OBERON COUNCIL

POLICY 2141

BRING YOUR OWN DEVICE POLICY

1. Overview

The purpose of this policy is twofold. Firstly, it aims to allow you to 'bring your own device' (BYOD) for business purposes. If your device is registered as a BYOD, you will be able to access Oberon Council's programs when and where you need to do so. Secondly, the policy aims to ensure that Oberon Council's systems and data are protected from unauthorised access, use or disclosure.

This document sets out the terms of use for BYOD within Oberon Council. The policy applies to all employees of Oberon Council, including permanent and temporary staff, contractors and employees of Oberon Council's partner organisations.

It affects any device or accompanying media that you may use to access the systems and data of Oberon Council, whether they are used within or outside your standard working hours.

2. Purpose

Oberon Council grants its employees the privilege of using their own, authorised devices at work subject to the procedures and requirements set out in this policy.

Oberon Council reserves the right to revoke this privilege if employees do not abide by these policies and procedures. Users may receive an allowance in recognition of the use of their personal device for work related activities.

This policy is intended to protect the security and integrity of Oberon Council's data and technology infrastructure.

Users must agree to the terms and conditions set forth in this policy.

Definitions
Application or App – Computer software designed to assist end users to carry out useful tasks. Examples of applications may include the Microsoft Office suite of products or smartphone applications such as Google Maps.

Bring Your Own Device (BYOD) - Any electronic device owned, leased or operated by an employee or contractor of Oberon Council which is capable of storing data and connecting to a network, including but not limited to mobile phones, smartphones, tablets, laptops, personal computers and net-books.

Data - Any and all information stored or processed through a BYOD. Oberon Council's data refers to data owned, originating from or processed by Oberon Council's systems.

Device hygiene - BYOD must have appropriate and up-to-date 'hygiene' solutions installed. Device hygiene includes anti-virus, anti-spam and anti-spyware solutions.

Minimum requirements - The minimum hardware, software and general operating requirements for a
BYOD.

Mobile Device Management (MDM) – Solution which manages, supports, secures and monitors mobile devices. Oberon Council is currently using Microsoft Intune to manage its mobile devices.

Personal information – 'Personal information' is defined by s 6(1) of the *Privacy and Personal Information Protection Act 1988* (NSW) as 'Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion'.

Wipe – A security feature that renders the data stored on a device inaccessible. Wiping may be performed locally, via an MDM product, or remotely by a network administrator.

3. Procedure

The purpose of this policy is to allow you to use a BYOD if you wish to do so, while also ensuring you take steps to minimise the risk of unauthorised access to Oberon Council's systems or unauthorised use or disclosure of the data held by Oberon Council.

You must review and accept this policy before using any BYOD. Your agreement to the requirements of this policy is indicated by your completion of the BYOD Acceptance Form found on the Oberon Council Intranet.

Acceptance indicates agreement to the following standard terms:

- **Acceptable BYOD:** Any device may be considered for use as a BYOD providing it meets the BYOD minimum requirements. (Set out in a separate document which will change to reflect the changing IT environment).
- **Minimum requirements:** The burden of proof for meeting minimum requirements rests with you, the requestor. The final decision on whether your device meets our requirements is subject to the approval of the IT and GIS Co-ordinator.
- **Matching our requirements and your work needs:** BYOD capabilities and device profiles must match Oberon Council's requirements as well as the scenarios where you need to use a device for work. For example, if you are usually a consumer of information when mobile, the profile of a tablet or smartphone would be a good match. If you are a "creator" of information, a laptop or desktop profile would be a better match.
- **Authority:** You agree to provide limited authority over the device for the sole purpose of protecting Council data and access on the device. This authority includes

permission to wipe the device in the event of loss or disposal. This may include personal data, address books and e-mail depending on the data classification of information locally stored, the device and whether an MDM tool is used. The authority is to remain in place from the time the device is registered until it is de-registered. If your device is not registered in Council's MDM solution, you should also provide your device to the IT and GIS Co-ordinator for a manual check when you cease employment. You may be present at the time the device is manually checked.

- **Security:** You are responsible for ensuring that your personal device is adequately secured against loss, theft or use by persons not authorised to use the device.
- **Support:** You are responsible for replacing, maintaining and arranging technical support for your BYOD. Oberon Council will only provide hardware, operating system, network connectivity or application support for the applications that Oberon Council has provided.
- **Access at Oberon Council's discretion:** Access to Oberon Council's systems and data is provided at the sole discretion of Oberon Council. Your access may be revoked at any time and for any reason.
- **Enforcement:** All breaches of this policy will be treated seriously. If you are found to have been in breach you may be subject to disciplinary action.

4. Device Requirements

Most device types are acceptable for registration on Oberon Council's Bring Your Own Device mobility service, if they are compatible with the MDM platform. You must confirm that your device is acceptable with Oberon Council's IT Co-ordinator. The device model must be capable of loading the latest version of the operating system.
The table below summarises Oberon Council's minimum requirements for a BYOD.

	Function	Minimum requirement
1	Operating systems	Your device must use a legitimate operating system that meets the defined minimum standards (i.e. you may not use a 'jail broken' or 'rooted' device).
2	Network authentication	The minimum network authentication is subject to Oberon Council's requirements..
3	Password protection/ User authentication	Your device will support password authentication and automatic locking that must be used at all times.
4	Automatic device lock	Your device must have the automatic lock enabled.

5	Device hygiene	Your device must have appropriate and up to date 'hygiene' (anti-virus) solutions installed. These may be installed by Oberon Council as part of the BYOD process.
6	Lost and stolen devices	If your device is lost or stolen you must report the loss or theft immediately to the IT and GIS Co-ordinator
7	Mobile device disposal	Any Oberon Council data on your device will be removed from the device at the end of its use within the Council environment.
8	Software licensing	With the exception of programs provided by Oberon Council, the operating systems and applications running on or required by BYOD will be your sole responsibility as the device owner.
9	Mobile device management	Oberon Council will conduct a risk assessment of the nature of services to be offered to mobile devices and specifically to BYOD. Oberon Council is using Microsoft Intune as its MDM platform
10	BYOD authority	If your device is registered and used for BYOD, you agree to surrender limited authority over the device for the sole purpose of protecting council data and access on the device.
11	Mobile device application control	Oberon Council has implemented a MDM solution, which has the ability to push and remove our supplied applications from your device to enhance its security or manageability.
12	Device support	You and the device supplier are responsible for supporting your device.
13	Voice Mail	If you are using your BYOD to receive work related phone calls your voice mail greeting should state your name and position at Oberon Council.

4.1 Device Registration, Configuration and Management

- Your BYOD must be registered before connecting to any Oberon Council internal IT service.
- A limit will apply to the number of devices that can be registered by each person. The device must be registered by connecting to Oberon Council BYOD management service
- You acknowledge that Oberon Council will directly and or remotely change security configurations of the device to protect Oberon Council data and software stored on the device.

  These changes may include but are not limited to:
  - Refusal to register a device that fails minimum requirements (outlined above) or that currently has installed banned software and services.
  - Configuring certain security settings
  - Preventing the user from changing certain security settings

  - Applying a login code with an acceptable level of complexity to enable secure access to the device
  - Automatically locking the device after an inactive time-out period (you will need to re-enter the login code)
  - Installing software and digital certificates necessary to maintain security
  - Encrypting data stored on the device
  - Automatically wiping all Council code and data, depending upon the MDM, device capabilities and specific requirements from the device after a specific number of failed login attempts
  - Should any Oberon Council configurations be removed that are required for proper use of the device with Council systems, these will be re-applied or access to Oberon Council systems, information and data will be prevented if the configurations cannot be maintained.

- You acknowledge that any Oberon Council data stored on the BYOD remains the sole property of Oberon Council and that you have an obligation to protect the security of the data.
- You acknowledge that Oberon Council has a right to inspect Oberon Council data held on your personal BYOD.
- You understand that Oberon Council may remotely monitor your device to ensure security and software configurations are maintained. (Private data will not be accessed).
- You will not be prevented from installing the software or applications of your choice on your device. However, Oberon Council may block your access to Oberon Council internal IT services if any software/applications/data present a threat to Oberon Council IT services, information or data.

4.2 Device Usage, Support and Costs

- The service and its use are at your sole discretion and risk.
- Oberon Council does not impose a charge on you for registering your device.
- You are responsible for supporting your device. Oberon Council will only provide support for the applications Oberon Council has provided. Support responsibility is set out in the following table.

	Support Option	Responsibility
1	Physical provisioning (purchase)	Device owner
2	Repair or replacement of defective/damaged device	Device owner
3	Operating system support including licensing	Device owner
4	Application support of device including licensing	Device owner
5	Council provided/supported mobile applications	Oberon Council IT

6	Council provided/supported thin-client applications	Oberon Council IT
7	Mobile internet	Device owner
8	Home internet / broadband	Device owner
9	VPN client (if applicable)	Oberon Council IT
10	Council WiFi	Oberon Council IT

- Oberon Council is not *responsible* for any costs incurred by your use of your BYOD. That is, Oberon Council will not reimburse voice and/or data costs, software or application acquisition fees, support, repair or insurance costs associated with your device.
- Oberon Council may reimburse voice and/or data costs, but only where the device is used for excessive business requirements. Such costs are claimed as expenses via the expense claim procedure.
- Oberon Council may provide an allowance after approval from your Manager. This allowance only recognises that additional data plan costs may be incurred by you when using your device regularly for work related activities and does not differentiate between high or low usage. It also recognises any phone call and SMS costs that may be incurred during business use. The allowance is only available to staff positions that have a Council issued phone.
- Oberon Council is not responsible for any inconvenience that you may experience in connection with using Oberon Council internal IT services on your BYOD.
- You have sole responsibility for ensuring no other person has access to Oberon Council software or data stored on your BYOD.
- Oberon Council will not monitor the phone call or text message history of a BYOD. Where needed (for example, in the case of a disciplinary matter) the call and text messages may be requested.
- Oberon Council will not monitor the web browser history on your BYOD when not connected to Oberon Council network(s).
- Oberon Council may restrict access to internet websites, services or other elements for operational or policy reasons while your BYOD is connected to Oberon Council networks including either wireless or cabled connections.
- Oberon Council may monitor your use of your BYOD while it is connected to Oberon Council network.
- You are responsible for abiding by all licence terms and conditions applicable to any software, apps, data or information provided by Oberon Council to your BYOD.

  You acknowledge that your use of a BYOD may involve Oberon Council:

  - Preventing you from accessing Oberon Council internal IT services
  - Wiping data and applications or locking your device in accordance with the following circumstances:

- Your BYOD is reported as being lost/stolen to Oberon Council
- You cease employment/contract with Oberon Council and fail to de-register your device
- There is a suspected security breach, examples include but are not limited to, modification of the device's operating system, breaching Oberon Council policies, or detection of viruses or malware on the device
- Should you fail 10 times in a row to enter a correct login password for your BYOD, a full wipe may be performed on the device. IT Staff will contact you before any wipe is performed.

- While Oberon Council will make all reasonable effort to ensure service is available Oberon Council does not guarantee that access to Oberon Council internal IT services, information or data will be available at all times.
- If your BYOD is lost or stolen, you are responsible for reporting the event as soon as practicable to Oberon Council IT Co-ordinator. You must also:
  - undertake a device wipe as soon as practicable via the MDM Portal or via personal configuration utility
  - take reasonable steps to ensure that it is replaced as quickly as possible.
- Oberon Council may also provide you with a loan device so that you are able to carry out your normal work activities.

4.3 Protection of Council data on your BYOD

- Oberon Council information, documents, and data not classified as Public, or that are subject to legal or professional privilege must not be stored on your BYOD and/or unapproved cloud-based services.
- Oberon Council data must only be backed up to approved locations either within council systems or approved cloud service locations or providers.
- You should check your device to ensure that automated cloud backup is disabled.
- You should take reasonable steps to reduce the risk of losing your personal data. You may, for example, store your personal data separately from Oberon Council data through file partitions or using a separate memory card.
- You are responsible for backing up and restoring the data and configuration settings of your BYOD. Personal data is not to be backed up to or stored by Oberon Council. Oberon Council is not responsible for any personal loss or damage you may suffer by actions undertaken by Oberon Council to protect Oberon Council data stored on your BYOD.

4.4 Device de-registration

- Oberon Council at its own discretion, may de-register any BYOD at any time without warning.
- Oberon Council may de-register a BYOD that has not accessed Oberon Council internal IT services for more than six (6) months.
- You can opt-out or de-register your BYOD at any time by visiting the MDM Portal

- You acknowledge that by de-registering your BYOD Oberon Council will remove all Oberon Council data, applications and security controls
- You will no longer be able to connect to Oberon Council internal IT systems and data, unless the device is re-registered.
- You will no longer receive an allowance for the use of your personal device for work activities, if you were receiving an allowance
- You are encouraged to remove any personal data if you are intending to dispose of your BYOD. If you intend to sell or gift the device to another person you should ensure that it is wiped.

5. References

You should also have regard to the following statutory rules, policy documents and standards. They provide direct or related guidance for the use of technology and the collection, storage, access, use and disclosure of data by NSW public agencies:

Workplace Surveillance Act 2005
Government Information (Public Access) Act 2009
Privacy and Personal Information Protection Act 1998

6. Responsibility

It is the responsibility of the IT and GIS Co-ordinator to review this policy every two years and amend as required.

7. Related Documentation

This policy supplements the following Oberon Council policies:

- Use of Internet and Email
- Code of Conduct
- Workplace Surveillance Policy

Approving Authority	Oberon Council
Contact	Director of Corporate Services
Approval	Ordinary Meeting – 20 December 2022): Item 13.02, Minute 17 201222
Revision Date	December 2024
Issue Date to Staff	December 2022