

Leicester U3A - LEICESTER U3A DATA PROTECTION POLICY

SCOPE OF THE POLICY This policy applies to the work of Leicester 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 collected, stored and managed in line with data protection principles and the General Data Protection Regulation (GDPR). 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 Leicester U3A's Privacy Policy.

WHY THIS POLICY EXISTS

This data protection policy ensures that the U3A:

- Complies with data protection law (GDPR) 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 COMMITTEE MEMBERS, CONVENORS AND RESPONSIBLE PERSONS

- 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.
- The U3A will provide induction training to committee members, group convenors and authorised responsible persons 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.
- Strong passwords must be used and they should never be shared.
- Personal data should not be shared outside of the U3A unless with prior consent and/or for specific and agreed reasons. Examples would include 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 support 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 can only 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 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; 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

The U3A 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 the contractual relationship that the U3A has with individual members. In addition, members will be asked to provide consent for specific processing purposes such as the taking of photographs. U3A 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 had 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 Committee of the U3A will seek to ensure that member information is not used inappropriately.

Appropriate use of information provided by members will include:

- Communicating with members about the U3A's events and activities.
- Group convenors communicating with their group members about specific group activities.
- Consent will be sought in order to add members' details to the direct mailing information for the Third Age Trust publications.
- Sending members information about Third Age Trust events and activities.
- Sending members information about relevant educational events and research projects asking for volunteers.
- 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.

The U3A will ensure that group convenors 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.

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.
- Mobile number
- Gift Aid entitlement
- Membership of other U3As
- Name of any other Leicester U3A member resident at the same address.
- Emergency contact details (for specific trips or events).

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. In light of recent pandemic, visitors will also be required to give name and address for the purposes of 'track and trace'. These will be destroyed after a suitable quarantine period as applied by government advise.

Where the U3A organises a trip that requires emergency contact information to be provided, the '**legitimate interest statement**' applies (see separate document). Members will be made aware that the assessment has been completed. The U3A will require the member to gain consent from the identified contact. The consent will provide permission for the information to be held for the purpose of supporting and safeguarding the member in question. 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 were to be required – with agreement – 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 member's 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 or the U3A in these instances where the U3A has a substantiated concern then consent does not have to be sought from the member.

Photographs

Photographs are classified as personal data. Where group photographs are being taken members will be asked to step out of shot if they do not 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 Secretary to advise that they no longer wish their photograph to be displayed.

Accuracy of Data and Keeping Data up to Date

The U3A has a responsibility to ensure members' information is kept up to date. Members will be informed to let the membership secretary know if any of their personal information changes. In addition, on an annual basis the membership renewal forms will provide an opportunity for members to inform the U3A as to any changes in their personal information and to reconfirm their consent where applicable.

Accountability and Governance

The U3A Committee are responsible for ensuring that the U3A 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 U3A Committee shall ensure that new members joining the Committee receive an induction into the requirements of GDPR and the implications for their role.

The U3A will also ensure that group convenors and other authorised responsible persons are made aware of their responsibilities in relation to the data they hold and process. 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. When Committee members, convenors and other authorised responsible persons relinquish their roles, they will be asked to either pass on data to those who need it and/or delete it.

Secure Processing

Access to member information is restricted to committee members, convenors and responsible persons who need it for specified, explicit and legitimate purposes as given above and are authorised by the committee. They have a responsibility to ensure that data is both securely held and processed. This will include:

- Using strong passwords.
- Not sharing passwords.
- Using member information only for those specified, explicit and legitimate purposes authorised by the committee.
- 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, group convenors and responsible persons.

The committee will endeavour to ensure that all relevant persons have up-to-date anti-virus protection and firewall security on their devices.

The U3A has contracted for services from the following 3rd party data processors:

- the online management system Beacon and Direct Mail for the distribution of Third Age Trust magazines through the Third Age Trust. The committee is responsible for confirming with the Third Age Trust that these suppliers are GDPR compliant.
- NamesCo for forwarding of generic emails. The committee is responsible for satisfying itself that this company is GDPR compliant.

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 expediently (generally one month) 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

Were a data breach to occur 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.
- The Chair of the U3A shall contact National Office as soon as possible after 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 committee shall also contact the relevant U3A members to inform them of the data breach and actions taken to resolve the breach.

Where a U3A member feels that there has been a breach by the U3A, a committee member will ask the member to provide an outline of the breach. If the initial contact is by telephone, the committee member will ask the U3A 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 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.

Approved: 27 May 2018

Reviewed November 2021

Next review due November 2024