Data Protection Policy

1 Introduction

This policy applies to the proceedings of The South Wales Network.

- The South Wales Network is hereafter known as The Network
- U3a Office is the National Office of the Third Age Trust (charity number 288007)
- The Officers are
    - Officers as defined in Section 4 of the Network Constitution and
    - Trust Volunteers.
- GDPR are the General Date Protection Regulations 2018
- Members are representatives of u3as who supply their personal details to The Network.
- Contact details for the Network Secretary and the Network website address are shown at the end of this document.

2 Policy

2.1 Scope of the policy

The policy sets out the requirements that The Network has to collect and process information for membership purposes. The policy details how personal information will be collected, stored and managed in line with data protection principles and the GDPR. The policy is reviewed on an ongoing basis by The Officers to ensure that The Network remains compliant. This policy is to be read in tandem with The Network Privacy Policy.

2.2 Why this policy exists

This data protection policy ensures The Network:

- 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

2.3 General guidelines for Officers

- The only people able to access data covered by this policy shall be those who need to communicate with or provide a service to members.
- Officers shall keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords must be used, and they must never be shared.

- Data may not be shared outside of The Network unless with prior consent and/or for specific and agreed reasons.
- Member information shall be refreshed periodically to ensure accuracy.
- Additional support will be available from u3a Office where uncertainties or incidents regarding data protection arise.

2.4 Data protection principles

GDPR identifies key data protection principles:

- Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner
- Principle 2 - Personal data must 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 purposes for which they are processed;
- Principle 4 – Personal data held shall be 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;
- Principle 5 – Personal data must kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for the 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 GDPR in order to safeguard the rights and freedoms of individuals;
- Principle 6 - Personal data must be processed in accordance with 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.

2.5 Lawful, fair and transparent data processing

The Network requests personal information from members for sending communications regarding members' involvement with The Network. Members will be informed 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 legitimate interest relationship that The Network has with

individual members. In addition, members will be asked to provide consent for specific processing purposes such as the taking of photographs. Network 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 have 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.

2.6 Processed for specified, explicit and legitimate purposes

Members will be informed as to how their information will be used and The Officers will seek to ensure that member information is not used inappropriately. Appropriate use of information provided by members will include:

- Communicating with members about Network events and activities
- Sending members information about u3a Office events and activities
- Communicating with members about their membership
- Communicating with members about specific issues that may have arisen during the course of their membership

The Network 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

2.7 Adequate, relevant and limited data processing

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

- Name
- Email address
- Phone number
- Their u3a
- Position in their u3a

Where additional information may be required such as health related information this will be obtained with the 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 Network organises a trip or activity that requires next of kin information to be provided, a legitimate interest assessment will have been

completed in order to request this information. Members will be made aware that the assessment has been completed.

2.8 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 Network Secretary to advise that they no longer wish their photograph to be displayed.

2.9 Accuracy of data and keeping data up-to-date

The Network has a responsibility to ensure members' information is kept up to date. Members will be informed to let the Network Secretary know if any of their personal information changes.

2.10 Accountability and governance

The Officers are responsible for ensuring that The Network 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 Officers will ensure that new Officers receive an induction into the requirements of GDPR and the implications for their role. Officers will stay up to date with guidance and practice within the u3a movement and will seek advice from u3a Office should any uncertainties arise. The Officers will review data protection requirements on an ongoing basis as well as reviewing who has access to date and how data is stored and deleted. When Officers relinquish their roles they will be asked to either pass on data to those who need it and/or delete data.

2.11 Secure Processing

The Officers have a responsibility to ensure that data is both securely held and processed. This will include:

- Officers using strong passwords
- Officers not sharing passwords
- Restricting access of sharing member information to those of the Officers who need to communicate with members on a regular basis
- Using password protection for files on laptops, PCs and other electronic devices that contain personal information
- Using password protection, a membership database or secure cloud systems when sharing data between Officers.

2.12 Subject Access Request

Members are entitled to request access to the information that is held byThe Network. The request needs to be received in the form of a written request to

the Network Secretary. On receipt of the request, it will be formally acknowledged and dealt with expediently (the legislation requires that information should generally be provided within one month) unless there are exceptional circumstances as to why the request cannot be granted. The Network 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.

2.13 Data Breach Notification

Were a data breach to occur action will be taken to minimise the harm. This will include ensuring that all The Officers are made aware that a breach has taken place and how the breach occurred. The Officers shall then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. The Chair of The Network will contact u3a Office as soon as possible after the breach has occurred to notify of the breach. A discussion will take place between the Chair and u3a Office as to the seriousness of the breach, action to be taken and, where necessary, the Information Commissioner's Office would be notified. The Officers shall also contact the relevant members to inform them of the data breach and actions taken to resolve the breach.

Where a member feels that there has been a breach by The Network, Officers will ask the member to provide an outline of the breach. If the initial contact is by telephone, The Officers will ask the member to follow this up with an email or a letter detailing their concern. The alleged breach will then be investigated by members or The Officers who are not in any way implicated in the breach. Where The Officers need support or if the breach is serious, they should notify u3a Office. The member should also be informed that they can report their concerns to u3a Office if they do not feel satisfied with the response from The Network. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.

3 Queries

For any queries regarding this Policy, contact details are shown below:

Network Contact	Chairman.SWN@gmail.com Phone: 01291 623986
Network Website	https://u3asites.org.uk/walesu3a/page/10321
Data Protection and Privacy Policies are held on the Network Website	