

# 1.Data Protection Policy

## 2.Policy

### 2.1 Scope of the policy

This policy applies to the work of Witney u3a. The policy sets out the requirements that Witney u3a has to collect and process information for the provision of membership services.

The policy details how personal information will be collected, stored and managed in line with data protection principles and the General Data Protection Regulation (GDPR).

The policy is reviewed and approved on an ongoing basis by Witney u3a committee members to ensure that Witney u3a remains compliant.

This policy should be read in tandem with Witney u3a Privacy Policy. (Available on the Witney u3a website.)

### 2.2 Why does this policy exist ?

This data protection policy ensures that Witney u3a

- Complies with data protection law and follows good practice
- Protects the privacy and data 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 committee members and group convenors

- The only people able to access data covered by this policy should be those who need to communicate with, or provide a service to Witney u3a members, hereafter "member(s)".
- Witney u3a will provide induction training to committee members and group convenors to help them understand their responsibilities when handling data.
- Committee members and group convenors should keep all data secure, by taking sensible and practical precautions and following the guidelines in this document. Where data is to be stored for legitimate legal purposes, it will need to be encrypted and accessible only to those with access rights approved and minuted by the committee of Witney u3a.

- Strong passwords must be used, regularly updated and they should never be shared.
- Data should not be shared outside of the u3a unless with prior consent and/or for specific and agreed reasons. Examples would include Gift Aid information provided to HMRC, to comply with a legal information request or information provided to a distribution company for the supply of the Trust's publications.
- Member information should be refreshed periodically to ensure accuracy using the membership renewal process, voluntary submissions or when data policy is changed.

## 2.4 Data protection principles

The 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 should 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 be kept in a form which permits identification of data subjects for no longer than is absolutely necessary and only for purposes for the which that personal data can be legitimately processed. Personal data may be stored for longer periods, where required, in order to be processed for legitimate and legal archiving, scientific, historical and statistical research purposes. This is subject to the full 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 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**

Witney u3a requests personal information from potential and existing members for membership applications and for sending communications regarding members' involvement with the u3a. 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 that the U3A has with individual members. In addition, members will be asked to provide consent for specific processing purposes such as the taking of photographs.

Witney u3a 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 committee of Witney 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 Witney u3a events and activities
- Group convenors communicating with group members about specific group activities
- Member information will be provided to the distribution company that supplies the Trust publication, Third Age Matters. Members will be informed and have a choice as to whether or not they wish to receive the publication.
- 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

Witney u3a will ensure that group convenors are made aware of what would be considered appropriate and inappropriate communication. Inappropriate communication would include sending U3A members marketing or promotional materials from external 'third party' service providers.

Witney u3a 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 of Witney u3a will only be asked to provide information that is relevant for membership purposes. This will include:

- Full Name (First and Last Names )
- Postal address with postcode.
- Email address
- Telephone and or mobile number
- Gift Aid entitlement status

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 Witney u3a 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 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 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 Membership secretary in writing to advise that they no longer wish their photograph to be displayed.

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

Witney u3a has a responsibility to ensure members' information is kept up to date. Members will be requested to let the membership secretary know if any of their personal information changes. In addition, on an annual basis, the membership renewal process will provide an opportunity for members to inform Witney u3a of any changes in their personal information.

## **2.10 Accountability and governance**

Witney u3a committee is responsible for ensuring and documenting that the u3a remains compliant with data protection requirements. Where consent is required for specific purposes then evidence of this consent (either electronic or paper) will be obtained and retained securely. Witney u3a committee will ensure that new members joining the committee receive an induction into the requirements of GDPR and the implications for their role. Witney u3a will also ensure that group convenors are made aware of their responsibilities in relation to the data they hold and process. Committee members will stay up to date with guidance and practice issued by the UK Government and within the u3a movement and will seek advice from the Third Age Trust/ National Office should any uncertainties arise. Witney u3a 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 Committee members and group convenors 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**

Witney u3a 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 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 personal information
- Using password protection, a membership database or secure cloud systems when sharing data between committee members and/or group convenors
- Paying for firewall security to be put onto committee members' laptops or other electronic devices.

### **2.12 Subject Access Request**

u3a members are entitled to request access to the information that is held by Witney u3a. A member's information request needs to be in writing and requested from the membership secretary of Witney u3a. On receipt of the request, the request 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. Witney 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.

### **2.13 Data Breach Notification**

Were a data breach to occur, action will be taken to minimise any harm. This will include ensuring that all Witney u3a committee members are made 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 and to prevent any further breaches. The Chair of Witney u3a will contact National Office as soon as possible after the breach has occurred to notify of the breach. A discussion will 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.

Where a U3A member feels that there has been a breach by the U3A, 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 U3A member to follow this up with an email or a 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 U3A member should also be informed that they can report their concerns to National Office if they do not feel satisfied with the response from u3a. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.