# Policy Guidelines 07 – Data Breach Prevention and Response

## 1. Introduction

U3A Hepburn Shire Inc. (U3A/HS) has an ongoing obligation to take steps to handle personal information in accordance with the Australian Privacy Principles.

A data breach is the unauthorized access of the organization data. The access may compromise the confidentiality, integrity or availability of the data. Good faith access of the data by employees or agents or legitimate purposes is not a breach

Members' Personal Identifiable data stored in U3A/HS's User Management System (UMAS) includes but is not limited to:

- Name
- Year of birth
- Home address
- e-mail address
- Phone number
- Emergency contact name and phone number

## 2. Purpose

This document outlines the procedures for U3A/HS to follow in order to prevent any breach of personal data held by U3A/HS and actions to be taken in the event of a breach of that data being identified.

## 3. Policy/Procedures

**3.1** The Committee will consider who within the U3A/HS Committee needs access to the full membership information and restrict access to those who need it.

**3.2** The Committee will ensure that Committee members/group conveners who hold information, delete or return all data when relinquishing their roles.

**3.3** The Committee will train / inform Committee members and activity convenors with regard to cybersecurity including the use of strong passwords to protect members' data and secure management of login details (for example regularly changing passwords, not sharing login details or passwords with others).

**3.4** Upgrades to UMAS, as provided by U3A Network Victoria, will be promptly installed.

**3.5** In the event of a detected data breach;

**3.5.1** U3A/HS will seek immediate support from the Information Technology experts at U3A Network Victoria.

**3.5.2** All administrator passwords for UMAS and the U3A/HS email accounts will be promptly changed.

## 4. Responsibilities

**4.1** The Committee of Management is responsible for:

- Deciding who needs access to membership data
- Ensuring that data is returned or deleted by retiring Committee members of conveners.

**4.2** The UMAS administrators are responsible for:

- The prompt installation of UMAS upgrades.
- The training of Committee members and conveners in cybersecurity matters.

## 5. Authorisation

**5.1** This policy was adopted by the Committee of Management of U3A Hepburn Shire, and minuted as such, on 7 December 2020.

**5.2** This policy will be published by the Committee of Management of U3A Hepburn Shire on its website within 4 weeks of the date of this authorisation.

## 6. Related Policies

Risk Management, Privacy