

Yorkshire and Humber Region u3a

General Data Protection Policy

SCOPE OF THE POLICY

This policy applies to the work of Yorkshire and Humber Region of the u3a (hereafter 'the YAHR'). The policy sets out the requirements that the YAHR has to gather personal information for communication 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 to be reviewed on an ongoing basis by the YAHR Management Team to ensure that the YAHR is compliant. This policy should be read in tandem with the YAHR's Privacy Policy.

WHY THIS POLICY EXISTS

This data protection policy ensures that the YAHR:

- Complies with data protection law and follows good practice.
- Protects the rights of individuals
- Is open about how it stores and processes data.
- Protects itself from the risks of a data breach.

GENERAL GUIDELINES FOR THE MANAGEMENT TEAM

- 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 individuals of the YAHR.
- Data should not be shared informally or outside of the YAHR.
- The YAHR will provide induction training to Management Team to help them understand their responsibilities when handling personal data.
- The Management Team 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 YAHR unless with prior consent and/or for specific and agreed reasons.
- Information should be reviewed, and consent refreshed periodically or when policy is changed.
- YAHR should request help from National Office if they are unsure about any aspect of data protection.

DATA PROTECTION PRINCIPLES

The General Data Protection Regulation identifies eight 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.

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.

Principle 8 - 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.

Lawful, fair and transparent data processing

The YAHR requests personal information for the purpose of sending communications about their involvement with the YAHR. The forms used to request personal information will contain a privacy statement informing members as to why the information is being requested and what the information will be used for. Members will be asked to provide consent for their data to be held and a record of this consent along with member information will be securely held, 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 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

Individuals will be informed as to how their information will be used and the Management Team of the YAHR will seek to ensure that information is not used inappropriately. Appropriate use of information provided will include:

- Communicating about the YAHR's events and activities.
- Sending information about Third Age Trust events and activities.
- Communicating about specific issues that may arise.

The YAHR will ensure that presenters at YAHR events/activities are made aware of what would be considered appropriate and inappropriate communication. Inappropriate communication would include sending marketing and/or promotional materials from external service providers without their explicit consent.

The YAHR will ensure that information is managed in such a way as to not infringe an individual right 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 will only be asked to provide information that is relevant for activity purposes. This will include:

- Name.
- Postal address.
- Email address.
- Telephone number.

Where additional information may be required, such as health-related information, it will be explained why this information is required.

Where the YAHR organises a trip that requires next of kin information to be provided, the YAHR 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 individual 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 an individual with the agreement of the YAHR.

There may be occasions where an individuals' 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 individual or the YAHR in these instances where the YAHR has a substantiated concern then consent does not have to be sought from the individual.

Accuracy of Data and Keeping Data up to Date

The YAHR has a responsibility to ensure information is kept up to date. Individuals will be informed to let the YAHR Secretary know if any of their personal information changes.

Accountability and Governance

The YAHR Management Team is responsible for ensuring that the YAHR remains compliant with data protection requirements and can evidence that it has. For this purpose, those from whom data is required will be asked to provide written consent. The evidence of this consent will then be securely held as evidence of compliance. The YAHR Management Team shall ensure that new members joining the Team receive an induction into how data protection is managed within by YAHR 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 Management Team 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 Management Team of the YAHR has a responsibility to ensure that data is both securely held and processed. This will include:

- Using strong passwords.
- Not sharing passwords.
- Restricting access of sharing member information to those on the Management Team 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 leaders.

YAHR has no contracted services with third party processors.

Subject Access Request

Individuals are entitled to request access to the information that is held by the YAHR. The request needs to be received in the form of a written request to the Secretary of the YAHR. 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. YAHR 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 YAHR shall contact National Office within 24-hours of the breach occurring to notify it of that 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 to inform it of the data breach and the actions taken to resolve the breach

If a u3a or an individual contacts the YAHR to say there has been a breach by the YAHR, the Chair or Secretary will ask that u3a or individual to provide an outline of the concerns. If the initial contact is by telephone, the Chair or Secretary will ask that this be followed up by an email or a letter with details of that concern. The concern will then be investigated by members of the YAHR Management Team who are not implicated in any way whatsoever in the breach. Where the Management Team needs support or if the breach is serious then National Office should be notified. The u3a or the individual involved should also be informed so that any concerns can be reported directly to National Office if it is felt that the response from YAHR is unsatisfactory. Breach matters will be subject to a full investigation, records will be kept and all those involved will be notified of the outcome.

Reviewing the Policy

This policy was reviewed by YAHR Management Team March 2022, next review due March 2024 and then every two years.