



# Data Protection Policy

## 1 Policy

### 1.1 Scope of the policy

This policy applies to the work of u3a Dacorum. The policy sets out the requirements that u3a Dacorum has to collect and process information for membership purposes and may use third parties to do so (for example Beacon). This policy details how personal information will be collected, stored and managed in line with data protection principles and the Data Protection Act 2018 and the 'General Data Protection Regulation'.

This policy is reviewed and updated on an ongoing basis by the u3a Trustees to ensure that u3a Dacorum remains compliant. This policy should be read in tandem with u3a Dacorum's Privacy Policy.

### 1.2 Why this policy exists

This data protection policy ensures u3a Dacorum:

- 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

### 1.3 General guidelines for Trustees, Committee Associates and Group Co-ordinators

- The only people able to access data covered by this policy should be those who need to communicate with or provide a service to u3a Dacorum members.
- u3a Dacorum will provide induction training to new Trustees, committee associates and group co-ordinators about their responsibilities when handling data and direct new Committee Members to the Committee Handbook for guidance.
- Trustees, Committee Associates and Group Co-ordinators 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.
- Data should not be shared outside the u3a unless with prior consent and/or for specific and agreed reasons. Examples would include Gift Aid information provided to HMRC or information provided to the distribution company for the Trust publications (for example u3a Matters).
- Member information should be refreshed periodically to ensure accuracy, via the membership renewal process or when policy is changed.

- Additional support will be available from the Third Age Trust where uncertainties or incidents regarding data protection arise.

## 1.4 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 must be collected for specified, explicit and legitimate purposes only 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 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 it is processed;
- Principle 4 – Personal data held should be accurate and, where necessary, kept up to date. All reasonable steps must be taken to ensure that inaccurate personal data is corrected 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 which the personal data is 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 manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

## 1.5 Lawful, fair and transparent data processing

u3a Dacorum requests personal information from potential members and members for membership applications and for sending communications regarding members' involvement with the u3a.

Members will be informed 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.

Group Co-Ordinators will be asked to record if members refuse permission to use their personal data for specific purposes such as the taking as photographs.

In addition, members will be asked to provide consent for specific processing purposes such the publication of personal data in for example The Digest.



u3a Dacorum members should contact the Chair if they wish their data not to be used for specific purposes for which they have not provided consent.

Where these requests are received, they will be acted upon promptly and the member will be informed as to when the action has been taken.

## **1.6 Processes for specified, explicit and legitimate purposes**

Members will be informed as to how their information will be used and the Trustees of u3a Dacorum will seek to ensure that member information is not used inappropriately. Appropriate use of information provided by members will include:

- Communicating with members about u3a Dacorum events and activities.
- Group Co-ordinator communicating with group members about specific group activities.
- Member information will be provided to the distribution company that sends out the Trust publication – u3a 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.

u3a Dacorum will ensure that group co-ordinators are made aware of what would be considered appropriate and inappropriate communication. Inappropriate communication could include sending u3a members marketing and/or promotional materials from external service providers.

u3a Dacorum 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

## **1.7 Adequate, relevant and limited data processing**

Members of u3a Dacorum will only be asked to provide information that is relevant for membership purposes. This will include:

- Name

- Postal address
- Email address
- Telephone number
- Gift Aid Entitlement
- Member Payments Made
- Date of Birth for Trustees Only (to meet requirements of Charity Commission)
- Next of kin and phone number (if requested by Group Co-ordinator).

If any additional information is required, eg Emergency Contact details - members will be advised why and what purpose it is to be used for. A 'Legitimate Interest Assessment' will have been completed by the Group Co-Ordinator.

Members may pass health related information to u3a Dacorum for purposes to facilitate assistance to be afforded in certain circumstances

## **1.8 Photographs**

Photographs are classified as personal data. Where group photographs are being taken members will be asked to step out of shot if they do not wish to be in the photograph. 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 The Chair or Vice Chair to advise that they no longer wish their photograph to be displayed.

## **1.9 Accuracy of data and keeping data up-to-date**

u3a Dacorum has a responsibility to ensure members' information is kept up to date. Members will be asked to keep the Membership Secretary advised of any changes to their personal data.

u3a Dacorum will, in turn, advise the member of any changes made to their stored data.

In addition, on an annual basis, the membership renewal process will provide an opportunity for members to inform u3a Dacorum of any changes in their personal information.

## **1.10 Accountability and Governance**

u3a Dacorum Trustees are responsible for ensuring that u3a Dacorum remains compliant with data protection requirements and that they can provide 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. u3a Dacorum Trustees will ensure that new members on becoming Trustees receive an induction into the requirements of GDPR and the implications for their role.

u3a Dacorum Trustees will also ensure that committee associates and group co-ordinators are made aware of their responsibilities in relation to the data they hold and process. u3a



Dacorum Trustees will stay up to date with guidance and practice within the u3a movement and will seek advice from the Third Age Trust National Office should any uncertainties arise. u3a Dacorum Trustees will review data protection requirements on an ongoing basis as well as reviewing who has access to date and how data is stored and deleted. When Trustees, Committee Associates and Group Co-Ordinators relinquish their roles, they will be asked to either pass on data to those who need it and/or delete any data they might hold in their personal records.

### 1.11 Secure Processing

u3a Dacorum Trustees have a responsibility to ensure that data is both securely held and processed. This will include:

- the use of strong passwords and these should be long (at least twelve characters) and have a combination of upper- and lower-case letters, numbers and the special keyboard characters like the asterisk or currency symbols.
- passwords must not be shared.
- restricting data access to those Trustees, Committee Associates and Group Co-Ordinators to that data that is required to complete a specific task.
- the use of password protection on laptops and PC's that contain personal information
- when sharing data between committee members and/or group co-ordinators the data must be password protected or sent securely through the archive.

Group Co-ordinators should ensure that members' e-mail addresses are not inadvertently shared. The options to do this are:

- use the 'bcc' field, which means you add the individual addresses. The e-mail address in the 'to' box, could be your own address, or that of the group e-mail address (eg [group999@u3adacorum.org](mailto:group999@u3adacorum.org)); or
- create an e-mail group in the address book within your e-mail system that contains the individual addresses and use this in the 'to' field;

It is important to do this so that personal information, such as e-mail addresses are not shared.

If a group co-ordinator needs to share a list of e-mail addresses (for example to hand over to new co-ordinator), then the information should be shared in a password protected format, with the password sent in a separate e-mail or text.

Group Co-ordinators may wish to set up a 'group' within Beacon (our membership system) to contact members of their groups. Please contact our Beacon administrator or Groups Secretary (see Digest) for information on how to do this.

### 1.12 Subject Access Request

u3a members are entitled to request access to the information that is held by u3a Dacorum about themselves. The request must be received in the form of a written request to the Membership Secretary of u3a Dacorum. On receipt of the request, the request shall



be formally acknowledged within 14 days 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. u3a Dacorum 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.

### 1.13 Response to data breach

Were a data breach to occur, action will be taken to minimise the harm. This will include ensuring that all u3a Dacorum Trustees are made aware that a breach has taken place and how the breach occurred, when known. The Trustees shall then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. The Chair of u3a Dacorum will 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 Chair shall also contact the relevant u3a member(s) to inform them of the data breach and actions taken to resolve the breach.

Where a u3a Dacorum member feels that there has been a breach, a Trustee will ask the member to provide an outline of the breach. If the initial contact is by telephone, the Trustee 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 the Trustees who are not in any way implicated in the breach. Where the Trustees needs support or if the breach is serious, they should notify the National Office. The u3a member should also be informed that they can report their concerns to National Office if they do not feel satisfied with the response from the Dacorum 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 adopted on: [6<sup>th</sup> February 2026]

Policy review date: February 2029

Data Protection Policy	u3a Dacorum
Version 1.2	27 Oct 2025
Version 1.3	26 Dec 2025
Version 1.4 for adoption	20 Jan 2026