

Wadhurst U3A Data Protection Policy

SCOPE OF THE POLICY

This policy applies to the work of Wadhurst U3A (hereafter 'the U3A'). The policy sets out the requirements that the U3A has to gather personal information for membership purposes. The policy details how personal information will be gathered, stored and managed in line with data protection principles and the General Data Protection Regulation. The policy is reviewed on an ongoing basis by the U3A committee members to ensure that the U3A is compliant. This policy should be read in tandem with the U3A's Privacy Policy.

WHY THIS POLICY EXISTS

This data protection policy ensures that the U3A:

- Complies with data protection law and follows good practice
- Protects the rights of members and other U3A partners
- Is open about how it stores and processes members data
- Protects itself from the risks of a data breach.

GENERAL GUIDELINES FOR COMMITTEE MEMBERS AND GROUP CONVENORS

- The only people able to access data covered by this policy should be those who need to communicate with or provide a service to the members of the U3A
- Data should not be shared informally or outside the U3A
- The U3A will provide induction training to committee members and group convenors to help them understand their responsibilities when handling personal data
- Committee members and group convenors should keep all data secure, by taking sensible precautions and following the guidelines below
- Passwords must be used, and they should never be shared
- Personal data should not be shared outside the U3A without prior consent and/or for specific and agreed reasons
- Membership information should be reviewed, and consent refreshed periodically via the membership renewal process or when policy is changed
- We shall seek advice/guidance from the Third Age Trust National Office if we are unsure about any aspect of data protection.

DATA PROTECTION PRINCIPLES

The General Data Protection Regulation identifies 8 data protection principles.

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

Principle 2 - Personal data can only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Principle 3 - The collection of personal data must be adequate, relevant and limited to what is necessary compared to the purpose(s) data is collected for.

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 are erased or rectified without delay.

Principle 5 – Personal data which is kept in a form which permits identification of individuals shall not be kept for longer than is necessary.

Principle 6 - Personal data must be processed in accordance with the individuals' rights.

Principle 7 - Personal data must be processed in 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.

Principle 8 - Personal data cannot be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal data.

Lawful, fair and transparent data processing

The U3A requests personal information from potential members and members for the purpose of sending communications about their involvement with the U3A. The forms used to request personal information will contain a privacy statement informing potential members and members as to why the information is being requested and what the information will be used for. Members will be asked to provide consent for their data to be held and a record of this consent along with member information will be securely held. U3A members will be informed that they can, at any time, remove their consent and will be informed as to who to contact should they wish to do so. Once a U3A member requests not to receive certain communications this will be acted upon promptly and the member will be informed as to when the action has been taken.

Processed for Specified, Explicit and Legitimate Purposes

Members will be informed as to how their information will be used and the Committee of the U3A will seek to ensure that member information is not used inappropriately.

The information you have supplied to us will be stored securely for membership purposes and used by Wadhurst U3A in the following ways:

- Communicating with members about the U3A's events and activities
- Enabling Group Conveners to contact their group members about activities
- Communicating with members about their membership and renewals
- Communicating with members about specific U3A issues that may have arisen
- Notifying HMRC that you wish to Gift Aid your membership fee (if applicable)
- Sending members information about events and activities organised by the Third Age Trust (the U3A national organisation)
- Sharing members' name and address details with the Third Age Trust for direct mailing of its magazines: *Third Age Matters* and *Sources*, and with our nominated print/ mailing company for the distribution of our *Wadhurst U3A News* magazine.

The U3A will ensure that group convenors are made aware of what would be considered appropriate and inappropriate communication.

The U3A will 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.

Adequate, Relevant and Limited Data Processing

Members of the U3A will only be asked to provide information that is relevant for membership purposes. This will include:

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

Where the U3A organises a trip or external activity, members may be asked to provide emergency contact details.

There may be occasional instances where a members' data needs to be shared with a third party due to an accident or incident involving statutory authorities. Where it is in the best interests of the member and the U3A has a substantiated concern, then consent does not have to be sought from the member.

Accuracy of Data and Keeping Data up to Date

The U3A has a responsibility to ensure members' information is kept up to date. Members should inform the membership secretary of any changes in their personal information. In addition, on an annual basis the membership renewal forms will provide an opportunity for members to resubmit their personal information and reconfirm their consent for the U3A to use their data for the purposes described above.

Accountability and Governance

The U3A Committee are responsible for ensuring that the U3A remains compliant with data protection legislation and can evidence this. Members consent will be held securely held as evidence of compliance.

All new U3A Committee members will receive an induction into how data protection is managed within the U3A and the reasons for this. Committee members will 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 U3A Committee will review its data protection arrangements on a regular basis, at least annually.

Secure Processing

The committee members of the U3A have a responsibility to ensure that data is both securely held and processed. This will include:

- Committee members using strong passwords
- Committee members 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 devices that contain or access personal information
- Using password protection or secure cloud systems when sharing data between committee members and/or group convenors.

Committee members should ensure appropriate security and virus checking software is installed on all devices used to access member information.

The committee will seek assurance that the systems and procedures of all third parties are secure and comply with current legislation.

Subject Access Request

U3A members are entitled to request access to the information that is held by the U3A. The request needs to be received in the form of a written request to the Membership Secretary of the U3A. On receipt of the request, the request will be formally acknowledged and dealt with within 14 days 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.

Data Breach Notification

Should a data breach occur, action shall be taken to minimise the harm by ensuring all committee members are aware that a breach has taken place and how the breach has occurred. The committee shall then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. The Chair of the U3A shall contact National Office within 24 hours of the breach occurring to notify of the breach. A discussion shall take place between the Chair and National Office as to the seriousness of the breach, and any actions to be taken. The committee will also contact the relevant U3A members to inform them of the data breach and actions taken to resolve the breach.

If a member contacts the U3A to report a suspected breach, a committee member will ask the member to provide an outline of their concerns. If the initial contact is by telephone, a nominated committee member will ask the member to follow this up with an email or a letter detailing their concern. The concern 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 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.

Date of Policy: April 2018

Next Review Date: April 2019