

1 INTRODUCTION

Waterlooville u3a treats the privacy of members' data seriously. This Data Protection Policy summarises the provisions of General Data Protection Regulations and the requirements that we have to collect and process information for membership purposes.

1.1 Meanings in this policy

- **We/Us/Our** means Waterlooville u3a
- **Trust** means the Third Age Trust (charity number 288007)
- **Committee** means an elected or co-opted member of the Waterlooville u3a Executive Committee

1.2 Scope of the policy

The policy details how personal information is collected, stored and managed in line with data protection principles and the General Data Protection Regulations. The policy is reviewed on an ongoing basis by Waterlooville u3a Committee members to ensure that we remain compliant. This policy should be read in tandem with our Privacy Policy.

1.3 Why this policy exists

This data protection policy ensures we :

- Comply with data protection law and follow good practice
- Protect the rights of our members
- Are open about how we store and process members data
- Protect Waterlooville u3a from the risks of a data breach

2 GENERAL GUIDELINES FOR COMMITTEE MEMBERS AND GROUP COORDINATORS

- The only people able to access data covered by this policy are those who need to communicate with or provide a service to Waterlooville u3a members.
- We provide training to Committee members and Group Coordinators to help them understand their responsibilities when handling data.
- Committee Members, Group Coordinators and authorised Volunteers are advised to keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords are encouraged and are never shared.
- Data should not be shared outside of the u3a unless with the prior consent of the member(s) concerned and/or for specific and agreed reasons. Examples would include Gift Aid information provided to HMRC or information provided to a distribution company for our own or Trust publications.
- To ensure accuracy, member information is refreshed periodically, usually via the membership renewal process or when policy is changed.

- Additional support is available to us from the Trust where uncertainties or incidents regarding data protection arise.

3 DATA PROTECTION PRINCIPLES

The General Data Protection Regulations identify key data protection principles :

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, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Principle 5 – Personal data must kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for the which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

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

4 LAWFUL, FAIR AND TRANSPARENT DATA PROCESSING

We request personal information from potential and current members for membership applications and for sending communications regarding members' involvement with us and our activities. Members are informed as to why the information is requested and what the information will be used for. The lawful basis for obtaining member information is due to the legitimate interest and contractual relationship that we have with individual members. In addition, members may be asked to provide consent for specific processing purposes such as the taking of photographs. Members are informed as to who they need to contact should they wish their data not to be used for specific purposes for which they have provided consent. Where these requests are received,

they are acted upon promptly and the member is informed as to when the action has been taken.

5 PROCESSED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

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

- Communicating with members about our events and activities
- Communicating with group members about specific group activities
- Member information provided to the distribution company that sends out the Trust publication – Third Age Matters - and member communications from us. Members are informed of this and that they have a choice as to whether or not they wish to receive these publications.
- Sending members information about Trust events and activities
- Communicating with members about their membership
- Communicating with members about specific issues that may arise during the course of their membership

We ensure that Group Coordinators and authorised Volunteers are made aware of what is considered appropriate and inappropriate communication. Inappropriate communication would include sending our members marketing and/or promotional materials from external service providers.

We ensure that members' information is managed in such a way as to not infringe an 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

6 ADEQUATE, RELEVANT AND LIMITED DATA PROCESSING

Our members are only asked to provide information that is relevant for membership purposes. This includes :

- Name
- Postal address
- Email address
- Telephone number(s)
- Gift Aid declaration

Where additional information may be required this is obtained with the consent of the member who is informed as to why this information is required and the purpose that it will be used for.

7 PHOTOGRAPHS

Photographs are classified as personal data.

Where a u3a event takes place (Open Day, Social, etc.) members should assume that photographs will normally be taken as a matter of course either by one or more U3A members or a photographer from local media or associated with any VIP guests. Prior advice regarding the possible taking of photographs at such events may be circulated with material advertising the event and a visible warning notice will be displayed at the main entry point for the event. Members not wishing to be in any such photographs are advised to ensure they are not within the vicinity of any photographer and to make their wishes known to the event organiser on the day.

Where group photographs are taken, members will be asked beforehand to step out of shot if they do not wish to be in the photograph. Otherwise consent is obtained from members in order for photographs to be taken and members are informed as to where photographs are displayed. Should a member wish at any time to remove their consent and to have their photograph removed or blurred they should advise the Secretary or a Committee member accordingly who will make the necessary arrangements.

8 ACCURACY OF DATA AND KEEPING DATA UP-TO-DATE

We have a responsibility to ensure members' information is kept up to date. Members are expected to let the Membership Secretary know if any of their personal information changes. The annual membership renewal process provides an opportunity for members to advise any changes in their personal information.

9 ACCOUNTABILITY AND GOVERNANCE

As Data Controller, members of the Committee are jointly responsible for ensuring that we remain compliant with data protection requirements and can evidence this. Where consent is required for specific purposes then evidence of this consent (either electronic or paper) is obtained and retained securely.

Members of the Committee ensure that new members joining the Committee receive training into the requirements of GDPR and the implications for their role. We ensure that Group Coordinators and authorised Volunteers are made aware of their responsibilities in relation to the data they hold and process. Members of the Committee are expected to keep up to date with guidance and practice within the u3a movement and to seek advice from the Trust should any uncertainties arise.

Members of the Committee review data protection requirements on an ongoing basis as well as reviewing who has access to data and how it is stored and deleted. When

Committee Members, Group Coordinators or authorised Volunteers relinquish their roles, they are asked to securely pass on data to those who need it and/or delete the data securely.

10 SECURE PROCESSING

Members of the Committee have a responsibility to ensure that data is both securely held and processed. This includes :

- Encouraging the use of strong passwords
- Discouraging the sharing of passwords
- Restricting access to member information to those Committee members and authorised Volunteers who need to communicate with members in order to perform their role within Waterlooville u3a
- Encouraging the use of password protection on any computing devices that contain personal information
- Encouraging the use of password protection, a membership database or secure cloud system when sharing data between Committee members, Group Coordinators or authorised Volunteers
- Ensuring there is firewall security installed on any/all computing devices used by Committee members and ensuring that the security is kept up to date

11 SUBJECT ACCESS REQUEST

Our members are entitled to request access to the information about them that is held by us. Such a request must be in writing to the Membership Secretary. On receipt of the request, it will be formally acknowledged and dealt with expediently, ideally within one month unless there are exceptional circumstances as to why the request cannot be granted. We will provide a written response detailing all information held on the member. A record will be kept of the date of the request, who has dealt with it and the date of the response.

12 DATA BREACH NOTIFICATION

Were a data breach to occur, action will be taken to minimise any potential harm. This will include ensuring that all of the Committee are made aware that a breach has taken place and how the breach occurred. The Committee will endeavour to rectify the cause of the breach as soon as possible to prevent any further breaches. The Chair of Waterlooville u3a will notify the Trust as soon as possible after the breach has occurred. Discussions will take place between the Chair and the Trust as to the extent of the breach, any action to be taken and, where necessary, notification of the Information Commissioner's Office. The Committee will also contact the relevant members to inform them of the data breach and any actions taken to resolve the breach.

Where a member feels that there has been a data breach they will provide outline details to any Committee member who will ask the member to provide an outline of the breach. If the initial contact is verbal, the member will be asked to follow this up with written confirmation detailing their concern. The alleged breach will be investigated by Committee members who are not in any way implicated in the breach. Where the Committee needs support or if the breach is serious, they will notify and consult the Trust. The member will also be informed that they can report their concerns to the Trust if they are not satisfied with our response. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.

13 AVAILABILITY AND CHANGES TO THIS POLICY

This policy is available in the Members' Area of our website (waterloovilleu3a.org.uk) and upon request to the Secretary or any Committee member. This policy may change from time to time and the latest version will always be available on our website (www.waterloovilleu3a.org.uk). Members will be informed of any material change to this policy via member/Committee updates.

14. QUERIES

If you have any questions regarding this Policy or the way we use your personal data, please contact the Secretary :

- email to secretary@waterloovilleu3a.org.uk

15 ADOPTION AND REVIEW

This policy was adopted at the Committee meeting held on 19th October, 2022.

Policy review date : April 2025.

Document history	
<i>Unknown</i>	<i>First issue</i>
<i>May 2018 : Kevin Stock</i>	<i>Replaced all previous content with sample wording provided by Third Age Trust, tailored to Waterlooville U3A</i>
<i>October 2022 : Third Age Trust Angela Chapman Committee discussions 19 Oct 2022</i>	<i>Replaced all previous content with sample wording provided by Third Age Trust, tailored to Waterlooville U3A Added new section 15 "Adoption and Review" Added header, footer & page numbers General reformatting</i>
<i>March 2023 : Angela Chapman</i>	<i>Updated S14 with new Business Secretary postal address</i>
<i>March 2024 : Angela Chapman per Committee discussions 17 Jan 2024 & 21 Feb 2024.</i>	<i>Replaced "U3A" with "u3a" Removed Secretary's postal address from S14 Changed review date from October 2023 to April 2025</i>