

Sheffield U3A Data Protection Policy

Scope of the policy

This policy applies to the work of SU3A. This policy sets out why SU3A has to gather 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. All data mentioned in this document refers to Personal Data only. The policy is reviewed on an annual basis by SU3A Executive Committee members to ensure that we are compliant. This policy should be read in tandem with SU3A's Privacy Policy.

Why this policy exists

This data protection policy ensures SU3A:

- 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

General guidelines for Executive Committee members and Group Coordinators

- The only people able to access data covered by this policy should be those who need to communicate with or provide a service to SU3A members.
- SU3A will provide induction training to Executive Committee members and relevant guidance to Group Coordinators to help them understand their responsibilities when handling data.
- Committee Members and Group Coordinators should keep all data secure, by taking sensible precautions and following the guidelines below.
- For data stored electronically, 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, for example 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:

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 be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for 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 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.

Lawful, fair and transparent data processing

SU3A requests personal information from potential members and members for membership applications and for 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. The lawful basis for obtaining member information is due to the contractual relationship that SU3A has with individual members. In addition members will be asked to provide consent for specific processing purposes. SU3A members will be informed as to who 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.

Processed for specified, explicit and legitimate purposes

Members will be informed as to how their information will be used and the Executive committee and Group Coordinators of SU3A will seek to ensure that member information is not used inappropriately. Appropriate use of information provided by members will include:

- Communicating with members about SU3A events and activities
- General and Group Coordinators communicating with Group members about specific Group activities
- Consent will be sought in order to add member's details to the direct mailing information for the Third Age Trust magazines – Third Age Matters and Sources and SU3A *Links*
- 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

SU3A will ensure that Group Coordinators are made aware of what would be considered appropriate and inappropriate communication. Inappropriate communication would include sending SU3A members marketing and/or promotional materials from external service providers.

SU3A 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 object

Adequate, relevant and limited data processing

Members of SU3A 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
- Year of birth

Where additional information may be required such as health related information 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.

Where SU3A organises a trip or activity that requires next of kin information to be provided, a legitimate interest assessment will have been completed in order to request this information. Members will be made aware that the assessment has been completed.

Photographs

Photographs are classified as personal data. Where member's 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 Group Coordinator that they no longer wish their photograph to be displayed

Accuracy of data and keeping data up-to-date

SU3A has a responsibility to ensure members' information is kept up to date. Members will be informed to update their personal information online via Wild Apricot or let the Membership Team 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 update their personal information

Accountability and governance

The SU3A Executive Committee are responsible for ensuring that SU3A remains compliant with data protection requirements and can 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. The SU3A Committee will ensure that new members joining the Executive Committee receive an induction into the requirements of GDPR and the implications for their role.

SU3A will also ensure that Group Coordinators are made aware of their responsibilities in relation to the data they hold and process. Executive Committee members shall stay up to date with guidance and practice within the SU3A movement and shall seek additional input from the Third Age Trust National Office should any uncertainties arise. The Executive Committee will review data protection

and who has access to information on a regular basis as well as reviewing what data is held. When Executive Committee Members, General Coordinators and Group Coordinators relinquish their roles, they will be asked to either pass on data to those who need it and/or delete data.

Secure Processing

SU3A Executive Committee members have a responsibility to ensure that data is both securely held and processed. This will include:

- Restricting access of sharing member information to those on the Executive Committee and members approved by the Executive Committee who need to communicate with members on a regular basis
- Using password protection on laptops and PCs that contain personal information
- Executive Committee members, Group Coordinators and those appointed by the Executive Committee to help with the administration of SU3A should ensure that Firewall Securing is on when using PCs and other electronic devices.

Subject Access Request

SU3A members are entitled to request access to the information that is held by SU3A. The request needs to be received in the form of a written request to the Membership Team of SU3A. On receipt of the request, the request will be formally acknowledged and dealt with expediently unless there are exceptional circumstances as to why the request cannot be granted. SU3A 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

Were a data breach to occur action shall be taken to minimise the harm. This will include ensuring that all SU3A Executive Committee members are made aware that a breach has taken place and how the breach occurred. The Executive Committee shall then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. The Chair of SU3A shall contact National Office within 24 hours of the breach occurring to notify 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 Chair shall also contact the relevant SU3A members to inform them of the data breach and actions taken to resolve the breach.

Where a SU3A member feels that there has been a breach by the U3A, an Executive Committee member will ask the member to provide an outline of the breach. If the initial contact is by telephone, the Executive Committee member will ask the SU3A 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 Executive Committee who are not in any way implicated in the breach. Where the Executive Committee needs support or if the breach is serious they should notify National Office. The SU3A 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.