

# Kettering U3A Data Protection Policy

## SCOPE OF THE POLICY

This policy applies to the work of Kettering 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 UK General Data Protection Regulation (UK-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 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, staff, customers and 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 LEADERS

- 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 of the U3A.
- The U3A will provide induction training to committee members and group leaders to help them understand their responsibilities when handling personal data.
- Committee Members and group leaders 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.
- Member information should be updated whenever a member informs the secretary of a change or when policy is changed.
- U3As should request help from National Office if they are unsure about any aspect of data protection.
- When taking a photograph,

## DATA PROTECTION PRINCIPLES

*Article 5 of the UK General Data Protection Regulation sets out 7 key principles which lie at the heart of the general data protection regime.*

*Article 5(1) requires that personal data shall be:*

*“(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');*

*(b) 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 ('purpose limitation');*

*(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*

*(d) 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 ('accuracy');*

*(e) 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 ('storage limitation');*

*(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."*

Article 5(2) adds that:

*"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')"*

### **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. When first joining and completing a membership application form, 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. Appropriate use of information provided by members will include:

- Communicating with members about the U3A's events and activities
- Group leaders communicating with their group members about specific group activities.
- Adding member's details to the direct mailing information.
- 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.
- Publishing photographs on the u3a web site, u3a newsletter, projecting them at monthly meetings and adding to the u3a Facebook page

### **Photographs**

Photographs constitute personal data. Where group photographs are being taken it is sufficient to ask any members of the group who don't wish to be in the photograph to move out of shot.

The u3a may need retain photographs as a photographic history.

As with any other data, members can ask for photographs to be removed.

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.

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.
- In Case of Emergency (ICE) contact
- Photographs taken at u3a meetings and events

Kettering U3A organises numerous meetings, trips and events and in the situation of a member falling ill, or having an accident, we request In Case of Emergency (ICE) information to be provided, the U3A will require the member to gain consent from the identified ICE contact. The consent will provide permission for the information to be held for the purpose of supporting and safeguarding the member in question.

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.

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.

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 or the U3A in these instances where the U3A has a substantiated concern then consent does not have to be sought from the member.

#### **Social Media**

Kettering u3a only have a Facebook social media account where adverts and news about u3a events are published. Also photographs taken at a u3a event are also published. A member can request the removal of a photograph at any time.

Although non u3a people can add to the Facebook account, it is monitored and any inappropriate posts are removed and if they are a persistent offender, they will be blocked.

#### **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 reminded annually to let the membership secretary know if any of their personal information changes. On joining and completing a membership application form, members gave their consent for the U3A to communicate with them.

#### **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. For this purpose, those from whom data is required will be asked to provide written consent. The evidence of this consent will be in the form of their original membership application. This will then be securely held as evidence of compliance. The U3A 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. 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.

### **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 of sharing member information to those on the Committee 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.

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

- MailChimp (e-mailing service for distributing U3A news)
- ISSUU (Newsletter publication)
- Microsoft
- Apple

The committee has scrutinised the Terms and Conditions of each supplier and judge that they are UK-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 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**

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 within 24 hours of the breach occurring 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.

If a U3A member contacts the U3A to say that they feel that there has been a breach by the U3A, a committee member will ask the member to provide an outline of their concerns. 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 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.

Policy Approved by Committee: 4<sup>th</sup> July 2023

Reviewed and updated July 2025