Rutland U3A: GDPR Policy

The Rutland U3A data protection policy serves to protect the rights of members and minimise risks of a data breach. It complies with the guidance of the Third Age Trust and relevant law and good practice.

General guidelines for committee members and group convenors

- The only people able to access data covered by this policy are those who need to communicate with or provide a service to Rutland U3A members.
- Rutland 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 precautions and following the guidelines below.
- Strong passwords must be used, and must never be shared.
- Data should not be shared outside of the U3A unless with prior approval by the Committee and for specific and agreed administrative reasons such as Gift Aid information provided to HMRC or information provided to the distribution company for Trust publications.
- Member information should be refreshed periodically to ensure accuracy, via the membership renewal process or when policy is changed.
- Additional support will be available from the Third Age Trust where uncertainties or incidents involving data protection arise.

Data protection principles

The General Data Protection Regulation 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, used and processed only for specified, explicit and legitimate purposes and in a manner that is compatible with those purposes; further processing for archiving purposes, 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 will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Principle 4 – Personal data held will be accurate and kept up to date; every reasonable step will be taken to ensure that personal data that are inaccurate are either rectified or erased without delay;
- Principle 5 – Personal data will be 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 is held but may be processed solely for archiving purposes, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- Principle 6 - Personal data must be processed in accordance with procedures that ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Accountability and governance

Rutland U3A Committee is responsible for ensuring that the U3A remains compliant with data protection requirements and can evidence this. Where consent is required for specific purposes then evidence of this consent (either electronic or paper) will be obtained and retained securely.

Rutland U3A Committee will ensure that new members joining the Committee receive an induction into the requirements of GDPR and the implications for their role. Rutland 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 within the U3A movement as guided by the Data Protection advisor. Rutland U3A Committee will review data protection requirements on an ongoing basis as well as reviewing who has access to data and how data is stored and deleted. When Committee Members and Group Convenors relinquish their roles, they will be asked to pass on data to others who have a legitimate need for it and then delete it entirely from their own records.

Secure Processing
Rutland Committee Members are responsible for ensuring that data is both securely held and processed. This will include:

- Committee members using strong passwords
- Committee members not sharing passwords
- Restricting access of member information to those on the Committee who require it in order to carry out their legitimate responsibilities, such as communicating with members.
- 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 conveners
- Requiring firewall security to be put onto Committee Members' laptops or other devices.

Subject Access Request
Each U3A member is entitled to request access to the information relating to him/herself that is held by Rutland U3A. The request needs to be received in the form of a written request to the Membership Secretary of Rutland U3A, who will inform the Data Protection advisor. On receipt, any such request will be formally acknowledged and dealt with expediently (legislation requires that generally information should be provided within one month). Unless there are exceptional circumstances as to why the request cannot be granted, Rutland 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
Should a data breach occur, prompt action will be taken to minimise the harm. This will include ensuring that all Rutland 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 to prevent any further breaches. The Committee shall also contact all relevant U3A members to inform them of the data breach and actions taken to resolve the breach.

The Chair of Rutland U3A will notify the National Office of the occurrence of the breach as soon as possible after it has occurred. A discussion will take place between the Chair and National Office as to the seriousness of the breach and action to be taken. Where necessary, the Information Commissioner's Office will be notified.

If a U3A member asks the committee whether there has been a breach by the U3A, the member will be asked to provide an outline of the suspected 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 Data Protection advisor considers the breach to be serious, National Office will be notified. The U3A member should also be informed that he or she can report their concerns to National Office if they feel dissatisfied with the response from Rutland U3A. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.

Dated 25 April 2022
Policy review date November 2023