Malmesbury and District u3a

Data Protection Policy

Scope of this Policy

This policy is based upon the national Third Age Trust's guidelines outlining the principles that underpin the UK General Data Protection Regulations (hereafter 'GDPR') and the legal restrictions on how personal information can be gathered, stored and managed.

This policy applies to the work of Malmesbury and District u3a (hereafter 'the u3a') and sets out the legal requirements that the u3a must follow when gathering, storing and managing information for membership purposes. It should be read in tandem with the u3a's Privacy Policy. The latter describes, in practical terms, how the u3a protects the personal information members have supplied so that it can provide the services and benefits of u3a membership.

The policy is reviewed at approximately two-year intervals by the u3a Committee who are collectively responsible for ensuring that the Data Protection and Privacy Policy and practice are consistent with the Third Age Trust's guidelines and compliant with GDPR.

Why this Policy Exists

This data protection policy ensures the u3a:

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

UK Data Protection Law

- 2018 Data Protection Act (amended 2021) - The UK implementation of the original EU General Data Protection Regulations (GDPR) 2018.
- 2021 UK General Data Protection Regulations - Mirrors the original EU GDPR but adapted to reflect UK status post-Brexit
- 2025 Data (Use and Access) Act – updates and amends some provisions of GDPR

Together these laws form the legal framework for Data Protection in the UK enshrining how personal data must be used and stored & giving substantial rights to people over their data.

Data Protection is a serious responsibility- compliance is overseen by the Information Commissioners Office (ICO) who can issue a maximum fine of £17.5m for breaches of the law.

UK GDPR Definitions

- 'personal data' – any information relating to an identifiable living person ('data subject') e.g. name, address, contact details, financial details
- 'processing' - collecting, recording, organising, storing, retrieving, using, disclosing, disseminating, erasure or destruction of data
- 'data controller' – organisation/body which determines the purposes and means of the processing of personal data (i.e. M&D u3a)
- 'data processor' - body which processes personal data on behalf of the controller (e.g. Third Age Trust)

Data Protection Principles & how Malmesbury u3a applies these:

1. Lawful, Fair and Transparent Data Processing

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

GDPR provides 6 'lawful reasons' for processing data:

- Consent
- Contract
- Legal Obligation
- Vital Interests
- Public task
- Recognised Legitimate Interests

Each organisation must clearly state which basis they are using for what data.

Malmesbury & District u3a is the 'data controller' for the purpose of processing members' data (i.e. it is responsible for keeping and using members' information appropriately) and this information is processed on the grounds of 'consent' and 'contract' in relation to managing and providing u3a services and activities. Emergency contact information is collected on the grounds of 'consent'. This information is voluntary and not essential for membership but greatly simplifies the task of organising help and support for a member in the case of a serious incident or accident.

U3a members will be asked to provide consent for specific processing purposes such as sharing information with Third Age Trust for the distribution of the national magazine. The u3a members will be informed as to whom they need to contact should they wish for their data not to be used for specific purposes for which they have provided consent. Where these requests are received, they will be acted upon promptly and the member will be informed as to when the action has been taken.

2. Specified, Explicit and Legitimate Purposes

Members will be informed as to how their information will be used and the u3a Committee will seek to ensure that member information is not used inappropriately. Appropriate use of information provided by members will include:

- Communicating with members about u3a events and activities
- Group leaders communicating with group members about specific group activities
- Consent will be sought in order to add members details to the direct mailing information for the Third Age Trust magazines
- Sending members information about Third Age Trust events and activities
- Communicating with members about their membership and/or renewal of their membership
- Communicating with members about specific issues that may have arisen during the course of their membership

The u3a will ensure that group leaders are made aware of what would be considered appropriate and inappropriate communication. Inappropriate communication would include sending u3a members marketing and/or promotional materials from external service providers.

The u3a will ensure that members' information is managed in such a way as to not infringe an individual member's 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

3. Adequate, Relevant and Limited Data Processing

Members of the u3a will only be asked to provide information that is relevant for membership purposes. This essential information is effectively part of the contract that enables the u3a to provide the services and benefits of membership. This will include:

- Name
- Postal address
- Email address
- Telephone number
- Gift Aid entitlement

Where additional information may be requested such as health-related information or emergency telephone numbers, this will be obtained with the consent of the member who will be informed as to why this information is required and the purpose that it will be used for.

Emergency contact information will only be used in the event of a serious incident/accident to contact someone who is able to support the member or liaise on their behalf with e.g. medical professionals.

4. Accuracy of Data and Keeping it Up to date

The u3a has a responsibility to ensure members' information is kept up to date. Members must let the membership secretary know if any of their personal information changes. In addition, on an annual basis, the membership renewal process will provide an opportunity for members to inform the u3a as to any changes in their personal information.

Where the membership secretary is informed that a member is now deceased, their status will be changed on the system, email address deleted and group leaders informed to help prevent inappropriate communication.

5. Storage Limitation

Members' personal data will be stored on the active database for the duration of their membership. Once they cease to be a current member, their record will be marked as no longer current and their information will be deleted from the system in December of the year following the year in which their membership ended. If there are legal, taxation or insurance reasons which require information to be held for longer e.g. for Gift Aid requirements, then information will be deleted a soon as those requirements have been met.

6. Integrity & Confidentiality

Membership information will be held on the Beacon database and access will be restricted via individual secure logins for committee members and group leaders as appropriate.

The u3a Beacon Membership System has in place a range of security safeguards to protect personal information against loss or theft, as well as unauthorised access, disclosure, copying, use, or modification.

Committee members' and group leaders' access on Beacon will be restricted to the information necessary for their particular role and access will be removed once someone relinquishes their role.

In limited circumstances where data may temporarily be stored on local devices or in paper form (e.g. for a specific trip/activity), this information will be kept secure and deleted as soon as it is no longer required.

7. Accountability and Governance

The u3a Executive Committee are responsible for ensuring that the u3a remains compliant with data protection requirements and can show 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. The u3a Committee will ensure that new members joining the Committee receive an induction into the requirements of GDPR and the implications for their role. The u3a will also ensure that group leaders are made aware of their responsibilities in relation to the data they hold and process. Committee Members shall also stay up to date with guidance and practice within the u3a movement and shall seek additional input from the Third Age Trust National Office should any uncertainties arise. The Committee will review data protection

requirements on an ongoing basis as well as reviewing who has access to data and how data is stored and deleted.

Subject Access Requests

Members are entitled to request access to their information that is held by the u3a and for that information to be updated or deleted. Requests can be made in any format to the Membership Secretary of the u3a. On receipt of the request, the request will be formally acknowledged and dealt with expediently (generally within one month) unless there are exceptional circumstances as to why the request cannot be granted. The 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.

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. Otherwise, consent will be obtained from members in order for photographs to be taken and members will be informed as to where photographs will be displayed. Should a member wish at any time to remove their consent and to have their photograph removed then they should contact the Committee's nominated Data Security Officer (see details at end of this policy) to advise that they no longer wish their photograph to be displayed.

Guidelines for Committee Members and Group Leaders to ensure strong data protection

u3a Committee Members and Group Leaders have a responsibility to ensure that data is both securely held and processed by taking sensible precautions and following the guidelines below:

- Access to members' personal data will be restricted to those who need to communicate with or provide a service to the u3a members.
- The u3a will provide induction training to committee members and group leaders to help them understand their responsibilities when handling data.
- Strong passwords must be used, and they should never be shared.
- Password/PIN/biometric protection must be used on laptops/PCs, i-pads/tablets or phones that contain personal information and these devices should have up-to-date virus protection.
- Other users on a shared device must not be allowed to access or view members' personal data.
- Free (non-password protected) wi-fi must not be used when accessing members' personal data.
- Password protection or secure cloud systems must be used when sharing data between Committee Members and/or Group Leader.
- Paper records must be locked away & securely destroyed it as soon as they are no longer needed.
- 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 support from the Third Age Trust where uncertainties or incidents regarding data protection arise.

Data Breach Notification

Were a data breach to occur, this should be reported promptly to the Data Security Officers (see below) to enable action to be taken to minimise the harm. This will include considering:

- How likely is it a person can be identified from the 'lost' information
- What type of information was included in the breach
- Who it was shared with/now has access to it
- What could someone do with that information

The Data Security Officers will then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. The Chair of the u3a will contact National Office as soon as possible after the breach occurring to notify them of 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, the Information Commissioner's Office would be notified. The Committee will be informed about the breach and actions taken and contact will be made with the relevant u3a members to inform them of the data breach and actions 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. If the initial contact is by telephone, the committee member will ask the u3a member to follow this up with an email or a letter detailing their concern.

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 could 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.

Data Security Officers

The u3a Committee Meeting have identified two Committee Members to act as Joint Data Security Officers until further notice. They are:

Karen Stott (Beacon Administrator): primarily concerned with the Beacon Membership Database and related practicalities of information management. Email: beacon@malmesburyu3a.org.uk

John Fairhurst (Chair): primarily concerned with policy development, its implications and dissemination. Email: chair@malmesburyu3a.org.uk

Appendix: BEACON ACCESS DOCUMENTATION

The GDPR requires that organisations document their use and location of data. All personal information is held within the Beacon Membership System (except for accounting documents and original Membership Application forms), and the following table shows who has access to the data that the u3a holds. It also defines how long the data should be retained after use and what considerations need to be given to maintaining data security.

Note: Group Leaders may maintain a sub-list of their group members' information to facilitate communication within the group. Such information will be afforded the same quality of protection as the Beacon Membership System data.

Job Holder	Data Access	Purpose	Retention Policy	How secured
Chair	View contact details	Communication	Duration of membership plus the period until the December of the year following termination.	Password access to computer; Username/password access to Beacon System
Secretary	View contact details	Communication	Duration of membership plus the period until the December of the year following termination.	Password access to computer; Username/password access to Beacon System
Treasurer	Accounting information; View contact details	Accounting	Duration of membership plus the period until the December of the year following termination.	Password access to computer; Username/password access to Beacon System
Treasurer	View contact	Gift Aid	6 years plus current year to comply with	Password access to

	details		HMRC ruling.	computer; Username/password access to Beacon System
Membership Secretary	Full Membership List	Membership List Maintenance	Duration of membership plus the period until the December of the year following termination.	Password access to computer; Username/password access to Beacon System
New Members Secretary	Full Membership List	Communications	Duration of membership plus the period until the December of the year following termination.	Password access to computer; Username/password access to Beacon System
Newsletter Editor(s)	Full Membership List	Communications	Duration of membership plus the period until the December of the year following termination.	Password access to computer; Username/password access to Beacon System
Groups Coordinator	View contact details; group administration	Group Coordination	Duration of membership plus the period until the December of the year following termination.	Password access to computer; Username/password access to Beacon System
Group Leaders	View contact details; group info	Group Membership List maintenance; Communication	Duration of membership plus the period until the December of the year following termination.	Password access to computer; Username/password access to Beacon System
Beacon Administrator	Full access	Beacon administration	Up to 6 years plus current year if required for legal obligations. Otherwise, duration of membership plus the period until the December of the year following termination.	Password access to computer; Username/password access to Beacon System

Paper Documentation

In certain circumstances, the use of paper records is unavoidable (e.g. in accounting and membership application). In these circumstances, such records will be kept in a locked container to ensure data security and should be destroyed in accordance with the Retention Policy outlined above.