Penicuik & District u3a
Data Protection Policy

1 Introduction

This document has been adapted to meet the particular needs of Penicuik & District u3a (hereafter 'the u3a')

2.1 Scope of the policy

This policy applies to the work of the u3a. The policy 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. The policy is reviewed on an ongoing basis by the u3a committee members to ensure that the u3a is compliant.

This policy should be read in tandem with the u3a's Privacy Policy.

2.2 Why this policy exists

This data protection policy ensures that the u3a:

- Complies with data protection law and follows good practice.
- Protects the rights of members, staff, customers and partners.
- 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 the members of the u3a.
- Data should not be shared informally or outside of the u3a.
- The u3a will provide induction training to Committee Members and Group Convenors/Contacts to help them understand their responsibilities when handling personal data.
- Committee Members and Group Convenors/Contacts should keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords must be used and they should never be shared.
- Personal data should not be shared 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 should request help from National Office if it is unsure about any aspect of data protection.

2.4 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 can only 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 compared 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 which is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for 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.

Principle 7 - 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.

2.5 Lawful, fair and transparent data processing

The u3a requests personal information from potential members and members for the purpose of sending communications about their 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 relationship 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. The 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 have been 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 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 Convenors/Contacts communicating with their group members about specific group activities.
- Member information will be provided to the distribution company that sends out 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.

The u3a will ensure that Group Contacts 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.

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.

2.7 Adequate, relevant and limited data processing
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 and mobile numbers.

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 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. The u3a will require the member to gain consent from the identified next of kin. The consent will provide permission for the information to be held for the purpose of supporting and safeguarding the member in question. Were this information to be 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.

There may be occasional instances where a members' 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 these instances where the u3a has a substantiated concern, then consent does not have to be sought from the member.

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 their photographs will be displayed. Should a member wish at any time to remove their consent and have their photograph removed then they should contact the u3a to advise them that they no longer wish their photograph to be displayed.

2.9 Accuracy of data and keeping data up to date

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 process will provide an opportunity for members to inform the u3a as to any changes in their personal information.

2.10 Accountability and governance

The u3a Committee is responsible for ensuring that the u3a 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 u3a Committee shall ensure that new members joining the Committee receive an induction into the requirements of GDPR and the implications for their role**.**

The u3a will also ensure that Group Contacts are made aware of their responsibilities in relation to the data they hold and process.

The 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 Contacts relinquish their roles, they will be asked to pass on data to those who need it and/or delete data.

The u3a shall seek additional input from the Third Age Trust National Office should any uncertainties arise.

2.11 Secure Processing

The Committee Members of the u3a 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 or access personal information.
- Using password protection or secure cloud systems when sharing data between Committee Members and/or Group Contacts.
- Paying for firewall security to be put onto Committee Members' laptops or other devices.

The u3a may contract for services from the following 3rd party data processors:

- Penicuik & District Town Crier
- Penicuik Community Development Trust (specifically Pen-y-Coe Press)

The committee has scrutinised the Terms and Conditions of these suppliers and judge that they are GDPR compliant. Similar scrutiny will be applied to any other data processor.

2.12 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 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 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

Should a data breach occur, action shall be taken to minimise the harm. This will include ensuring all Committee Members are made aware that a breach has taken place and how the breach had 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 u3a shall 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 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.

This policy was revised on 1 September 2023