

Bristol u3a Data Protection Policy

Created Author/Date	Updated Author/Date	Approved by Exec Committee/Date	Review Date
Secretary 17 Dec 2020	KP Apr 2023	2 May 2023	May 2023

Scope of the Policy

This policy applies to the work of Bristol u3a (hereafter 'the u3a'). The policy sets out the requirements that the u3a has to gather personal information. The policy explains in broad terms how such personal information will be gathered, stored and managed in line with the principles of the General Data Protection Regulation. The policy is reviewed from time to time by the u3a Executive Committee members to ensure that the u3a remains compliant. This policy should be read in tandem with the u3a's Data Protection Code of Practice.

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 stakeholders.
- Is open about how it stores and processes member data.
- Protects itself from the risks of a data breach.

Data Protection Principles

The General Data Protection Regulation identifies six 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 for the purpose(s) it is collected for.

Principle 4 – Personal data held should be accurate and 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 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 1 - 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 including recording and updating membership status. The forms used to request personal information shall 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.

Principle 2 - Processed for Specified, Explicit and Legitimate Purposes

Members shall be informed as to how their information will be used. The Executive Committee shall seek to ensure that member information is not used inappropriately. Appropriate use of information provided by members will **only include**:

- Communicating with members about the u3a's events and activities
- Statistical analysis to further the development and efficient operation of the u3a
- Group convenors/leaders communicating with their group members about specific group activities.
- Adding member 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.
- Aiding the u3a's administrative and financial management
- Sending member information to HMRC to support the Gift Aid declaration, subject to explicit consent.

Principle 3 - Adequate, Relevant and Limited Data Processing

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

- Name
- Gender
- Emergency contact details
- Postal address
- Email address
- Mailing preferences
- Telephone number(s)
- Gift Aid declaration

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.

Principle 4 - Accuracy of Data and Keeping Data up to Date

Members will be able to inform the membership secretary if any of their personal information changes. In addition, on an annual basis membership renewal forms will provide an opportunity for members to resubmit their personal information and reconfirm their consent for the u3a to communicate with them.

Principle 5 – Storage Limitation

Membership data will be retained insofar as it is necessary to meet the specified, explicit and legitimate purposes identified by this policy. This includes retention of personal information of former members for the purposes of compliance with HMRC Gift Aid requirements and for statistical analysis for the development and effective operation of the u3a.

Principle 6 – Integrity and Secure Processing

The Executive Committee will develop a Code of Practice applicable to its own members, to Group Leaders and to others who may have a legitimate requirement to work with personal data. The Executive Committee will also develop a Service Continuity Plan describing how data processing resources will be securely operated and protected.

Accountability and Governance

The Executive Committee is responsible for ensuring that Bristol u3a remains compliant with data protection requirements and for ensuring the availability of evidence to this effect. For this purpose, those from whom data is required will be asked to provide their written consent. The evidence of this consent will then be securely held as evidence of compliance. The Executive Committee shall ensure that new members joining the committee receive an induction into how data protection is managed within the u3a and the reasons for this. Executive 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

Executive Committee will review data protection policy and practice and who has access to information on a regular basis.

Any person with access to the u3a membership data will be required to sign a Data Protection Agreement in which they confirm their obligation to respect the privacy and security of confidential and private data to which they have access in the course of their u3a activities. These declarations will be retained by the Data Protection Officer, if appointed. Currently this responsibility lies with the Secretary.

The Executive Committee should appoint a Data Protection Officer to be its principle point of contact for Data Protection issues; until then this responsibility rests with the Secretary. The committee shall nevertheless retain collective responsibility for Data Protection compliance.

International Transfers

The u3a has no requirement to transfer personal data outside the UK and does not intend to do so.

Protection of Rights

The u3a acknowledges that members' information must be managed in such a way as not to infringe 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.

Subject Access Request

Bristol u3a members are entitled to request access to the information that is held by Bristol u3a. The request needs to be received in the form of a written request to the Secretary. 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. Bristol 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

In the event of a data breach action shall be taken to minimise the harm by ensuring all Executive 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 Bristol u3a shall notify the TAT National Office of the breach within 24 hours of becoming aware of it. A discussion should take place between the Chair and National Office as to the seriousness of the breach and action to be taken. Where necessary, the Information Commissioner's Office would be notified. The committee should also contact the relevant u3a member(s) to inform them of the data breach and actions taken to resolve the breach.

If a member contacts Bristol u3a to say that they feel that there has been a breach by the u3a, the Data Protection Officer (or nominated alternate) will ask the member to provide an outline of their concerns. If the initial contact is by telephone, the u3a member will be asked 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 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.