Data Breaches

Introduction

U3A Bendigo Incorporated is committed to safeguarding the privacy of personal information, belonging to members.
This policy should be read in conjunction with the Privacy Policy, The Privacy & Data Protection Policy. 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/.
U3A Bendigo seeks to comply with the Victorian Protective Data Security Framework.

What is a data breach?

A data breach occurs when personal information or sensitive information about the organisation that is held by the organisation is accessed or disclosed in a way that it should not have been, for example 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, physical, or emotional harm.

Once notified of a data breach, the breach must be notified to the President, Vice President, Treasurer and Secretary (members of the Executive). 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.

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

When a data breach has been identified, irrespective of its possible severity or impact, it should be notified initially and immediately, to U3A Bendigo Privacy and Data Security Officer (PDSO), and the I.T. Manager.

Depending on the nature of the data that may have been breached the following parties may need to be notified:

- Financial Institution (Banks, Credit Agencies, etc) if the data is relating to financial or banking details
- The individual or individuals' whose information may have been breached
- U3A Network Victoria's State Government funders, in accordance with our service agreements.

If the breach is deemed serious it may be further reported to:

- Victoria Police on 13 14 44 or contact 000 for immediate safety concerns, such as a threat to physical safety
- ACSC (Australian Cyber Security Centre) via their website https://cyber.gov.au
- ACCC (Australian Competition and Consumers Commission), especially where a scam may be associated with the Data Breach. https://scamwatch.gov.au
- IDCare on 1300 432 273 or visit www.idcare.org where Identity theft or fraud is associated with the data breach

The PDSO and the I.T. Manager will coordinate and liaise with CoM to determine which parties including third-party support and suppliers to engage and what actions need to be executed to remedy the breach.

In determining whether to escalate data breaches the following should be considered:

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a real risk of serious harm to the affected individual or individuals?
- Does the breach or suspected breach indicate a systemic problem in our processes or procedures?
- Could there be media or stakeholder attention because of the breach or suspected breach?

Reporting and recording Data Breaches

When a data breach is identified the details should be entered into the Data Breach Form and forwarded to the Privacy and Data Security Officer as well as the I.T. Manager.

The details of the breach should include as much relevant information as possible (if known):

- Time and date when the Data Breach was identified
- The nature of the breach – misdirected email, loss of a device, computer message indicating a breach, etc
- The contact details of the person reporting the breach
- The type of data that has been breached, and its possible sensitivity or importance
- The PDSO and I.T.M should investigate the breach and forward the outcome to the President and the Executive.
- The incident should also be entered into the Risk Management Register.

Authorisation:

This policy was adopted by Committee of Management of U3A Bendigo Incorporated, and minuted as such, on 6th September 2021.