Stanway U3A - IT and Data Security Policy V1.2

Date Approved by Executive Committee: 3rd July 2018

Date Policy Due For Review: 3rd July 2019

Contents

1. SCOPE OF THE POLICY

This policy applies to the work of Stanway U3A (hereafter 'the U3A') and should be read in tandem with the U3A's Privacy Policy.

1.1. Personal Data

This policy primarily 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 General Data Protection Regulation which came into force on 25 May 2018. This policy is reviewed on an ongoing basis by the U3A Executive Committee members to ensure that the U3A remains compliant.

1.2. Confidential Information

This policy also covers non-personal data that require confidential handling and restricted circulation, such as financial records, contracts, plans, and dealings with other organisations.

1.3. Equipment

This policy also covers any IT, Audio/Visual or other equipment owned by the U3A that requires secure handling and storage.

2. WHY THIS POLICY EXISTS

This policy reflects the U3A Executive Committee's commitment to ensure it:

- Complies with data protection law and follows good practice.
- Protects the rights of Trustees, Executive Committee members, Sub-committee members, Group Leaders, members, and those to whom we have a responsibility when working with them as partners.
- Is open about how it stores and processes members' data.
- Protects itself from the risks of a data breach.
- Communicates IT security and data protection responsibilities to the U3A volunteer officials
- Provides training and support for those who handle personal data, so that they can act confidently and consistently.
- Maintains secure handling of equipment and confidential (non-personal) information.

This policy reflects current practice that data is held and processed by the U3A volunteer officials, using devices issued by the U3A or using their own personal devices.

3. KEY RISKS

The key risks identified for the U3A regarding IT security and data protection are that:

- Information about members may get into the wrong hands, through poor security or inappropriate disclosure of information, leading to distress or harm to the members concerned.
- Confidential (non-personal) information may be inappropriately disclosed or lost, leading to reputational harm for the U3A.
- Equipment may be damaged, stolen or lost, leading to financial cost to the U3A.

4. ACCOUNTABILITY AND GOVERNANCE - GUIDELINES FOR COMMITTEE MEMBERS AND GROUP LEADERS

The U3A Executive Committee are committed to, and are responsible for ensuring that the U3A remains compliant with data protection requirements, and can evidence this. For this purpose:

- Those from whom data is required will be asked to provide written consent. The record of this consent will then be securely held as evidence of compliance.
- 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 and Group Leaders to help them understand their responsibilities when handling personal data.
- The U3A Executive Committee will review data protection and who has access to information on a regular basis, as well as reviewing what data is held.
- The U3A Executive Committee Members and Group Leaders should keep all data secure, by taking sensible precautions and following the guidelines stated in this policy.
- Strong passwords must be used on devices and for individual user accounts, and they should never be shared.
- Personal and confidential data should not be shared informally, or outside of the U3A unless with prior consent and/or for specific and agreed reasons.

- Member information should be reviewed and consent refreshed periodically via the membership renewal process or when policy is changed.
- The U3A Executive Committee Members shall 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 about any aspect of data protection.

To further demonstrate this commitment the Executive Committee has created an IT and Data Security Officer role. His/her responsibilities will include:

- Briefing the U3A Executive Committee on data protection responsibilities and other security matters.
- Establishing and reviewing policies and procedures related to IT security and data protection.
- Ensuring that data protection induction and training takes place for those handling personal data.
- Notification to Information Commissioner's Office (if required) of any data breach.
- Handling Data Subject access requests.
- Reviewing and approving data protection related statements for publication on applications, publicity materials, letters, website etc.
- Auditing data protection and security arrangements and making recommendations for improvement.

5. DATA PROTECTION PRINCIPLES AND HOW THE U3A COMPLIES

The General Data Protection Regulation identifies 8 data protection principles and the U3A states alongside these principles how it complies.

5.1. Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner

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. The lawful basis for obtaining member information is due to the contractual relationship that the U3A has with individual members. In addition members will be asked to provide consent for specific processing purposes. 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 for their data not to be used for specific processing purposes. 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.

5.2. 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.

Members will be informed as to how their information will be used and the Executive 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 members' details to the direct mailing information for the Third Age Trust magazines – Third Age Matters and Sources (where members have agreed to receive them).
- 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 administration, planning and management of the U3A.
- To monitor, improve and develop the provision of the U3A's activities

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.

5.3. Principle 3 - The collection of personal data must be adequate, relevant and limited to what is necessary compared to the purpose(s) data is collected for.

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.
- Subscription preferences
- 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 purpose that it will be used for.

Where the U3A organises a trip or activity that requires next of kin/emergency contact information to be provided, it will only be held for the purpose of supporting and safeguarding the member in question. Where this information is 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 attend either a one-off event or on an ongoing basis to support a U3A member with the agreement of the U3A. The U3A has completed a legitimate interest assessment in order to request this information and this assessment will be made available to members on the U3A website.

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

Photographs are classified as personal data. Where group photographs are being taken members will be asked to step out of shot if they don't 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 the photographs will be displayed. Should a member wish at any time to remove their consent and to have their photograph removed they should contact the officer at Section 9 of this policy to advise that they no longer wish their photograph to be displayed.

5.4. 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.

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 resubmit their personal information and reconfirm their consent for the U3A to communicate with them.

Where personal data is taken over the telephone, a copy must be sent to the individual to check and to ensure the information has been recorded accurately.

Where personal data is supplied by email or mail and it is ambiguous, contact must be made with the individual to clarify any uncertainty.

5.5. Principle 5 – Personal data which is kept in a form which permits identification of individuals shall not be kept for longer than is necessary.

The U3A will set appropriate retention periods for data. Documentation containing personal data or confidential information must be securely disposed of after the appropriate retention period:

- hard copies - by shredding, preferably with a cross-cut shredder.
- electronic copies- by secure deletion from devices or systems.

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

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.

5.7. 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.

The Executive Committee and Sub-committee members of the U3A have a responsibility to ensure that data is both securely held and processed. This will include:

- Restricting access to, or sharing member information with, those who need to communicate with members on a regular basis.

- Using password protection or secure cloud systems when sharing data between committee members and/or Group Leaders.

Computers and mobile devices
Any devices used to store and manage the U3A personal or financial data must have appropriate security features enabled or installed, including:

- Access via a sufficiently strong and secure PIN or password that cannot easily be guessed.
- Antivirus software.
- Firewall.
- Operating systems and relevant applications must be regularly updated to ensure security patches are applied, preferably via automatic updating enabled.
- Separate user accounts should be in place if a device is shared with others, user account passwords should not be shared.

Care must be taken to guard against loss or unauthorised access to such devices, including via:
- Scam phone calls requesting remote access to equipment or systems.
- "Phishing" emails that are unsolicited and may trick the user into following suspicious links, password resetting, etc.

Documents
Documents, spreadsheets etc. containing personal data or confidential information must be password protected with a strong password that cannot be easily guessed. This is especially relevant if the document is to be exchanged by email or portable storage e.g. USB/flash drive.

Hard copy documentation relating to personal or financial data must be held in a secure locked cabinet.

Use of Contact details
Volunteer official or member personal contact details may only be given over the phone or by email where the volunteer official or member has agreed.

Business Continuity
To avoid a situation where a volunteer official in a key role is unable to carry out their responsibilities and data is rendered inaccessible, there should be a designated deputy who is, by arrangement, able to provide business continuity.

Key documents or systems holding the U3A personal or financial data must be backed up frequently so that a loss or compromise of the device or system does not mean loss or harm to essential data.

Where key documents containing personal data are password protected a backup copy and the password must be made available to the deputy or other nominated committee member.

5.8. 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.

The membership data held by the U3A is currently managed locally and is not managed or processed by a third party. Where this changes and the U3A enters into a contract with a supplier for membership data processing then the U3A Executive Committee shall scrutinise the Terms and Conditions of each supplier and satisfy themselves that they are GDPR compliant and their systems are secure.

6. 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.

7. DATA BREACH NOTIFICATION
Were a data breach to occur, action shall be taken to minimise the harm by ensuring all the U3A Executive Committee members are aware that a breach had taken place and how the breach had occurred. The U3A Executive 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 Executive 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, an Executive Committee member will ask the member to provide an outline of their concerns. If the initial contact is by telephone, the Executive 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 Executive Committee who are not in any way implicated in the breach. Where the Executive 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.

8. ENFORCEMENT

Failure of a U3A Executive Committee member or other volunteer official to comply with the U3A IT and Data Security Policy and related procedures may result in disciplinary procedures and removal from post. Membership of the U3A may also be terminated.

9. CONTACT

For queries about this policy please contact the IT and Data Security Officer at dataU3AStanway@gmail.com