

# **BURTON-ON-TRENT u3a**

## **DATA PROTECTION POLICY**

### **SCOPE OF THE POLICY**

This policy applies to the work of Burton-on-Trent u3a (hereafter called the u3a). The policy sets out the requirements that the u3a has to gather personal information for membership 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 reviewed on an ongoing basis by u3a committee members to ensure that the u3a is 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, staff, customers and partners.
- 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 GROUP COORDINATORS**

- 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 Coordinators to help them understand their responsibilities when handling personal data.
- Committee Members and group Coordinators 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. Examples would include Gift Aid information provided to HMRC or to the distribution company for the Trust publications.
- Member information should be reviewed and consent refreshed periodically 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.

### **DATA PROTECTION PRINCIPLES**

The General Data Protection Regulation 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.
- 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.
- 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 a manner that ensures appropriate security of the personal data
- 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 purpose of sending communications about their involvement with 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. Members will be asked to provide consent for specific purposes such as the taking of photographs. 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.

### **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 information provided by members will include:

- Communicating with members about the u3a's events and activities
- Group Coordinators communicating with their group members about specific group activities.
- Member information will be provided to the distribution company that sends out the Trust publications.
- 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 will ensure that Group Coordinators 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 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 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.

Where additional information may be required, such as health-related information, 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 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 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 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 advise that they no longer wish their photograph to be displayed.

### **Accuracy of Data and Keeping Data up to Date**

The u3a has a responsibility to ensure members' information is kept up to date. Members are responsible for informing the Membership Secretary if any of their personal information changes. In addition, on an annual basis the membership renewal forms will provide an opportunity for members to resubmit their personal information and reconfirm their consent for the u3a to communicate with them.

### **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 asked to provide 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. The committee will also ensure that group coordinators are made aware of their responsibilities in relation to the data they hold and process.

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

### **Subject Access Request**

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 expediently 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 that all committee members are made 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 ensure that contact is made with the National Office as soon as possible after the breach has occurred 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, the 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.

Policy review date: March, 2025