Forfar and District u3a

learn, laugh, live

Data Protection Policy

1. Introduction

This document is the Data Protection Policy for the Forfar and District u3a.

2. Policy

2.1 Scope of the policy

This policy applies to the work of Forfar and District u3a. It sets out the information that Forfar and District u3a has to collect and process for membership purposes. The policy details how personal information will be collected, stored and managed in line with data protection principles and General Data Protection Regulation (GDPR).

The policy will be reviewed on an ongoing basis by the Membership Secretary, and annually by the Committee, to ensure that Forfar and District u3a remain compliant. This policy should be read in conjunction with Forfar and District u3a's Privacy Policy.

2.2 Why this policy exists

This data protection policy ensures that Forfar and District u3a:

- complies with data protection legislation and follows good practice;
- protects the rights of its 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 Leaders

- The only people able to access data covered by this policy will be those who need to communicate with or provide a service to Forfar and District u3a members.
- Forfar and District u3a will provide information for Committee Members and Group Leaders to ensure they understand their responsibilities when handling data.
- Committee Members and Group leaders will keep all data secure, by taking sensible precautions and following the guidelines outlined below.
- Strong passwords must be used, and they should never be shared.
- Data will not be shared outwith the u3a unless with prior consent and/or for specific and agreed reasons.
- Member information will be refreshed periodically to ensure accuracy, via the membership renewal process or whenever the policy is changed.
- Additional support will be available from the Third Age Trust where uncertainties or incidents arise regarding data protection.

2.4 Data protection principles

The General Data Protection Regulation (GDPR) identifies six 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 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 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 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

Forfar and District u3a requests personal information from members and potential members for membership applications and for sending communications regarding members' involvement with the u3a. Members will be told why the information is being requested and how the information will be used.

The lawful basis for obtaining member information is the legitimate interest relationship that the u3a has with individual members.

Members will be asked to provide consent for specific processing purposes such as the taking of photographs. Forfar and District u3a members should contact the Committee Secretary if they wish to withdraw any previous consent to the specific use of their data. Where these requests are received, they will be acted upon promptly and the member will be informed when the request has been actioned.

2.6 Processed for specified, explicit and legitimate purposes

Members will be told how their information will be used and the Committee of Forfar and District 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 Forfar and District u3a 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 period of their membership;
- Group Leaders communicating with group members about specific group activities;
- sending members information about Third Age Trust events and activities;
- sending member information to the distribution company that sends out the Trust publication, *u3a Matters*. Members will be told about the publication and will be able to decide whether they wish to receive it.

Continued on next page

Forfar and District u3a will ensure that Group Leaders are made aware of what would be considered appropriate communication and what is inappropriate. In the event that the Beacon Administrator is not a member of the Executive Committee Forfar and District u3a will ensure that the Beacon Administrator is also aware. Inappropriate communication would include sending u3a members marketing and/or promotional materials from external service providers.

Forfar and District u3a will ensure that members' information is managed in such a way that it will not infringe an individual member's rights. This includes:

- 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 Forfar and District u3a will be asked only for information that is relevant for membership purposes. This will include:

- name
- postal address
- email address
- telephone number
- next of kin

Where additional information may be required, such as health-related information, this will be obtained with the consent of the member who will be told why this information is required and the purpose that it will be used for.

Where Forfar and District u3a organises an activity that requires next of kin and and/or details of any medical condition to be provided, a risk assessment will be completed in order to request this information. Members will be made aware that the assessment has been completed by the Group Leader.

2.8 Photographs

Photographs are classified as personal data. Where group photographs are taken, members will be asked if they wish to be included in the photo and, if they give consent, they will be advised where the photograph 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 Group Leader who will then inform the Website Administrator that they no longer wish their photograph to be displayed.

2.9 Accuracy of data and keeping data up to date

Forfar and District u3a has a responsibility to ensure members' information is kept up to date. Members will be told to let the Membership Secretary know if any of their personal information changes. The annual membership renewal process will provide an opportunity for members to inform the Membership Secretary of any changes in their personal information.

2.10 Accountability and governance

The Committee of Forfar and District u3a is responsible for ensuring that the u3a remains compliant with data protection requirements and can demonstrate that it is. Where consent is required for specific purposes then evidence of this consent (either electronic or paper) will be obtained and retained securely.

Forfar and District u3a Committee will ensure that newly appointed Committee Members are provided with a summary of the legislation to help them understand the requirements of GDPR and the implications for their role. It will also ensure that Group Leaders are made aware of their particular responsibilities in relation to the data they hold and process. In the event that the Beacon Administrator is not a member of the Executive Committee, Forfar and District u3a will check that the Beacon Administrator is aware of GDPR requirements and protects members' data according to the terms of the legislation.

Committee Members will stay up to date with current guidance and practice within the u3a movement and will seek advice from the Third Age Trust National Office should any uncertainties arise. Forfar and District 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 Leaders 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

Forfar and District 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 to member information to those on the Committee who need to communicate with members on a regular basis;
- using password protection on laptops and computers that contain personal information;
- using password protection, a membership database or secure cloud systems when sharing data between Committee Members and/or Group Leaders;
- paying for firewall security to be put onto Committee Members' laptops or other devices.

2.12 Subject Access Request

Forfar and District u3a members are entitled to request access to the information that is held by the branch. The request needs in the form of a written request to the Membership Secretary of Forfar and District u3a. On receipt of the request, it will be acknowledged formally and dealt with promptly - the legislation requires that information should generally be provided within one month unless there are exceptional circumstances which mean the request cannot be granted.

Forfar and District 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

If a data breach were to occur, by a member or members, action will be taken to minimise the harm. This will include ensuring that all Forfar and District u3a Committee Members are made aware of the breach 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 Chair of the Forfar and District u3a will notify National Office of the breach as soon as possible after the breach has occurred and the Chair and National Office will discuss the level of gravity, action to be taken. Where necessary, the Information Commissioner's Office would also be notified. The Committee will also contact the person causing the breach and those impacted by the breach 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 description 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 Committee Members who are not in any way implicated in the breach.

Where the Committee needs support or if the breach is considered serious, National Office should be notified. The u3a member should also be informed that they can report their concerns to the National Office if they remain dissatisfied 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.

Policy adopted: 08/09/2022, reviewed on an ongoing basis and annually by the Committee.

Reviewed and updated: 10/06/24 Secretary

Reviewed and updated: 04/09/25 Committee

Next full review: September 2026