BANYULE
UNIVERSITY OF THE THIRD AGE
Office: Upper Ground Floor, 275 Upper Heidelberg Rd, Ivanhoe
Mail: PO Box 454, Rosanna, Victoria, 3084
Website: www.u3abanyule.org.au
Email: info@u3abanyule.org.au
U3A Banyule Inc.
ABN 76 751 606 570
Mobile: 0418 749 228

Policy Guideline 05 – Security of Information and Assets

Introduction

1. U3A Banyule acknowledges that it is the custodian of important and sensitive information about its members and is responsible for protecting that information.

2. U3A Banyule is the owner of various items of equipment and property (assets), and substantial costs would be incurred if these assets were damaged, stolen or compromised in any way.

Purpose

3. This policy addresses the various ways in which information and assets will be protected and should be administered in conjunction with U3A Banyule's Privacy Policy and Code of Conduct.

The purpose of this policy is to:

a. identify the types of information and assets which are deemed to need protection

b. describe the types of procedures to be adopted for protection of information and assets

c. identify those responsible for implementing the policy.

Personal and Other Sensitive Information

4. In the conduct of its operations, U3A Banyule collects and retains personal information about its members, as well as operational

information such as Minutes of Committee meetings and financial records. This information is stored in various places, including:

a. the MyU3A database

b. the U3A Banyule cloud storage system (e.g., Dropbox)

c. U3A Banyule computers

d. U3A Banyule email programs

e. the private computers and other devices (mobile phones, tablets, etc.) of U3A Banyule Committee members and other volunteers

f. the private cloud storage systems of Committee members and other volunteers

g. the private email programs of U3A Banyule Committee members and other volunteers

h. portable storage devices (DVD's, USB devices, etc.) owned by U3A Banyule Committee members, other volunteers and tutors

i. paper records

j. external organisations including: The Australian Tax Office (ATO), U3A Banyule's banks, Consumer Affairs Victoria (CAV) and Australian Charities and Not-for-Profits Commission (ACNC).

Protection of Personal and Other Sensitive Information

5. Access to the MyU3A database, the U3A Banyule cloud storage system, the ATO, CAV and the ACNC is restricted to authorised members in accordance with the document '2020 U3A Banyule Committee of Management Access, Authority & Working Party' updated at least annually by the Committee of Management.

6. Authorised members, who in the course of their duties, access these restricted sites must use a secure log on procedure, in accordance with U3A Banyule's Password Protocol.

7. Access to U3A Banyule computers is protected by password or PIN in accordance with U3A Banyule's Password Protocol.

8. Each U3A Banyule computer is protected by security software, installed and managed by the Privacy and Security Officer.

9. Digital information, except for the MyU3A database, will be backed up to a secure cloud-based storage system approved by the Committee of Management.

10. The Privacy and Security Officer will conduct an annual review of the software installed on U3A Banyule computers. Any software that is not authorised by the Committee of Management will be subject to removal.

11. U3A Banyule members should not store members' personal and other sensitive information on private computers, in private cloud storage systems, in private email programs or on portable devices. All official documents should be stored in U3A Banyule's cloud storage system and not on private computers.

12. The Privacy and Security Officer is responsible for preparing appropriate security protocols for approval by the Committee of Management.

13. Members' personal and other sensitive information stored in paper form should be converted to digital form wherever possible, and any retained paper documents should be stored in a locked compartment within the U3A Banyule office. Scanned and temporary paper documents should be shredded.

Equipment

14. Any equipment that is in the premises of U3A Banyule, but is not owned by U3A Banyule, remains the responsibility of the owner. Privately owned equipment is not covered by U3A Banyule's insurance policy and should not be left unattended.

15. Assets owned by U3A Banyule includes furniture and electronic items as listed in the U3A Banyule Assets Register.

16. U3A Banyule leases its office from the Banyule City Council and shares its classrooms and waiting areas with other clients of the Ivanhoe Library and Community Hub (ILCH). Equipment owned by U3A Banyule should be clearly labelled and not left unattended. Items of equipment that are owned by U3A Banyule should not be stored in waiting areas or

classrooms unless they are in locked cupboards.

17. The U3A Banyule office and classroom storage cupboards should be locked whenever unattended.

18. U3A Banyule computers should be turned off when not in use. For brief interruptions to work, the "sleep" mode may be used, provided a password or PIN is required for return to normal operation.

Access to the U3A Banyule office

19. Access to the U3A Banyule office outside its normal operating hours must be approved by the Office Manager.

20. Only Committee members and rostered Office Assistants are permitted to access the Office, except for those seeking support from an Office Assistant.

21. Keys to the U3A Banyule Office will be restricted in accordance with the Protocol for Key Access to the U3A Banyule office.

Security Breaches

22. If members' personal or other sensitive information is lost, stolen or otherwise compromised, this breach must be advised immediately to the Privacy and Security Officer. The breach will then be investigated, and a report prepared for the Committee of Management, with recommendations for corrective action and review of this policy and associated procedures if appropriate. Recommendations may include insurance claims and referral to the Police if criminal activity is suspected.

Responsibilities

23. The Committee of Management is responsible for:

- developing, adopting, implementing and publishing this policy
- providing secure storage for U3A Banyule equipment
- authorising the procurement of security software for U3A Banyule computers
- maintaining an insurance policy for loss, theft or destruction of assets

- authorising and regularly reviewing protocols for the protection of personal and other sensitive information which it stores, and equipment which it owns
- responding to recommendations resulting from security breaches reported by the Privacy and Security Officer
- regularly reviewing the document 'U3A Banyule Access, Authority and Working Party'
- monitoring and revising this policy as and when the need arises
- preparing and reviewing annually a position description for a Privacy and Security Officer
- appointing a Privacy and Security Officer.

24. Members, volunteers and tutors are responsible for immediately reporting security breaches to the Privacy and Security Officer.

25. The Privacy and Security Officer is responsible for:

- preparing and reviewing annually this policy for consideration by the Committee of Management
- chairing the Privacy and Security Working Party
- preparing and reviewing annually a set of security protocols for consideration by the Committee of Management
- training authorised members in the application of security protocols
- maintaining a record of passwords and PINs used by U3A Banyule computers and software systems
- monitoring adherence to this policy including investigating security breaches and preparing reports and recommendations for the Committee of Management
- developing a cyber security response plan
- regularly reviewing and updating operating systems and security software on computers owned by U3A Banyule
- monitoring software installed by users on computers owned by U3A Banyule
- maintaining U3A Banyule's Assets Register as a means of improving security over those assets
- advising the Committee of Management on anticipated changes to U3A Banyule's security regime
- reviewing systems for the storage of personal and other sensitive information
- implementing access to U3A Banyule's cloud storage system in conjunction with the Access and Authorities Reference Group.

Authorisation

This Security Policy was adopted by the Committee of Management of U3A Banyule and minuted on 19 March 2021.
This policy will be published by the Committee of Management of U3A Banyule on its website.

Related Documents

- U3A Network Victoria's Privacy and Data Security Policy
- U3A Banyule's Code of Conduct
- U3A Banyule's Volunteer Agreement
- U3A Banyule's Privacy Policy
- U3A Banyule's MyU3A Access Reference Group (TOR to be revised)
- Terms of Reference for the Data Privacy and Security Project
- Position Description for Privacy and Security Officer (to be developed)
- '2020 U3A Banyule Committee of Management Access, Authority & Working Party'
- U3A Banyule's Password Protocol (to be developed)
- U3A Banyule Protocol for Key Access to the U3A Banyule Office (to be developed)
- U3A Banyule's Assets Register (to be developed)

Version Number	U3A Banyule Policy Guideline – Security V1
Endorsed by U3A Banyule Committee of Management	Date: 19 March 2021

This document was prepared on 13 March 2021 by Michael Maguire on behalf of the Data Privacy and Security Project Team.