DATA PROTECTION AND PRIVACY POLICY

This Data Protection and Privacy Policy outlines how Congleton & District u3a (the u3a) collects, manages, stores and protects your personal information in compliance with the General Data Protection Regulation (GDPR). Note: the u3a in this context is considered the Data Controller.

1. Overview and Principles

The u3a is committed to treating your privacy rights seriously. We process personal data lawfully, fairly, and transparently, collecting only what is necessary for specific, legitimate purposes. Our data management is guided by the following principles:

- Accuracy: We take reasonable steps to ensure data is accurate and up to date.
- Storage Limitation: Personal data which is kept in a form which permits identification of individuals shall not be kept for longer than is necessary.
- Security: Personal data must be processed in a manner that ensures appropriate security of that data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- Processing and usage:
    - Personal data shall be processed lawfully, fairly and in a transparent manner.
    - 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.
    - The collection of personal data must be adequate, relevant and limited to what is necessary for the purpose(s) for which it is collected.
- Health & Safety: Disability information (to assist Group Leaders) and emergency contact and carer details. You must give explicit consent for disability information to be collected by us. Note: You must have permission from your emergency contact or carer to share their details with us.

If you have someone else receiving emails on your behalf (‘email buddy’), you must ensure that you have permission for their email address to be recorded against your details in the database and to receive emails addressed to you. The ‘email buddy’ can withdraw their permission at any time by contacting the Membership Secretary.

2. Information We Collect

We collect information directly from you when you express interest or register for membership. This includes:

- Personal Details: Title, name, postal address, email, and telephone numbers.
- Membership Info: Membership type, Gift Aid entitlement, and affiliations (e.g., National Trust).

3. How We Use Your Information

Your data is used to provide u3a activities and services, and to manage the organization. Key uses include:

- Communication: Sending weekly bulletins, activity updates, and renewal information via your preferred method (post, email, or telephone).
- Group Management: Sharing relevant details (including declared disabilities) with group leaders to facilitate participation.
- Administration: Planning, provisioning and monitoring services, and fulfilling statutory duties like Gift Aid claims.

4. Data Sharing and Third Parties

We will send you messages by email, other digital methods, telephone and post to advise you of u3a activities, depending on your preference. As part of your registration process to the u3a, you will be asked to opt-in to communications by one or more of these methods.

We do not share data informally. Sharing only occurs:

- Internally: With Committee members, Group Leaders, and authorised data administration staff who need it to perform their roles.
- Externally (with your consent): For services like the Third Age Matters magazine, the u3aWeb management system or website.
- Legally: When required by law, such as sharing Gift Aid information with HMRC.
- Vital interest: When necessary to protect someone's life in an emergency (e.g. a medic attending an unconscious person).

5. Email Use

The u3a website and administrative systems incorporate the facility to generate and transmit email messages between the committee and the membership, between group leaders and members of their groups, and between individual members.

The data administrator and other authorised members of the administration team monitor and oversee the operation of the email system, to ensure it is protected from the ingress of spurious messages (spam), or other abuse.

Email messages are not private, but may be read at any point during transmission, including as part of the email monitoring process. The u3a uses encryption and secure platforms (u3aWeb) to mitigate these risks wherever possible.

Message content will be handled in accordance with this policy by all parties, as other personal data provided to the u3a. You must not use the email system to send any form of confidential information,

such as banking details. No personal information may be sent over email unless it is appropriately encrypted, and password protected.

6. External Links for Non-u3a Websites

All external links from the u3a website are provided for information and convenience only. The u3a cannot accept responsibility for the websites linked to, the information found therein, nor the privacy policy of those websites. A link does not imply an endorsement of a website or service.

7. Security and Storage

Your digital information is stored on secure external servers (u3aWeb) which undergo regular maintenance and backups.

- Access Control: Only authorized personnel with strong, private passwords can access member data.
- Email Security: While our system monitors for spam, email is not inherently private; confidential info (like bank details) should never be sent via email.
- Role-Based Storage: Where possible, Committee members should use dedicated u3a email addresses (e.g. chair@u3a.org.uk) to ensure a smooth transition and easy deletion of data upon retirement from their role.

Members of the u3a authorised to receive personal information from the database to carry out their assigned duties must take reasonable precautions to keep this information secure and confidential. Members must take care that the information is not disclosed, intentionally or otherwise, and must ensure that any information received or gathered is destroyed once the purpose for which it was provided is fulfilled.

8. Photography and Cookies

- Photographs: These are classified as personal data. You will be asked for consent before photos are taken and have the right to step out of any shot. Otherwise your consent will be obtained for photographs to be taken, and you will be told where photographs will be used or displayed. Should you wish at any time to have your photograph removed, then you should contact the u3a Membership Secretary.
- Cookies: Our website uses a single cookie solely to remember your membership number for login convenience. It is not used for any other purpose nor shared with any third parties.

9. Data Retention and Destruction

This section describes how long your data is retained, and how it is removed from our systems.

- Retention Schedule

Data Category	Retention Period	Note
Routine Enquiries (General "How do I join?" etc.)	Current membership year	Delete after the end of the current membership year.
Membership Records	3 Years after membership ceases	Delete contact threads 3 years after membership ceases. *There may be exceptions where legal or insurance needs require information to be held for longer. Where this is the case, you will be told how long the information will be held for and when it is deleted.*
AGM and Committee Minutes & Agendas	Life	To comply with Charity Commission requirements.
Financial Records (Invoices, Gift Aid, Expense claims) etc	6 Years	To Comply with HMRC and Charity Commission requirements.
Insurance & Accident Reports	3 Years	3 Years after the event. To protect the u3a against long-term liability claims. Excludes insurance policies provided by the National U3A organisation.
Disciplinary Reports/Complaints	2 Years	2 years after the resolution of the action/complaint.
Serious Incident Reports	10 Years	To comply with HMRC and Charity Commission requirements.

- Committee Member Responsibilities - when a committee member resigns or completes their term:-
    - Relevant historical records (Minutes, Financials, Policy docs) must be transferred to the successor or the Secretary before they leave the post.
    - All other emails containing member personal data must be deleted from the outgoing member's devices and "Sent" folders before they leave the post .

10. Data Breaches

If a data breach occurs, action will be taken to minimise any harm. This will include ensuring that all Committee members are aware and how the breach occurred if known. The Committee will then seek to rectify the cause of the breach as soon as possible, and to prevent any further breaches. The Chair of the u3a will notify the u3a National Office, and discuss the seriousness of the breach, action to be

taken and, if necessary, the Information Commissioner's Office will be notified within 72 hours of discovery of the breach if considered a high-risk. The committee will also contact any u3a members impacted, to inform them of the data breach and actions taken to resolve the situation.

If you feel that there has been a breach by the u3a, a committee member will ask you to provide an outline of the breach. If the initial contact is by telephone, the committee member will ask you to follow this up with an email or a letter detailing your concern. The alleged breach will then be investigated by members of the committee 6 to the u3a National Office if you don't feel satisfied with our response. Breaches matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.

11. Your Rights

Under GDPR data protection laws you have core rights over your data:

- Right to be informed: To know how your data is being collected and used
- Right of access: To get a copy of your personal data and supplementary info.
- Right to rectification: To have inaccurate data corrected or completed.
- Right to erasure: To have your data deleted (the "right to be forgotten") in certain situations.
- Right to restrict processing: To limit how your data is used.
- Right to data portability: To receive your data in a common format and transfer it to another service.
- Right to object: To object to certain types of data processing, like direct marketing.
- Rights related to automated decision-making and profiling: To not be subject to decisions based solely on automated processing, including profiling.

Subject Access Requests: You are entitled to request access to the information about you that we hold. The request must be made in writing to the Membership Secretary. 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. We will provide a written response detailing all information held on you. A record will be kept of the date of the request and the date of the response.

12. Contact and Complaints

For queries regarding this policy or to report a suspected data breach, please contact:

- Technical Services: techservices@congletonu3a.org.uk
- Membership Secretary: membersec@congletonu3a.org.uk

If at any time a member is unsatisfied with the response to a data concern, the next step would be to raise it with the Chair of Congleton u3a - chair@congletonu3a.org.uk.

If they are unhappy with the Chair's response, then they could report it to the Third Age Trust national office.

13. Availability and changes to this policy

This policy is available on the u3a website and may change from time to time. If we make any material changes we will inform you through the weekly Bulletin or the Committee Update.

Policy effective date: 31 March 2026

Policy review date: March 2028
