Data Privacy and Security Policy: Use of the U3A's IT Network

Purpose

The purpose of this policy is to:

- State the business rules for using U3A Yarra City's IT equipment and related infrastructure
- Identify who holds responsibility for carrying out or endorsing each element
- Ensure data privacy and security is protected through a range of preventative methodologies.

The aspects of our U3A's operations that are covered by this policy are:

- Eligibility to have access to our IT system
- Software considerations
- Who has access to personal data
- Cyber security threats
- Back up of data files
- Equipment disposal
- Training.

This policy does not cover equipment owned by individual committee members, staff or volunteers. Refer to the policy Bring Your Own Devices (BYOD) for business rules relating to using your own device for U3A-related reasons.

This policy does not cover access to the MyU3A membership system, except for reference to access for basic office assistance.

Policy

Access to our IT system

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

- Volunteers appointed to roles in subcommittees or projects will be given access to the relevant aspects of our desktop system including access to the basic functions of MyU3A adequate for assisting with the registration of new members and members' queries.
- Contractors that support our IT and telephony systems.

Software considerations

- Anti-virus software is installed and kept up to date on all owned devices by the Systems Administrator
- Data encryption and multi-factor authorisation is used on all software that enables it
- Software required for data security will be installed and managed by the Systems Administrator
- The Systems Administrator will maintain a register of all purchased office software licenses
- Passwords, PINs and passphrases must not be shared
- Only software authorised by the Systems Administrator will be installed on our U3A's hardware
- The Systems Administrator will ensure that any software no longer required will be removed from our owned devices
- The Systems Administrator will liaise with the Privacy Officer to revoke accounts for anyone who departs the organisation, and arrange for their accounts to be monitored or handed over to another authorised person

Access to Personal Information

- Electronic documents which hold personal information will only be available to people who have been authorised under approved guidelines administered by the Privacy Officer
- Any personal information downloaded by volunteers or committee members must be deleted when no longer required. This is the responsibility of the individual, with assistance from the Systems Administrator
- Personal information must not be downloaded to memory sticks, external hard disks or personal cloud locations, unless encrypted.

Cyber Security Threats

- Any cyber security threats must be immediately reported to the Systems Administrator and to the Committee of Management
- The Systems Administrator will immediately initiate the cyber security incident response plan
- A data privacy and security review will be conducted on an annual basis, in conjunction with our risk management process.

Back Up of Data Files

- Data backups of individual accounts for volunteers and committee members will be managed by the Systems Administrator
- The Systems Administrator will be responsible for regularly backing up key electronic data files
- Backups will be regularly tested by the Systems Administrator to ensure they are able to be restored if the need arises

Equipment Disposal

- All IT equipment containing data must have data removed prior to disposal
- The Systems Administrator will ensure that the discs are securely erased
- The Systems Administrator will decide on the method of equipment disposal, which may include destruction, or disposal.

Training

- The Privacy Officer and the Systems Administrator will provide induction and follow-up training in privacy and data security practices to all staff, committee members and volunteers, as well as contractors.

Breaches of this policy may result in:

- Loss of access to our data systems

Version 1.1	Data Privacy and Security Policy: Use of the U3A's IT Network
Endorsed by U3A Yarra City Committee of Management	Date: 11/08/2021