

# South Lakes U3A Data Protection Policy

## SCOPE OF THE POLICY

This policy applies to the work of South Lakes U3A (hereafter 'SLU3A'). For membership purposes SLU3A requires to gather personal information, and this policy details how that information will be gathered, 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 SLU3A committee members to ensure that we are compliant with GDPR, and should be read in tandem with the SLU3A Privacy Policy.

## WHY THIS POLICY EXISTS

This data protection policy aims to ensure that SLU3A:

- 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 COMMITTEE MEMBERS AND 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 the members of SLU3A.
- SLU3A will emphasise to committee members and special interest group coordinators their responsibilities when handling members' personal data.
- Committee Members and group coordinators will keep all personal data secure by taking sensible precautions and following the principles below. When data is stored in digital form access will require strong passwords and these passwords will not be shared.
- Data will not be shared outside SLU3A except with members' prior consent and/or for specific and agreed reasons. (Examples include Gift Aid information provided to HMRC or information provided to the distribution company for the Third Age Trust publications.)
- Member information will be refreshed periodically to ensure accuracy, via the membership renewal process or when policy is changed.

## DATA PROTECTION PRINCIPLES

SLU3A will comply with The General Data Protection Regulation which 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.

Principle 3 - The collection of personal data must be adequate, relevant and limited to what is necessary to fulfil the purposes for which they are processed.

Principle 4 - Personal data held should be accurate and kept up to date. Every reasonable step must be taken to ensure that personal data found to be inaccurate or held unnecessarily 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 to fulfil the purposes for which the data are kept. Personal data may be stored for longer periods if it is to be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and 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 data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by use of appropriate technical or organisational measures.

## Lawful, fair and transparent data processing

SLU3A requests personal information from potential and existing members for membership applications and for the purpose of sending communications about their involvement with SLU3A. The forms used to request personal information will contain a privacy statement explaining to potential members and members the reasons for the information being requested and what it will be used for. The lawful basis for obtaining member information is the contractual relationship that SLU3A has with individual members. In addition members will be asked to provide consent for other specific processing purposes. Members will be informed who to contact should they wish that their data are no longer used for any specific purposes for which they have previously provided consent. When these requests are received they will be acted upon promptly and the member informed when the action has been taken.

#### **Processed for Specified, Explicit and Legitimate Purposes**

Members will be told how their information will be used and the SLU3A Committee will seek to ensure that member information is not used inappropriately. Appropriate use of information provided by members will include:

- Communicating with members about SLU3A's events and activities
- Communication with special interest group members by coordinators about specific group activities.
- 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.

Consent will be sought in order to add SLU3A members' details to the direct mailing information for the Third Age Trust magazines – Third Age Matters and Sources.

SLU3A will ensure that special interest group coordinators are made aware of what would be considered appropriate and inappropriate communication. Inappropriate communication would certainly include sending members marketing or promotional materials from external service providers.

SLU3A 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 data portability
- The right to object

These rights are further explained on the [Information Commissioner's Office](#) web site.

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

Members of SLU3A will be asked to provide only information that is relevant for membership purposes. This will include:

- Name
- Postal address
- Email address
- Telephone number
- Gift Aid entitlement

Where additional information may be required, such as health-related information for coordinators or leaders of walking groups, 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 for which it will be used.

#### **Photographs**

Photographs are classified as personal data. Where group photographs are being taken that might be published, displayed or otherwise shared, members should be asked to step out of shot if they do not wish to be in the photograph. Otherwise later consent will be obtained from members in order for photographs to be published or displayed.

### **Accuracy of Data and Keeping Data up to Date**

SLU3A has a responsibility to ensure members' information is kept up to date. Members are advised to notify the membership secretary should any of their personal information change. In addition the membership renewal process will provide an opportunity for members to inform SLU3A of any changes.

### **Accountability and Governance**

The Committee is responsible for ensuring that the SLU3A remains compliant with data protection requirements and can provide 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 Committee will ensure that new members joining the Committee are made fully aware of the requirements of GDPR and the implications for their role. SLU3A will also ensure that special interest group coordinators are made aware of their responsibilities in relation to the data they hold and process. Committee members will also maintain an awareness of changes in guidance and practice within the U3A movement, and may seek additional advice 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 and Coordinators relinquish their roles, they will be asked to pass on data to those who need it and to delete any data that is no longer required.

### **Secure Processing**

SLU3A Committee members 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 to shared member information to those on the Committee who need to communicate with members.
- Using password protection on laptops and personal computers that contain or access personal information
- Ensuring that portable devices are securely held during transport.
- Using password protection or secure cloud systems when sharing data between committee members and/or coordinators
- Ensuring that firewall security is used on Committee members' computers or other devices that access personal information.

SLU3A intends to contract for services from the U3A Beacon team data processors, who have published their own Data Protection policy relating to those services ([U3A - Beacon Team Data Protection Policy](#))

The committee of SLU3A has scrutinised the Beacon Terms and Conditions and judge that they are GDPR compliant and will comply with the terms of this policy.

### **Subject Access Request**

SLU3A members are entitled to request access to the information that is held by SLU3A. The request needs to be received in the form of a written request to the Membership Secretary of SLU3A. On receipt of the request, it will be formally acknowledged and dealt with expediently unless there are exceptional circumstances as to why the request cannot be granted. SLU3A will provide a response in writing or by email 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 committee members are aware that a breach has taken place and how the breach 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 SLU3A shall notify National Office as soon as possible following the discovery of a breach. A discussion will take place between the Chair and National Office concerning 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 SLU3A members to inform them of the data breach and the actions taken to resolve the matter.

Where a member feels that there has been a data breach by SLU3A, 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 member to follow this up with an email or 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 SLU3A 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 SLU3A. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.

Policy review date: May 2019