Centre Managers are responsible for ensuring equipment is appropriately secured and available for authorised emergency use.

Damage, loss, theft or malfunction of Starlink equipment must be reported to the Disaster Management Officer as soon as practicable. The Disaster Management Officer will coordinate any required technical support, repair or replacement.

8. TRAINING AND TESTING

Authorised personnel responsible for the deployment, activation or use of Starlink services must receive appropriate instruction to ensure they understand their responsibilities and can use the service effectively during an emergency.

Starlink services should be tested periodically to confirm connectivity, accessibility and operational readiness. Testing should be coordinated by the Disaster Management Officer, with technical assistance sought where required.

Testing and training activities should be recorded, and any issues identified should be addressed to maintain the readiness and effectiveness of the service.

9. DEFINITIONS

Authorised user – An employee, contractor, volunteer or other person approved to access or use Starlink services in accordance with this policy.

Community centre – A facility designated by the organisation to provide community services and/or support during disaster or emergency events.

Disaster – An event that causes, or threatens to cause, significant disruption to the community and requires a coordinated response.

Emergency activation – The authorised commencement of Starlink services at a community centre in response to a disaster, emergency event or significant telecommunications disruption.

Emergency event – An actual or imminent event requiring action to protect people, property, essential services or community wellbeing.

Starlink services – Satellite internet connectivity provided through the Starlink service and authorised for use under this policy.

10. RELATED DOCUMENTS

Confidentiality Policy (MSC)

Public Internet Terms and Conditions (MSC)

QPP Privacy Policy (MSC)

11. POLICY REVIEW

It is the responsibility of the Chief Executive Officer to monitor the adequacy of this policy and implement and approve appropriate changes. This policy will be formally reviewed every two (2) years or as required by Council.