Data Protection Policy

Scope of the Policy

This policy applies to the work of Chess Valley u3a (hereafter 'the u3a'). 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 we are compliant. This policy should be read in tandem with the u3a's Privacy Policy.

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
- is open about how it stores and processes members' data
- protects itself from the risks of a data breach

General guidelines for Committee Members and Groups 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 provides 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 they should never be shared
- Personal data should not be shared outside of the u3a unless with prior written consent and/or for specific and agreed reasons. Examples include Gift Aid information provided to HMRC or information provided to the distributors of the Third Age Trust's publications and the u3a newsletter.
- Member information should be reviewed periodically by the member to ensure its accuracy.
- Additional support is available from the Third Age Trust where uncertainties or incidents arise concerning data protection.

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 be considered to be compatible 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 are erased or rectified without delay. (In the u3a, it is the responsibility of the member to ensure that their data is accurate and up-to-date).

Principle 5 - Personal data which is kept in a form which permits identification of individuals shall not be kept for longer than is necessary for the purposes for which the data are processed.

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.

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. Forms used to request personal information will contain a privacy statement informing potential members and members why the information is being requested and what the information will be used for. The legal basis for obtaining a member's information relates to the contractual relationship they have with the u3a. In addition, members are asked to provide consent for specific processing purposes. These consents are included within the member's personal information and the member is responsible for their accuracy.

Processed for specified, explicit and legitimate purposes

Members will be informed about how their information will be used and the Committee of the u3a will seek to ensure that members' information is not used inappropriately. Appropriate use of information provided by members will include:

- Communicating with members about the u3a's events and activities, including via the quarterly Chess Valley u3a newsletter and the monthly Chess Valley u3a e-mail bulletin
- Group Convenors communicating with their group members about specific group activities
- Adding members' details to the direct mailing information for the Third Age Trust magazines - *Third Age Matters* and *Sources*.
- 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 ensures that Group Convenors are made aware of what is considered appropriate and inappropriate communication. Inappropriate communication would include sending u3a members marketing and/or promotional materials from external service providers.

The u3a ensures that members' information is managed in such a way as not to 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.

Adequate, relevant and limited data processing

Members of the u3a are only asked to provide information that is relevant for membership purposes. This includes:

- Name
- Postal address
- Email address
- Telephone number
- Gift aid status.

Where additional information – such as health-related information – is required, this is obtained with the specific consent of the member who will be informed as to why this information is required and the purpose for which it will be used.

There may be occasional instances where a member's 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.

Photographs

Photographs are classified as personal data. Where group photographs are taken, members are asked to step out of shot if they do not wish to be included. Otherwise, consent is obtained from members for photographs to be taken and they are told where these will be displayed. Should a member wish at any time to remove their consent and to have a photograph removed, they should contact the appropriate u3a person responsible for the display.

Accuracy of data and keeping data up-to-date

It is each member's responsibility to ensure that their information is accurate and kept up-to-date.

A member's personal information is held as a record in the Chess Valley u3a secure central membership system. The Membership System enables a member, via a secure personal login, to access their personal record to view and amend their personal information.

Alternatively a member may ask for their information to be amended on their behalf by the membership secretary, who may be contacted at any time:

By email: membership@cvu3a.uk

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, evidence of this consent is obtained (either electronically or physically) and retained securely. The u3a Committee ensures that new members joining the Committee receive an induction into the requirements of GDPR and its implications for their role. The u3a also ensures that Group Convenors are made aware of their responsibilities in relation to the data they hold and process. 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 reviews data protection and who has access to information on a regular basis as well as reviewing what data is held. When Committee Members and Group Convenors relinquish their roles, they are asked to either pass on any relevant data to their successor and/or delete the data.

Secure processing

The Committee Members of the u3a have a responsibility to ensure that data is both securely held and processed. This includes:

- 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.

The u3a has contracted for services from the following 3rd party data processors:

- Web Integrate Ltd (t/a Simple Membership)
- South Bucks Business Services (newsletter printing and distribution)

The Committee has scrutinised the Terms and Conditions of the above suppliers and judge that they are GDPR compliant.

Subject access request

Where a member of the u3a is unable to access their personal information on the u3a membership system, they are entitled to make a written request to the Membership Secretary for a print-out of their information. On receipt of such a request, it is formally acknowledged and dealt with expeditiously unless there are exceptional circumstances why this cannot be done. (Legislation requires that information should generally be provided within one month.) A record is kept of the date of the request and the date of the response.

Data breach notification

Were a data breach occurs, action shall be taken to minimise the harm. This includes ensuring that all U3Al 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. A discussion will take place between the Chair and National Office about the seriousness of the breach and, action to be taken and, where necessary, the Information Commissioner's Office is 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 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 concern is then 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.

Policy review date

1 April 2025.

Approval

This Policy was reviewed by the Trustees and approved by them on 18/04/2023.

Signed on behalf of the Trustees:

James Cadle
Chair, Chess Valley U3A

Revision history

13/03/2018	First issued version
06/08/2019	Second issued version; incorporates revised guidance from Third Age Trust.
15/02/2020	Third issued version; no change.
18/04/2023	Fourth issued version; no change other than substitution of ‘u3a’ for ‘U3A’ throughout to conform with corporate branding.

