

Preston Park u3a Data Protection Policy

Scope Of The Policy

This policy applies to the work of Preston Park u3a (hereafter 'the u3a'). The policy sets out the requirements that the u3a has to gather personal information for membership and other purposes. The policy details how personal information will be gathered, stored, and managed in line with data protection principles and Data Protection legislation. 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 Notice.

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 member's data.
- Protects itself from the risks of a data breach.

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.
- The u3a will provide induction training to committee members and group convenors to help them understand their responsibilities when handling personal 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 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 when policy is changed. It is a condition of membership that members ensure their own information is kept up to date.
- Additional support will be support from the Third Age Trust where uncertainties or incidents regarding data protection arise.

Data Protection Principles

UK Data Protection legislation identifies 8 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 purpose(s) data is collected for.

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 are erased or rectified without delay.

Principle 5 – Personal data which is kept in a form which permits identification of individuals shall not be kept for longer than is necessary.

Principle 6 - Personal data must be processed in accordance with the individuals' rights.

Principle 7 - 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.

Lawful, fair and transparent data processing

The u3a requests personal information from potential members and members for the legitimate purposes of the u3a. The forms used to request personal information will contain a privacy statement informing potential members and members as to why the information is being requested and what the information will be used for. We may also collect personal information in the course of communications between you and us (including by phone, email or otherwise).

The lawful basis for obtaining and processing member information is the Legitimate Interest of the Preston Park u3a. In addition, members will be asked to provide consent for other specific processing purposes. The U3A members will be informed that they can, at any time, remove their consent and will be informed as to who to contact should they wish to do so. Once a U3A member requests not to receive certain communications this will be acted upon promptly and the member will be informed as to when the action has been taken.

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 the information provided by members will include:

1. Communicating with members about the u3a's events and activities.
2. Group conveners/leaders communicating with their group members about specific group activities.
3. To send your details to the Third Age Trust (the national organisation to which u3as are affiliated) including adding member's details to the membership management system and the direct mailing information for the Third Age Trust magazines.
4. Communicating with members about Third Age Trust other u3a related events and activities.
5. Communicating with members about other third-party organisations which are charitable, educational or non-profit making organisations.
6. Communicating with members about their membership and/or renewal of their membership.
7. Communicating with members about specific issues that may have arisen during the course of their membership.
8. To share and use your details in connection with any meetings, events and social or other outings you attend as part of a Preston Park u3a activity.
9. Communicating in an emergency with a nominated emergency contact.
10. To monitor develop or improve the activities provided by the u3a.
11. For administration, planning or management of the u3a.

The 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 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 of rectification
- The right to erasure

- The right to restrict processing
- The right to data portability
- The right to object

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 a committee member to advise that they no longer wish their photograph to be displayed.

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:

1. Name.
2. Home address.
3. Email address.
4. Phone & mobile numbers.
5. Subscription preferences.
6. Year of birth.
7. Gift aid details.
8. Photographs.
9. Posts on social network sites.
10. Any specialisms or particular skills.
11. Emergency Contact Information.

Where additional information may be required, such as health-related information and date of birth, this will be obtained with the specific 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 that requires next of kin information or emergency contact information to be provided, 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.

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.

Accountability and Governance

The u3a Committee are responsible for ensuring that the u3a remains compliant with data protection requirements and can evidence that it has. For this purpose, those from whom data is required will be

informed of what personal data we hold, our legal basis for holding it and how we use it. Where the legal basis is written consent, the evidence of this consent will then be securely held as evidence of compliance. The u3a Committee shall ensure that new members joining the Committee receive an induction into how data protection is managed within the u3a and the reasons for this. Committee Members shall also stay up to date with guidance and practice within the u3a movement and shall seek additional input from the Third Age Trust National Office should any uncertainties arise. The Committee will review data protection and who has access to information on a regular basis as well as reviewing what data is held.

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 convenors.
- Paying for firewall security to be put onto Committee Members' laptops or other devices.

When the u3a contracts for services from 3rd party data processors, the committee will scrutinise the Terms and Conditions of each supplier to ensure that they are compliant with Data Protection legislation.

Subject Access Request

The 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 within 14 days 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.

Data Breach Notification

Were a data breach to occur action shall be taken to minimise the harm by ensuring all committee members are aware that a breach had 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 within 24 hours of the breach occurring to notify of the breach. A discussion would 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.

If a u3a member contacts the u3a to say that they feel that there has been a breach by the u3a, a committee member will ask the member to provide an outline of their concerns. 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 concern 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.