U3A HIGHVALE POLICIES AND PROCEDURES

Privacy and Security

Overview

In 12 March 2014, the Australian Privacy Principles (APPs) replaced the National Privacy principles (NPPs). The 13 APPs are significantly different from the 10 NPPs. The following policies and procedures are designed to comply with the way personal and sensitive information is collected, stored, shared and disposed of.

Also, in October 2019, the Victorian Government adopted new Victorian Protective Data Security Standards which introduce risk-based practices to manage the security of information – that is, U3As must assess the amount of risk in their procedures.

The purpose of this policy is to set out members' privacy rights and to document the framework that U3A Highvale will apply when collecting, storing, using and securing members' personal information. Personal information includes information about members:

- name
- postal, street and/or email addresses
- telephone contact number/s
- previous profession or occupation
- skills or interests
- emergency contact details
- image (photo or video)
- other information you provide to us through member surveys or for other purposes.

Policy

U3A Highvale recognises the importance of protecting members' privacy in relation to their personal information. As a volunteer community organisation providing learning and social facilities for older adults, it will collect personal information from members through membership and course registration.

For example, names and addresses are collected for the mail-out of newsletters, timetables and enrolment confirmations. Phone numbers are recorded for contact purposes (eg. cancellation of a class). Such data form the basis of the U3A Membership

Register which is a statutory requirement. Personal information is collected so that the association can provide services and perform functions that are consistent with its primary purpose and constitution. These include:

- making classes and other activities available to members
- purposes of communication, administration, marketing, and planning, programme development, quality control and research
- maintaining accurate and up-to-date membership records.

Members will be informed of the reason(s) why information is collected and how it is administered and that any personal information held about them is accessible to them. Tutors and facilitators are provided with lists of course members, their names and phone numbers. Class attendance records are maintained and available to tutors and facilitators as required.

All reasonable steps will be taken to ensure that personal information held is protected from misuse, loss and unauthorised access. Members' personal information will not be shared or disclosed other than as described in this policy. U3A Highvale Inc. does not disseminate information about its members to outside bodies. Personal information will not be made available to others for direct marketing purposes.

U3A Highvale Inc. may disclose personal information, for purposes that are directly relevant to its constitution, to:

- volunteers, for example, tutors and members of the Committee of Management
- related organisations, for example, U3A Network Victoria Inc
- employees, contractors or service providers where it is essential to the service being provided.

As the U3A Highvale website is linked to the internet, and the internet is inherently insecure, there is no assurance regarding the security of transmission of information communicated online. These communications will be at members' own risks. However, U3A Highvale will do its best to ensure:

- Physical security of premises
- Physical security of computers or other office devises that can access members details
- Cyber security of office computers and devices used or supplied by key volunteers.

Procedures

Access and Complaints

Members

1. Request access to any personal information U3A Highvale holds about them by contacting the U3A Highvale Enrolment Officer who will aim to provide a suitable means of accessing the information.
2. If a member believes that personal information held about him/her is incomplete or inaccurate, ask the Enrolment Officer to amend it.
3. If members believe their privacy has been breached, they should contact the U3A Highvale Secretary and provide details of the incident so that it can be investigated.
4. Refer any questions or concerns about this policy, or a complaint regarding the treatment of personal information, to the U3A Highvale Secretary.

Enrolment Officer

5. Respond to a member's request for access to the personal information held by U3A Highvale about that member and for requests to correct personal information that is believed to be inaccurate or out of date.

Secretary

6. Receive enquiries about this policy and complaints about a potential breach of this policy; and bring a complaint before the Committee of Management for investigation and resolution.
7. Treat confidentially all requests or complaints lodged regarding this policy.
8. Contact the complainant within a reasonable time after receipt of a complaint to discuss the concerns
9. Outline options regarding how complaints may be resolved. Aim to ensure that a complaint is resolved in a timely, impartial and appropriate manner.

Implementation of Members' Privacy

Committee Members

10. Determine which members of committees and volunteers are authorised to access personal information in the system or records.
11. Develop, adopt, implement and publish this policy.
12. Collect, store and use members personal information in accordance with this policy.
13. Monitor and revise this policy as and when the need arises.

Security of Premises and Computers

Tutors (Computing)

14. Add the WiFi password to the U3A.Highvale local Home Page. Update it at the start of each term, or as necessary.
15. Advise students where to look for the latest password.

Members

16. Get in the habit of regular WiFi password changes and going to the local Home Page to see what it currently is

Cyber Security

Tutors and Members

17. Use strong unique passwords
18. Consider using a password manager
19. Keep your software up to date on all your devices
20. Use the latest version of your web browser
21. Install security software such as antivirus protection
22. Only connect to trusted Wi-Fi networks, not public ones
23. Beware of online scams and phishing
24. Do not open suspicious attachments or click unusual links in messages
25. Do not enter your username and password in response to emails or messages, go to the official website or app
26. Always use a PIN or password on your devices
27. Do not use USBs or other external devices unless you own them
28. Only download apps from official stores
29. Consider using a reputable Virtual Private Network (VPN) application on your device.