Somerset
REGIONAL COUNCIL

Policy Subject/Title:	Opt-In Bring Your Own Device (BYOD)
Policy Number:	**C/040**

Responsible Officer:	Director Corporate and Community Services
Related Policies / Procedures:	Information Security Policy
Authorised by:	Somerset Regional Council
Authorised on:	15 November 2023
Amendments:	[Doc Id 1561508]

1. OBJECTIVE

To provide a guideline on the use of non-Council computing or telephony devices for Council purposes.

2. BACKGROUND

Council strives to provide a balance between a secure information management environment and ease of accessibility for end users. Allowing approved staff and contractors to use their own device as a replacement for a Council issued device for limited purposes reduces Council costs and allows greater flexibility for end users.

3. PURPOSE

The purpose of this policy is to inform staff, contractors and volunteers of their obligations when using non-Council devices for Council work purposes, and to ensure security risks and associated controls are clearly defined.

4. SCOPE

This policy applies to all staff, contractors or volunteers (collectively known as 'users') using or wanting to use a non-Council telephony device ('BYOD device') for Council work purposes or wanting to connect that device to Council networks. BYOD devices may also include other devices (eg tablets) as approved by the CEO on a case by case basis.

To remove any doubt, this opt-in policy does not affect contractual arrangements in place prior to the adoption date.

5. POLICY

5.1 Users must uphold Council's mission, vision and values while using a BYOD device for Council work purposes and must abide by all relevant policies as if the device were owned by Council, particularly with reference to confidentiality and information privacy.

5.2 Users will not be entitled to receive any additional benefit, monetary or otherwise from Council for using a BYOD device under this opt-in policy.

5.3 Users are responsible for backing up data on their BYOD device. Non-Council data is not to be stored or backed up on Council networks.

5.4 Users are required to remove all Council-related material and accounts from their BYOD device upon separation from Council.

5.5 The only Council services that BYOD devices are permitted to connect to are publicly accessible Council services, the Council email system, Council guest wireless network, and other Council supported Apps as approved by the CEO (E.G. Skytrust, NAB Flexi Purchase).

5.6 BYOD devices are required to be protected by a PIN and/or password.

5.7 Lost or stolen BYOD devices must be reported to Council ICT staff within 24 hours of loss.

5.8 In the case of a suspected security breach, Council reserves the right to do one or more of the following without notification:

- disconnect BYOD devices from the Council network and/or disable BYOD services;

- remotely remove, modify and/or otherwise destroy all Council accounts and data from BYOD devices;

5.9 Council will not be responsible for diagnosing issues or providing technical or billing support for any BYOD device outside of work-related applications.

5.10 Approval to utilise BYOD devices will be at the discretion of the Chief Executive Officer, with specific devices proposed for use requiring the approval of the ICT Coordinator to ensure that these meet minimum security requirements.

6. DATE OF RESOLUTION

This policy was approved by the Chief Executive Office and adopted by the Somerset Regional Council at the Ordinary Meeting of 15 November 2023.

Signed:  Date: 15 November 2023