

Melbourne Area Derby U3A

Data Protection Policy

Scope of the policy

This policy applies to the work of Melbourne Area Derby U3A (MAD u3a). The policy sets out the terms on which MAD u3a collects and processes information for membership purposes. The policy details how personal information will be collected, stored and managed in line with data protection principles and the General Data Protection Regulation (GDPR). The policy is reviewed on an ongoing basis by MAD u3a committee members to ensure that MAD u3a remains compliant. This policy should be read in association with MAD u3a's Privacy Policy.

Why this policy exists

This data protection policy ensures MAD u3a:

- Complies with data protection law and follows good practice
- Protects the rights of members
- Is open and transparent about how it stores and processes members' data
- Protects itself from the risks of a data breach

General guidelines for committee members and group leaders

- The only people able to access data covered by this policy should be those who need to communicate with or provide a service to MAD u3a members.
- MAD u3a will provide induction training to committee members and group convenors to help them understand their responsibilities when handling data.
- Committee Members and group leaders should keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords must be used and they should never be shared.
- Data should not be shared outside of the U3A unless with prior consent and/or for specific and agreed reasons. Examples would include Gift Aid information provided to HMRC or information provided to the distribution company for the Trust publications.
- Member information should be refreshed periodically to ensure accuracy, via the membership renewal process or when policy is changed.
- Additional support will be available from the Third Age Trust where uncertainties or incidents regarding data protection arise.

Data protection principles

The General Data Protection Regulation identifies key data protection principles: [adapted]

Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner

Principle 2 - Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Principle 3 - The collection of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Principle 4 – Personal data held should be accurate and up to date. Reasonable steps must be taken to ensure that inaccurate personal data, in relation to the purposes for which they are processed, are corrected or erased without delay.

Principle 5 – Personal data which permits identification of individuals must be retained for the minimum time necessary to fulfil the purposes for which it is collected. Personal data may be stored for longer periods if archived, either in the public interest, or for scientific, statistical or historical research. In order to safeguard the rights and freedoms of individuals, all such retained data shall be subject to the relevant technical and organisational requirements of the GDPR.

Principle 6 - Personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Lawful, fair and transparent data processing

MAD u3a requests personal information from potential members and members for membership applications and for sending communications regarding members' involvement with the U3A. Members will be informed as to why the information is being requested and what the information will be used for.

The lawful basis for obtaining member information is based on the contractual relationship that the U3A has with individual members. In addition, members will be asked to provide consent for specific processing purposes such as the taking of photographs.

MAD u3a members will be informed who they need to contact should they wish to withdraw their consent for the use of their data for specific purposes for which they have previously given consent. Where these requests are received they will be acted upon promptly and the member will be informed when the action has been taken.

Processed for specified, explicit and legitimate purposes

Members will be informed how their information will be used and the Committee of MAD u3a will seek to ensure that member information is used appropriately. Appropriate use of information provided by members will include:

- Communicating with members about MAD u3a events and activities.
- Group leaders communicating with group members about specific group activities.
- Providing Member information to the company that sends out the Trust publication "Third Age Matters". [Members will be required to actively choose whether or not they wish to receive the publication].
- Sending members information about Third Age Trust events and activities.
- Communicating with members about their membership and/or its annual renewal.
- Communicating with members about specific issues that may arise during the course of their membership.

MAD u3a will ensure that group leaders are made aware of what is considered appropriate and inappropriate communication. An example of inappropriate communication would include sending U3A members marketing and/or promotional materials from external service providers.

MAD u3a will ensure that members' information is managed in ways that protect individual members' rights which include:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

Adequate, relevant and limited data processing

Members of MAD u3a will only be asked to provide information that is relevant for membership purposes. This will include:

- Name
- Postal address
- Email address
- Telephone number

Where additional information may be required such as *health related information*, this will be obtained with the express consent of the member who will be informed why this information is required and the purpose that it will be used for.

Where MAD u3a organises a trip or activity that requires *next of kin information* to be provided, a legitimate interest assessment will have been completed to justify requesting this information. Members will be made aware that the assessment has been completed.

Photographs

Photographs are classified as personal data. Where group photographs are being taken, members will be asked to step out of shot if they don't wish to be in the photograph. Consent will be obtained from members for photographs to be taken and members will be informed as to where such photographs will be displayed. Should a member wish to withdraw their consent to display their photograph, they should contact an officer or committee member and all reasonable efforts will be made to remove the photograph.

Accuracy of data and keeping data up-to-date

MAD u3a has a responsibility to ensure members' information is kept up to date. Members are advised to inform the membership secretary if any of their personal information changes. In addition, on an annual basis, the membership renewal process will provide an opportunity for members to review and update their personal information.

Accountability and governance

MAD u3a Committee is responsible for ensuring that the U3A remains compliant with data protection requirements and can show evidence that it has. Where consent is required for specific purposes then evidence of this consent (either electronic or paper) will be obtained and retained securely.

MAD u3a Committee will ensure that new members joining the Committee receive an induction into the requirements of GDPR and the implications for their role. MAD u3a will also ensure that group convenors are made aware of their responsibilities in relation to the data they hold and process. Committee Members will stay up to date with guidance and

practice within the U3A movement and will seek advice from the Third Age Trust National Office should any uncertainties arise.

MAD u3a Committee will review data protection requirements on an ongoing basis, reviewing who has access to data and how data is stored and deleted. When Committee Members and Group Convenors relinquish their roles, they will be asked to either pass on data appropriately and securely to those who need it and/or delete data.

Secure Processing

MAD u3a Committee Members have a responsibility to ensure that data is both securely held and processed. This will include Committee members:

- Using and maintaining strong passwords
- Not sharing passwords
- Restricting access to member information to those on the Committee who need to communicate with members on a regular basis
- Using password protection on all official and personal laptops and PCs that contain secure information
- Using password protection, a membership database or secure cloud systems when sharing data between committee members and/or group leaders.
- Installing firewall and virus protection on to Committee Members' laptops or other devices.

Subject Access Request

Members of MAD u3a are entitled to request access to the information that the organisation holds. The request must be made as a written request to the MAD u3a Membership Secretary. Such a request will be formally acknowledged and dealt with expediently (the legislation requires that information should generally be provided within one month) unless there are exceptional circumstances as to why the request cannot be granted. MAD u3a will provide a written response detailing all information held on the member. A record shall be kept of the date of the request and the date of the response.

Data Breach Notification

If a data breach occurs, action will be taken to minimise the harm. This will include ensuring that all MAD u3a Committee Members are made aware that a breach has taken place and how the breach occurred. The Committee will then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. The Secretary of MAD u3a will contact National Office as soon as possible after the breach has been identified to report the breach. A discussion will take place between the Chair and National Office as to the seriousness of the breach, action to be taken and, where necessary, whether the Information Commissioner's Office will be notified. The Committee shall also contact the relevant U3A members to inform them of the data breach and actions being taken to resolve the breach.

Where a U3A member feels that there has been a breach by the U3A, a committee member will ask the member to provide an outline of the breach and confirm the details in writing in a letter or email detailing their concerns. The alleged breach will then be investigated by members of the committee who are not in any way implicated in the breach. Where the committee needs support or if the breach is serious they should notify National Office. The U3A member should also be informed that they can report their concerns to National Office if they don't feel satisfied with the response from the U3A. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.

END

Status	Review Date	Action	Operator	Date
Version 00		Draft	Geoff Dowell	19/08/2019
Version 03		Adopted	Committee	19/09/2019
Version 04	19/09/2020	Reviewed and updated	G.Dowell I.Turner	22/02/2021
Version 04		Endorsed	Committee	18/03/2021