Elmbridge U3A (EU3A) Data Protection Policy

SCOPE OF THE POLICY

This policy applies to the work of Elmbridge U3A (hereafter 'EU3A'). The policy sets out the requirements that EU3A has to gather personal information for membership purposes. It details how personal 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 EU3A's Committee members to ensure that EU3A is compliant. This policy should be read in tandem with EU3A's Privacy Policy.

WHY THIS POLICY EXISTS

This data protection policy ensures that EU3A:

- Complies with data protection law and follows good practice.
- Protects the rights of members, suppliers and partners.
- Is open about how it stores and processes member data.
- Protects itself from the risks of a data breach.

GENERAL GUIDELINES FOR COMMITTEE MEMBERS, OFFICERS, TECHNICAL SUPPORT VOLUNTEERS AND GROUP LEADERS

- The only people able to access data covered by this policy should be the Committee and those authorised by it who need to communicate with or provide a service to the members of EU3A.
- Data will not be shared informally and will be shared within and outside EU3A only for limited purposes authorised by the Committee
- EU3A will provide induction training to Committee members, officers, support volunteers and group leaders to help them understand their responsibilities when handling personal data.
- Committee Members and others authorised by the Committee to have access will 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 will not be shared outside of EU3A unless with prior authorisation and consent and/or for specific and agreed reasons.
- Member information will be reviewed and consent refreshed at least annually or whenever the policy is changed.
- EU3A will request help from National Office if unsure about any aspect of data protection.

DATA PROTECTION PRINCIPLES

The General Data Protection Regulation identifies 8 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 compared to the purpose(s) for which data is collected.

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.

Principle 6 - Personal data must be processed in accordance with the individuals' rights.

Principle 7 - 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 8 - Personal data cannot be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal data.

Lawful, fair and transparent data processing
EU3A requests personal information from potential members and members in order to allow it to fulfil its objects. 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 for what purposes the information will be used. It will be made clear to members and potential members that it is a condition of membership that EU3A be able to collect, store and use that personal information. EU3A members will be informed that they can, at any time, change or correct the information and will be informed as to how or as to who to contact should they wish to do so. Once an EU3A member requests not to receive certain optional 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 EU3A 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 EU3A's events and activities
- Group leaders communicating with their group members about specific group activities.
- Supplying member details to the companies effecting the direct mailing of EU3A's newsletters and the Third Age Trust magazines – Third Age Matters and Sources.
- 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.

The U3A will ensure that group leaders and others 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 not to 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 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, this will be obtained with the specific consent of the member who will be informed as to why this information is required and the purposes for which it will be used.

Where EU3A organises a trip that requires emergency contact/next of kin information to be provided, EU3A 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 was to be required – with agreement – for a longer purpose. The same would apply to carers who may, with the agreement of EU3A, attend either a one-off event or on an ongoing basis to support a member.

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 EU3A in these instances where EU3A has a substantiated concern then consent does not have to be sought from the member.

Accuracy of Data and Keeping Data up to Date
EU3A has a responsibility to ensure members' information is kept up to date. Members will be asked to let the membership secretary know if any of their personal information changes. In addition, on an annual basis the membership renewal forms will reiterate EU3A's right to collect, store and use members' personal information and will provide an opportunity for members to resubmit that information.

Accountability and Governance
The EU3A Committee are responsible for ensuring that EU3A remains compliant with data protection requirements and can evidence that it is. For this purpose, those from whom data is required will be asked to provide consent. The evidence of this consent will be their application to join and each successive renewal of their Membership. The Committee shall ensure that new members joining the Committee receive an induction into how data protection is managed within EU3A 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 measures and who has access to information on a regular basis as well as reviewing what data is held.

Secure Processing
The Committee members of EU3A 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 shared 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 and others.
- Ensuring that Committee members and members supporting them have firewall security on their laptops or other devices.

EU3A has contracted for services from the following 3rd party data processors: the Third Age Trust and Third Age Trust Trading Limited (TATTL) for the Beacon system and for the distribution of TAT magazines, McLellan Printing. for the distribution of EU3A newsletters, Dropbox for file sharing between authorised users, Microsoft and others for a variety of necessary computer software.

The Committee has scrutinised the Terms and Conditions of each supplier and judged that they are GDPR compliant.

Subject Access Request
U3A members are entitled to request access to their 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 EU3A 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 EU3A members to inform them of the data breach and the actions taken to resolve the breach.

If an EU3A member contacts EU3A to say that they feel that there has been a breach by EU3A, 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 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 EU3A member should also be informed that they can report their concerns to National Office if they don't feel satisfied with the response from EU3A. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.

Policy review date: 20/5/2020