U3A YARRA CITY
UNIVERSITY OF THE THIRD AGE

Data Privacy and Security Policy: Bring Your Own Device

Purpose

U3As using a variety of computer technologies often need to allow members to use their own devices to access, work or store information relevant to the business of that U3A. This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets or storage devices for U3A Yarra City's business purposes. It does not cover the use of U3A Yarra City-owned equipment. Refer to the policy Use of the U3A's IT system for business rules relating to using our U3A's IT system.

Eligibility to access our IT system from a personal device

The following groups of people will have access to aspects of our IT system using their personal device, when required:

- Elected or seconded members of our Committee of Management
- Volunteers appointed to roles in subcommittees or projects
- Contractors that support our IT and telephony systems.

Policy

1. Device owners must take full responsibility for maintaining the security of their equipment by installing and keeping software, virus protection and malware protection regularly updated

2. Strong passwords and multifactor authentication are advised to access data

3. Approved password manager software is encouraged to protect data privacy

4. Any U3A-related personal data stored on personal devices should be maintained in line with agreed guidelines or removed following use

5. Personal devices used to access our U3A's internal (including wifi) networks should be registered

6. Personal devices may be used for the following business purposes:
   - Email access
   - Business internet access
   - Telephone calls and texts
   - Authorised access to MyU3A member database system
   - Preparation of documents for U3A Yarra City use.

Implementation

7. Prior being granted permission to access our IT system using a personal device for U3A business, each person must sign off their agreement to:

   - Not download or transfer business or personal information to the device outside of U3A authorised applications. This information includes intellectual property, volunteer details and financial information
   - Not access confidential information if it can be observed by others
   - Avoid, if possible, using public Wi-Fi hotspots when accessing our IT system. Use home or Network Wi-Fi, private mobile data hotspots or mobile data instead
   - Not leave devices unattended in a public place
   - Turn off Bluetooth if it is not in use
   - Regularly backup the device to a secure place such as a portable hard drive that is kept secure.
   - Carry devices onboard in carry-on baggage if travelling by air
   - Delete U3A-related data from private devices when they are no longer in a relevant role.

This sign off is overseen by the Privacy Officer using the U3A's induction documentation.

Breaches of the policy may result in:

- Loss of access to U3A data systems
- Loss of membership rights

Version 1.1	Data Privacy and Security Policy: Bring Your Own Device
Endorsed by U3A Yarra City Committee of Management	Date: 11/08/2021