|  |
| --- |
| **Data Privacy and Security Policy:****Privacy Officer Role Description** |

## **Purpose**

The Privacy Officer position is held by the Secretary with oversight of overall compliance within the U3A. They are the first point of contact within the organisation for all matters related to privacy, data security and personal information. They play an important role in promoting an awareness of privacy within our U3A and ensuring that we uphold our privacy and data security obligations.

**Responsibilities**

## **Key responsibilities**

The Privacy Officer assists us in complying with The Privacy and Data Protection Act 2014 (Vic) (PDP Act), and the associated Information Privacy Principles (IPPs).

This position may also respond to privacy enquiries and complaints from volunteers within the organisation, and members of the public.

### **Other responsibilities**

Other responsibilities include:

* Developing policies around the management of personal information and data security
* Providing training about our privacy obligations and data security considerations
* Developing and reviewing the organisation’s Privacy Impact Assessments (PIAs) on an annual basis in line with our risk management review processes
* Co-ordinating the handling of internal and external privacy enquiries, privacy complaints, and requests for access to, and correction of, personal information
* Engaging with U3A Network Victoria in relation to data privacy and security

## **Relationships with Others**

Working effectively with our Committee of Management, Systems Administrator and our membership is vital. The Committee holds overall responsibility for ensuring that we achieve our data privacy and security obligations.

This includes:

* **Approving** business rules, policies and procedures
* **Monitoring** compliance to the legislation and IPPs

Aspects of the role may be performed in conjunction with the Systems Administrator.

These may include:

* **Advising** the Committee on privacy and data security related matters
* **Recommending** strategies to the Committee
* **Managing** the organisation’s response to data breaches

## **Reporting**

The role reports to the Committee of Management and provides update reporting to U3A Network Victoria when requested.

|  |
| --- |
| **Data Privacy and Security Policy:****Systems Administrator Role Description** |

# Sherbrooke U3A Systems Administrator Role Description

## Purpose of the Policy

The Systems Administrator is responsible for advice about the upkeep, configuration, and reliable operation of our computer systems.

## Key responsibilities

The Systems Administrator assists us in complying with The Privacy and Data Protection Act 2014 (Vic) (PDP Act), and the associated Information Privacy Principles (IPPs).

Their key responsibilities are to:

1. Provide support as needed in administering the U-MAS system and any other technology used by the U3A
2. Provide support as needed for backup, recovery, updates and upgrades for all systems
3. Represent the U3A at system user meetings
4. Liaise as necessary with the system’s support team, report any system issues and suggest priorities for improvement
5. Advise the Committee of Management on technology and data security issues
6. Manage the hosting contract with VentraIP and other external providers
7. Assist in the development and implementation of a data breach response plan

### Other responsibilities

Other responsibilities include:

* Working with the U3A’s Privacy Officer in developing and reviewing the organisation’s Privacy Impact Assessments (PIAs) on an annual basis in line with our risk management review
* Engaging with U3A Network Victoria in relation to data privacy and security

## Relationships with others

The Committee holds overall responsibility for ensuring that we achieve our data privacy and security obligations. This includes:

* **Approving** business rules, policies and procedures
* **Monitoring** compliance to the legislation and IPPs

Aspects of the role may be performed in conjunction with the Privacy Officer. These may include:

* **Advising** the Committee on privacy and data security related matters
* **Recommending** strategies to the Committee
* **Managing** the organisation’s response to data breaches

## Reporting

The role reports to the Committee of Management and provides update reporting to U3A Network Victoria when requested.

## Related Policies

* Privacy Policy

|  |
| --- |
| **Data Privacy and Security Policy:****Data Privacy and Security Statement** |

Our U3A is committed to safeguarding privacy of personal information. Overall responsibility for this policy rests with our Committee of Management. Our Privacy Officer holds responsibility for compliance.

We seek to abide by the Privacy and Data Protection Act 2014 (Vic**) (PDP Act**). The Act is administered by the Office of the Victorian Information Commissioner (OVIC) at <https://ovic.vic.gov.au/> Our U3A seeks to comply with the Victorian Protective Data Security Framework and the Victorian Privacy Principles (VPPs).

## **What is Personal Information and Why Do We Collect It?**

Personal Information may include

* Name
* Year of birth
* Postal, street and email addresses
* Telephone contact numbers
* Previous profession or occupation
* Skills or interests
* Emergency contact details
* Images such as a photo or video
* Other information you provide to us through member surveys or for other purposes

Our U3A will collect personal information about each member directly from the member in question. This will be done through membership and course registration processes.

Approval to use a member’s image in our publications will be assumed on completion of the membership application and membership renewal processes. Members who wish to decline to allow use of their image are to indicate so on the membership application and membership renewal documentation.

Personal Information may be obtained in many ways including via:

* Correspondence
* Telephone
* Email
* Voice and video recordings
* Online forms, such as in relation to membership applications or registration for events
* Via our website
* From subscribing to our newsletters

You may unsubscribe from our newsletters by opting out or at any time by contacting us in writing.

We do not guarantee any websites which are accessed from our website via links or the policy of authorised third party software providers.

We collect personal information from members so that we can provide services and perform functions that are consistent with our constitution, including:

* To make classes and other activities available to members
* For communication, administrative, marketing and planning purposes
* For program development, quality control and research purposes
* To maintain accurate and up-to-date membership records

We will:

* Only collect information that is consistent with our primary purpose and constitution
* Inform members of the reason why information is collected and how it is used
* Inform members that any personal information held about them is accessible to them
* Take all reasonable steps to ensure that personal information held is accurate and up to date
* Take all reasonable steps 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. Personal information will not be made available to others for direct marketing purposes.

We may disclose your personal information, for purposes that are directly relevant to our constitution, to:

* Our volunteers, for example, tutors and members of the Committee of Management
* Employees, contractors or service providers where it is essential to the service to be provided.

When we collect personal information we will, where appropriate and where possible, explain to you why we are collecting the information and how we plan to use it. We will only transfer your personally identifiable information to hosting services which meet or are deemed equivalent to the Victorian Privacy Principles.

We cannot provide any assurance regarding the security of transmission of information you communicate to us via unsecured or public Wi-Fi. These communications will be at your own risk.

**Reporting to U3A Network Victoria**

Under the terms and conditions for membership of U3A Network Victoria, we are required to report deidentified statistics about membership annually to Network. The current requirement is to report in May each year.

In order to report, we must enter the required reporting details into the Network Members Database (NMDB). Entry to the NMDB is obtained via the Network website, and then logging in using a unique ID and passcode supplied to us.

**Other Reporting Information**

The categories of information collected currently through NMDB include:

* U3A details
* Office bearers
* Numbers of members
* Age breakdown by male and female, and
* Volunteer numbers and hours

The information is used by Network to:

* Calculate annual subscriptions to be paid to the Network. Currently it is calculated at $2 per full member
* Demonstrate growth in membership over time to funders
* Communicate with U3As and their Presidents, Secretaries and other key position holders
* Record key U3A representatives
* Allow the public to search via the Network website for a U3A in their area

Apart from entering our own data, we are not able to access NMDB to view the details about other U3As.

**Personal Information entered into NMDB**

Each U3A is required to enter the name, email address, home and mobile numbers of key office bearers including:

* President
* Vice President
* Secretary
* Treasurer
* Course Coordinator
* Council Delegate

**Sensitive Information**

Sensitive information is defined in the PDP Act to include information or opinion about such things as an individual's racial or ethnic origin, political opinions, membership of a political association, religious or philosophical beliefs, membership of a trade union or other professional body, criminal record or health information. Our U3A does not collect sensitive information.

## **Disclosure of Personal Information**

Your personal information may be disclosed in a number of circumstances including the following:

* Third parties where you consent to the use or disclosure
* Where required or authorised by law

## **Security of Personal Information**

We store our data with VentraIP. Their servers are located in Victoria and NSW.

We use a combination of people, process and technology safeguards to store personal information in a manner that reasonably protects it from misuse and loss and from unauthorised access, modification or disclosure.

Personal information stored in physical files in our U3A are held in a locked filing cabinet, kept secure and retained by us for a maximum of seven years.

Our U3A uses the following physical security and access strategies to protect information stored at our site:

* Files containing personal information are locked in a filing cabinet which can only be accessed by our Executive
* Access to our office is limited to Executive, Tutors and Office Volunteers

**Online Applications**

Our website uses the Wordpress platform.

Our U3A uses Zoom for video-conferencing. Zoom meetings can be recorded locally by the host. Participants can take screen shots. Zoom recordings are encrypted with complex passwords.

**Access to your Personal Information**

You may access the personal information we hold about you and update or correct it by logging-in to the UMAS database. If you need help with accessing your personal information, please contact us.

In order to protect your personal information we may require identification from you before releasing the requested information.

## **Maintaining the Quality of your Personal Information**

It is important to us that your personal information is up to date. We will take reasonable steps to make sure that your personal information is accurate, complete and up to date. If you find that the information we have is not up to date or is inaccurate, please advise us as soon as practicable so we can update our records and ensure we can continue to provide quality services to you.

## **Procedures**

* Members may request access to any personal information our U3A holds about them by contacting our Secretary who will aim to provide a suitable means of accessing the information.
* Where a member believes that personal information held about them is incomplete or inaccurate the member may update it using UMAS or ask the Secretary to amend it.
* Where a member believes their privacy has been breached, they should contact the Secretary/Privacy Officer and provide details of the incident so that it can be investigated.
* Any questions or concerns about this policy, or a complaint regarding the treatment of personal information, should be referred to our Secretary/Privacy Officer.
* We will treat confidentially all requests or complaints lodged regarding this policy. We will contact you within a reasonable time after receipt of your complaint to discuss your concerns and to outline options regarding how they may be resolved. We will aim to ensure that your complaint is resolved in a timely, impartial and appropriate manner.

.

## **Policy Updates**

This policy may change from time to time and is available on our website.

## **Privacy and Data Security Policy Complaints and Enquiries**

If you have any queries or complaints about this policy, please contact us at:

PO Box 1153, Upwey. 3158

secretary@sherbrookeu3a.org.au

9754 3339

|  |
| --- |
| **Data Privacy and Security Policy:****Use of the U3A’s IT Network** |

## **Purpose**

The purpose of this policy is to:

* State our business rules for using our U3A’s IT equipment
* 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.

This policy does not cover access to the UMAS membership system.

**Policy**

**Access to our IT system**

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

* The Systems Administrator and Executive members have access to our IT system.
* Members of our committee of management may use our IT system in order to perform their role.
* Volunteers or tutors may be given access to the relevant aspects of our system for certain projects.
* Contractors that support our IT and telephony systems may be given access.

## **Software considerations**

* On all U3A owned devices, Anti-virus software is only to be installed or uninstalled after consultation with the Systems Administrator, but kept up-to-date by the primary user of the device.
* The Secretary will maintain a register of all IT equipment, software licenses, web hosting, access IDs and passwords. As a security precaution this register will be kept off-site.
* Only software authorised by the Systems Administrator will be installed on our U3A’s hardware
* Software no longer required can only be removed after consultation with the Systems Administrator.

## **Access to Personal Data**

* Electronic documents which hold personal information will only be available to people who have been authorised by the Secretary/Privacy Officer.
* Any personal data downloaded by volunteers or committee members must be deleted when no longer required. This is the responsibility of the individual, with assistance from the Secretary/Privacy Officer.
* Personal data must not be downloaded to memory sticks, external hard disks or personal cloud locations.

## **Cyber Security Threats**

* Any cyber security threats must be immediately reported to the Privacy Officer or 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 a two-yearly basis, in conjunction with our risk management process.

## **Back Up of Data Files**

* The primary user of a device will be responsible for backing up new work. The Systems Administrator will be responsible for regularly checking that back-ups of key electronic data files have been completed.
* 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/or the Systems Administrator will provide induction and follow-up training in privacy and data security practices to committee members and volunteers, as well as contractors

Breaches of this policy may result in:

* Loss of access to our data systems

# **Data Privacy and Security Policy:**

**Data Breaches**

## **Purpose**

Sherbrooke U3A is committed to safeguarding the privacy of personal information belonging to its members.

We seek to abide by the Privacy and Data Protection Act 2014 (Vic). The act is administered by the Office of the Victorian Information Commissioner (OVIC) at <https://ovic.vic.gov.au>.

**What is a data breach?**

A data breach occurs when personal or sensitive information that is held by an organisation is accessed or disclosed in a way that it should not have been, eg, where it is lost, stolen or given to the wrong person.

Data breaches have the potential to cause us or our organisation harm including financial, emotional or physical harm.

Examples of data breaches can include, but are not limited to:

* Loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
* Unauthorised access to personal information by a volunteer
* Inadvertent disclosure of personal information due to ‘human error’, for example an email sent to the wrong person
* Disclosure of an individual’s personal information to a scammer, as a result of inadequate identity verification procedures

**Notification of a Data Breach**

Any data breach, irrespective of its possible severity, must be notified to the Secretary/Privacy Officer and Systems Administrator. A plan should be enacted quickly to reduce chances of experiencing any harm, damage, or loss of reputation. Where personal information is involved the member(s) need to be involved and communicated with.

Where it is deemed that there is a real risk of serious harm the Office of the Australian Information Commissioner will be notified by accessing the appropriate form at <https://www.oaic.gov.au>.

**Data Breach Response Process**

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

The following four step plan will be adopted when responding to a data breach:

STEP 1 – Contain the breach and make a preliminary assessment

* Immediately contain breach – Systems Administrator and Privacy Officer to implement
* Convene a meeting of the Sherbrooke U3A Executive and keep committee and affected individuals informed, providing regular updates.
* Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing Sherbrooke U3A to take appropriate corrective action.
* Consider developing a communications or media strategy to manage public expectations or media interest.

STEP 2 – Evaluate the risks for individuals associated with the breach

* Conduct initial investigation and collect information about the breach promptly, including:
- the date, time, duration and location of the breach
- the type of personal information involved in the breach
- how the breach was discovered and by whom
- the cause and extent of the breach
- a list of the affected individuals or possible affected individuals
- the risk of serious harm to those affected
- the risk of other harms
* Determine whether the content of the information is important.
* Establish the cause and extent of the breach.
* Assess priorities and risk based on what is known.
* Keep appropriate records of the suspected breach and the response, including the steps taken to rectify the situation and the decisions made.

STEP 3 – Consider breach notification

* Determine who needs to be made aware of the breach (internally and potentially externally) at this preliminary stage.
* Determine whether to notify affected individuals. Is there a real risk of harm to the affected individuals?
* Consider whether others need to be notified, including police, Australian Privacy Commissioner or other agencies.

STEP 4 – Review the incident and take action to prevent future breaches

* Fully investigate the cause of the breach.
* Report to Committee on outcomes and recommendations:
- update security if necessary
- make appropriate changes to policies and procedures if necessary
- revise training practices if necessary
- consider the option of an audit to ensure necessary outcomes are achieved.

**Authorisation**

This Policy was adopted by the Committee of Management of Sherbrooke U3A Inc., and minuted as such, on 29 October, 2021.