



THE UNIVERSITY OF THE THIRD AGE

## SHIPSTON ON STOUR AREA U3A DATA PROTECTION & PRIVACY POLICY

[u3asites.org.uk/shipston-on-stour](http://u3asites.org.uk/shipston-on-stour)

### CONTENTS

1. Scope of the policy .....	p2
2. Why this policy exists.....	p2
3. Data protection principles .....	p2
3.1 Lawful, fair and transparent data processing.....	p3
3.2 Specified, explicit and legitimate purposes .....	p4
3.3 Adequate, relevant and limited data processing .....	p4
3.4 Accuracy and currency of data .....	p5
3.5 Secure processing.....	p5
3.6 Subject access request .....	p6
3.7 Data breach notification .....	p6
4. Accountability and governance .....	p6
5. How do we use your personal information? .....	p7
6. Who do we share your personal information with? .....	p7
7. How long does the U3A keep your personal information? ..	p7
8. General guidelines for EC members and group leaders ...	p8
9. Committee members additional consent .....	p8
10. Membership secretary additional consent .....	p8
11. Group leaders additional consent .....	p9
12. Web contact details .....	p9
13. Photographs .....	p9
14. Availability and changes to this policy .....	p9
15. Contact.....	p10

## **1. Scope of the policy**

This policy applies to the operation of Shipston on Stour Area U3A (hereafter 'the U3A' or 'we'). The policy identifies that the U3A has to gather and share personal information for membership purposes. The policy details how personal information will be gathered, stored, managed and shared in line with data protection principles and the General Data Protection Regulation (hereafter 'GDPR'). The policy is reviewed on an ongoing basis by the U3A executive committee to ensure that the U3A remains compliant.

The first part of this policy explains some of the Data Protection principles and the later parts give details of the U3A's compliance.

## **2. 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.
- Is open about how it stores and processes members' data.
- Protects itself from the risks of a data breach.

## **3. 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 considering the purpose(s) for which the data is collected.
- 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 individual's 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.

### **3.1 Lawful, fair and transparent data processing**

The regulation requires, in the first instance, that the organisation defines and document its Lawful Basis for the collection, storage and processing of personal data. The documentation forms part of this Policy.

The primary Lawful Basis for the U3A shall be that of Consent. Consent shall be the basis for the normal processing of members personal data.

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 (total or to restrict processing) and will be informed on the consent form, as to whom 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.

A full removal of consent to collect and process their data would make their membership very difficult to manage. The member shall be advised that, although their membership is not being terminated (it is against the law to do this) they will have to rely on general publicised information or to seek out what they are looking for at the monthly meeting etc. The U3A would have to advise Group Leaders etc. that the particular member has withdrawn their consent.

The processing of next-of-kin and emergency contact details shall be permissible under the Legitimate Interest lawful basis.

To rely on “legitimate interest” as a lawful basis, the GDPR requires the U3A to carry out an assessment and balancing of the risks and benefits of such processing. This is referred to by the Information Commissioner’s Office (ICO) as a legitimate interest assessment (LIA) and can be broken down into a 3-part test:

- Purpose test: Are you pursuing a legitimate interest? Here the U3A would be processing the data to ensure that it can contact a member’s nominated relative or contact in case something happens to that member. The data would not be used in any other way, including in an unethical or unlawful way. Both the member and the relative/contact would effectively and positively benefit from the processing.
- Necessity test: Is the processing necessary for that purpose? Without such processing there could be a risk of a member’s relative or contact not being informed of something that happened to that member and not being able to do anything about it – which would be a worst outcome for both the member and the next of kin. Such processing is a targeted and proportionate way of achieving the U3A purpose. There does not seem to be a less intrusive way of achieving that purpose. Indeed, it would be too cumbersome or difficult to get that next of kin’s consent before processing the data; relying on Legitimate Interest is a reasonable way to process such data.
- Balancing test: Do the individual’s interests override the legitimate interest? The data collected (name, address and phone number) is personal data, but is not extensive or sensitive. The individual would expect their data to be collected in such a way and is

unlikely to object to such processing or to find such processing intrusive. The processing is unlikely to have a negative impact on the individual.

### **3.2 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. Appropriate use of information provided by members shall be limited to:

- Communicating with members about the U3A's events and activities
- Group leaders communicating with their group members about specific group 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.
- Sending members information about Third Age Trust events and activities.
- Communicating with members about external matters that the U3A consider may be of interest and/or benefit.
- Adding members' details to the direct mailing information for the Third Age Trust magazines – Third Age Matters and Sources where requested.
- Communicating with HMRC regarding gift aid donation.

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 and divulging the personal information outside the U3A.

The U3A will ensure that members' information is managed in such a way as not to infringe 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.

### **3.3 Adequate, Relevant and Limited Data Processing**

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

1. Name.
2. Postal address.
3. Email address (where relevant).
4. Telephone number.
5. TAM magazine preferences.
6. Gift Aid declaration.

This information is provided on the initial/renewal membership form (hereafter 'membership form'). Items 1 to 4 are the subject of a specific consent clause and tick box on the form. Where information is given the Consent authorises the U3A to use whichever method (post,

email and phone) is appropriate at the time. The U3A would prefer to use email whenever appropriate, but members can restrict the method of communication by not providing the necessary data.

Items 5 and 6 are the subject of two separate consent clauses and tick boxes as they involve sending the data outside of the U3A and to different organisations. Consent to item 5 gives consent to inform the TAT of the member's address for mailing purposes.

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

All U3A members will be encouraged to provide, or make available when required, next of kin or other emergency contact details. Processing of this data shall be authorised under Legitimate Interest as described above. Were this information to be needed as a one-off for a particular trip or event then the information will be deleted once that event or trip has taken place unless it was to be required – with agreement – for a longer purpose. The same would apply to carers who may attend either a one-off event or on an ongoing basis to support a U3A member with the agreement of the U3A.

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. This distribution of next of kin/emergency contact details is covered under the Legitimate Interest lawful basis. This Policy shall not prevent any member using another member's data when there is an emergency, and when it is in their best interest to do so.

### **3.4 Accuracy and Currency of Data**

The U3A has a responsibility to ensure members' information is kept up to date. Members will be requested to inform the membership secretary if any of their personal information changes. In addition, on an annual basis the membership forms will provide an opportunity for members to resubmit their personal information and reconfirm their consent for the U3A to process their data.

### **3.5 Secure Processing**

The committee members and any member legitimately holding members' personal data have a responsibility to ensure that data is both securely held and processed. This will include:

- Using strong passwords. The normal advice is 8 characters minimum with a mixture of UPPER CASE, lower case, numbers and allowable symbols.
- Not sharing passwords.
- Restricting access of sharing member information only to those who need to communicate with members on a regular basis.
- Using password protection on laptops and PCs that contain or access personal information.
- Using password protection or secure cloud systems when sharing data between committee members and/or group leaders.
- Paying for firewall security to be put onto committee members' laptops or other devices.

### **3.6 Subject Access Request**

U3A members are entitled to request access to their own personal data 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. The contact details will be on the membership form, correct at the time of membership renewal but if out of date, from the U3A website or any committee member. 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.

### **3.7 Data Breach Notification**

A data breach is defined as any sharing of personal data beyond the scope of the Consent. If a U3A member contacts the U3A to say that they feel that there has been a breach by the U3A, the concern will be investigated by members of the committee who are not in any way implicated in the alleged 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.

Where a data breach has been identified, action shall be taken to minimise the harm by ensuring all committee members are aware that a breach had taken place and how the breach had occurred. The committee shall then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. In the case of a serious breach, an officer of the U3A shall contact National Office within 24 hours of the breach being identified, to notify of the breach. A discussion would 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 shall also contact the relevant U3A members to inform them of the data breach and actions taken to resolve the breach.

## **4. Accountability and Governance**

The U3A committee are responsible for ensuring that the U3A remains compliant with data protection requirements and can provide evidence that it is. For this purpose, those from whom data is required will be asked to provide written consent. The evidence of this consent will then be securely held as evidence of compliance. The U3A committee shall ensure that new members joining the committee receive information about how data protection is managed within the U3A and the reasons for this. 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 and who has access to information on a regular basis as well as reviewing what data is held.

The EC shall appoint a Data Controller who shall be responsible for implementing the data protection aspects of this Policy and shall act as the first point of call in any matter relating to this Policy. The Data Controller holds the master copy of the members' data base and is responsible for ensuring that only appropriate use is made of these data by data

processors. The Data Controller shall be the Membership Secretary who must also be a committee member.

Other members as described in this document are permitted to use some or all of the personal data held by the membership secretary. These persons are referred to in the legislation as Data Processors. The Data Controller is also a Data Processor.

## **5. How do we use your personal information?**

We use your personal information:

- To provide our U3A activities and services to you.
- For administration, planning and management of our U3A.
- To communicate with you about your group activities.
- To monitor, develop and improve the provision of our U3A activities.

We'll send you messages by email, other digital methods, telephone and post to advise you of U3A activities.

## **6. Who do we share your personal information with?**

We may disclose information about you, including your personal information:

- Internally - to committee members and other members –but only as required to facilitate your participation in our U3A activities. This includes, the business secretary, treasurer, interest group leaders and any member of a membership subcommittee assisting with any processing of the data, e.g. for membership renewal or meeting invitations.
- Externally –With your consent for direct mailing for the Trust magazines (Third Age Matters and Sources). Your gift aid consent will be shared with HMRC as you have agreed to this on your membership form.
- If we have a statutory duty to disclose it for other legal and regulatory reasons.

Where we need to share your information outside of the U3A in addition to that stated above, we will seek your permission and inform you as to whom the information will be shared with and for what purpose.

## **7. How long do we keep your personal information?**

The U3A needs to keep your information so that we can provide our services to you. In most instances information about your membership will not be stored for longer than 15 months. The exceptions to this are instances where there may be legal or insurance circumstances that require information to be held for longer whilst this is investigated and resolved. Where this is the case then the member(s) will be informed as to how long the information will be held and when it is deleted.

Your information is refreshed each year by submitting a new membership form.

If a member does not renew after a reasonable time (45 days) and after reasonable attempts to contact the member, their membership will be cancelled and the data erased. The member will be informed in the final communication, that this is the case.

## **8. General guidelines for committee members and group leaders**

- The only people able to access data covered by this policy shall be those who need to communicate with or provide a service to the members of the U3A.
- Data shall not be shared informally inside or outside the U3A
- The U3A will provide or make available copies of this policy.
- Committee members and group leaders will not, in general, have free access to members' data.
- Any member having a legitimate reason to communicate with any or all members shall address their request to the membership secretary, who will respond appropriately. Note that communications about non-U3A activities may require Committee approval.
- Committee members and group leaders should keep all data secure, by taking sensible precautions and following the guidelines below.
- Committee members will need to have free access to each other committee members' data for the purposes of ready communications between them. A list of names, addresses, phone numbers and email addresses shall be maintained by the Business Secretary and emailed/handed to each committee member. Approval to share data in this manner and for this purpose shall be subject to specific consent (see below).
- Personal data collected by interest group leaders shall be the minimum necessary to fulfil the immediately foreseeable requirements and shall be deleted when no further use is foreseen.
- Personal data shall not be shared outside the U3A unless with prior consent and for specific and agreed purposes.
- Particular care must be taken not to divulge a person's home address unless specific consent is given either in writing or verbally.
- Member information will be reviewed and consent refreshed periodically via the membership renewal process or when policy is changed.
- The U3A should request help from National Office if they are unsure about any aspect of data protection.
- To maximise privacy, unless specifically necessary, recipients email addresses shall be rendered invisible. This can normally be achieved by blind carbon copying (Bcc) instead of carbon copying (Cc). Some email clients and services may employ other methods. Exceptions are permitted for communications between committee members (see below) and within interest groups, where knowledge of all recipients is desirable or necessary.

## **9. Committee members additional consent**

Committee members will be requested to consent to the sharing of their name, email address, telephone number and address, by consenting to this whenever a new committee contact information list is produced and distributed. Committee members are allowed under the GDPR to refuse this consent, under which situation, an alternative means of communication shall be agreed if practical.

## **10. Membership secretary additional consent**

The membership secretary is normally the principal contact for members and prospective members. His/her contact details, name, phone number, email address (possibly anonymised) and home address, are freely given on publicity material and enrolment forms etc. To facilitate the smooth running of the U3A, the membership secretary and any member of a membership subcommittee will be requested to consent to this personal data being freely and publicly shared.

## **11. Group leaders additional consent**

Group Leaders' contact details (name, phone number, and/or email address) are publicised freely amongst the membership and visitors, in order to facilitate contacts from interested members. As this is outside the normal members' data consent, a separate consent will be required. This will be incorporated in the Group Leaders Handbook. A group leader is permitted to refuse this consent under which circumstances, other communications means will need to be put in place.

## **12. Web contact details**

Certain officers and holders of specific functions can be contacted by the general public through the SOSAU3A Website. These contacts are anonymised such that, in the first instance, the sender will not know the recipients identity or contact details. The recipient can, if willing, reply using their personal email address, but an anonymised address may be provided if requested. The members currently affected are:

- Treasurer
- Business secretary
- Membership secretary
- Groups coordinator
- Speakers secretary

This list will be reviewed as necessary or as requested.

## **13. Photographs**

- Photographs are considered to be personal data and hence come under the control of the GDPR.
- On any occasion that photos are being taken at a U3A event for subsequent SOSAU3A publication, members should be advised beforehand and given the opportunity to opt out of the photo.
- Any photo which is published, shall not state the name of any person shown, unless specific written permission is obtained from the person concerned. A consent form will be provided for this.
- No photo shall be taken of any minor (under 18 yrs), without the written permission of their parent or guardian. A consent form will be provided for this.
- The consent given on the membership form, shall allow the display of anonymised photos in SOSAU3A publication (newsletters, website, PowerPoint presentations etc.). This consent shall not permit the display of these photographs outside SOSAU3A (including U3A Central Office) without additional explicit permission.

## **14. Availability and changes to this policy**

This policy will be made available on the SOSAU3A web site and at the monthly meetings. An electronic copy (preferred) or printed copy will be sent to anyone requesting it. This policy may change from time to time. If material changes are made, the U3A will make members aware of this via the 'Your News' newsletter and the monthly members' meetings.

## **15. Contact**

If you have any queries about this policy, need it in an alternative format, or have any complaints about our privacy practices, please contact, in the first instance, the Membership Secretary in his/her capacity as the Data Controller.

The Membership Secretary shall, if not able to resolve the matter, refer the matter to the committee through any of the appointed Officers.

Policy review date: