Beacon Team Data Protection Policy

Scope of the Policy
This policy applies to the work of the Third Age Trust's Beacon Team. The policy sets out the requirements that the Team has for personal information for: Team management purposes, for the delivery of the Beacon Service and when processing personal data on behalf of client U3As. 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 Team Coordinator to ensure that the Team is compliant. This policy should be read in tandem with the Team's Privacy Policy.

Terms used in this Policy

Administrator	A specified member of the Beacon Team.
Beacon Team	A Team of volunteers which delivers Beacon as a Service to U3As on behalf of the Third Age Trust.
Client U3A	A U3A which has formally agreed to the Beacon Terms and Conditions and therefore has a contract with the Third Age Trust.
Contractor	A commercial organisation contracted to maintain and support parts of the System under direction of the Beacon Team.
Coordinator	A specified member of the Beacon Team.
Data Controller	A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data subject	An individual who is the subject of personal data.
Installation	The date on which a U3As Beacon site becomes 'Live'.
National Office	The Registered Office of the Third Age Trust.
System	The Beacon System comprising the operating system, data storage and support services and materials.
Trust	The Third Age Trust.
U3A	A University of the Third Age organisation for a locality, affiliated to the national Third Age Trust.

Purpose
This data protection policy ensures that the Team:

- Complies with data protection law and follows good practice.
- Protects the rights of data subjects (including Team members and potential members, Trust members, contractors' staff and U3A members).
- Is open about how it stores and processes personal data.
- Protects itself from the risks of a data breach.

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 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 Beacon Team's lawful bases for processing are:

- Legitimate interests; for personal data processed in order to provide the Beacon Service. A Legitimate Interests Assessment has been conducted and shall be reviewed annually or when circumstances change.
- Contract; for personal data processed on behalf of client U3As. Third party processing by the Team for client U3As is in accordance with the Trust's Beacon Terms and Conditions.

In providing the Beacon Service, the Team sometimes requests personal contact information from data subjects for communicating about their involvement with the Team. Forms used to request personal information will contain a privacy statement informing data subjects why the information is being requested and what the information will be used for. If a data subject requests not to receive certain communications this will be acted upon promptly and the Team member will be informed as to when the action has been taken.

Processed for Specified, Explicit and Legitimate Purposes

Data subjects shall be informed as to how their information will be used and the Team Coordinator shall seek to ensure that data is not used inappropriately. Appropriate use of information provided by Team members will include:

- Communicating with Team members about the Team's events, activities and management of work.
- Communicating with Team members information about Third Age Trust policies, events and activities.
- Communicating with Team members and contractors' staff about specific issues that may arise during the course of their membership or contract.
- Communication with client U3A contacts in order to manage the contract with them and to deliver the Beacon Service.

The Team Coordinator shall ensure that Team members are made aware of what would be considered appropriate and inappropriate communication. Inappropriate communication would include sending Team members marketing and/or promotional materials from external service providers.

The Team Coordinator shall ensure that all data subjects' 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
Data subjects will only be asked to provide information that is relevant the delivery of the Beacon Service. This will include:

- Name.
- Email address.
- Telephone number.

Where additional information may be required, such as health-related information, this will be obtained only from the data subjects who will be informed as to why this information is required and the purpose that it will be used for.

There may be occasional instances where a data subject's data needs to be shared with a third party due to an accident or incident involving statutory authorities, or where it is in the best interests of the data subject, or in those instances where the Team has a substantiated concern.

Data subjects' contact details shall be deleted no longer than two years after the data subject ceases to have involvement with the Team.

Where Team members have responsibility for processing client U3As' personal data, there shall be two levels of documented access to client U3As' personal data.

- SuperUsers. These are a limited number of people who have ongoing access to all data across all U3As. This level of access is required to maintain the system.
- Ordinary (all others including Regional Support Teams). These are people who may have limited-period occasional access to data for individual U3As.

Accuracy of Data and Keeping Data up to Date
The Team Coordinator has a responsibility to ensure data subjects' information is kept up to date. Data subjects' information (not client U3As' data) shall be reviewed and validated at least annually or when policy is changed. Data subjects are informed to let the Team Administrator know if any of their personal information changes.

Subject Access Request
Data subjects are entitled to request access to the information that is held about them by the Team. The request needs to be received in the form of a written request to the Team Administrator. 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. The Team Administrator 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.

Accountability and Governance
The Team Coordinator is responsible for ensuring that the Team remains compliant with data protection requirements and can evidence that it has.
The Team Coordinator shall ensure that new members joining the Team receive an induction into how data protection is managed within the Team. All Team members shall confirm agreement with this policy annually.
The Team Coordinator shall review what data is held, its protection and manage/record who has access to it.
The Team Coordinator shall also stay up to date with Data protection guidance and practice within the U3A movement.

Secure Processing
The Beacon Team Coordinator is the Data Controller and has responsibility to ensure that data is both securely held and processed. Data handling shall follow documented processes. These will include but are not limited to:

- Team members using strong passwords.
- Team members not sharing passwords.
- Restricting access of sharing member information to those on the Team who need to communicate with data subjects 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 Team members.
- Ensuring firewall security on Team members' laptops or other devices.

Where Team members have responsibility for processing client U3As' personal data during migration, they shall:

- They shall use password protected files when sending data via email.
- They shall not copy data files onto memory sticks
- They shall delete a U3A's data files, including where attached to emails, from all devices once an issue is complete.

Personal data shall not be shared outside of the Team unless with prior consent of the Team Coordinator and/or for specific agreed and documented reasons.

Service Providers
The Team Coordinator has scrutinised the Terms and Conditions of each Beacon supplier listed below and judged that they are GDPR compliant.

Beacon supplier	Terms Reviewed	Judged GDPR Compliant (Y/N)	Used for Client U3A data
Siftware Ltd	24/03/18	Y	
SendGrid	04/03/18	Y	Y
FastHosts	04/03/18	Y	Y
TSOHost	04/03/18	Y	Y
Trello	24/03/18	N - Use to be discontinued	
Wufoo	04/03/18	Y	

Data Breach Notification
Were a data breach to occur action shall be taken to minimise the harm by ensuring all data subjects are aware that a breach had taken place and how the breach had occurred. The Team Coordinator shall then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. The Team Coordinator shall contact National Office within 24 hours of the breach occurring to notify of the breach. A discussion would take place between the Team Coordinator 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 Team Coordinator shall also contact the relevant data subjects to inform them of the data breach and actions taken to resolve the breach.

If a data subject or a client U3A contacts the Team Coordinator to say that they feel that there has been a breach by the Team, the Team Coordinator will ask them to provide an outline of their concerns. If the initial contact is by telephone, Team Coordinator will ask them to follow this up with an email or a letter detailing their concern. The concern will then be investigated by Team members who are not in any way implicated in the breach. Where the Team needs support or if the breach is serious they should notify National Office. The Team member or client U3A should also be informed that they can report their concerns to National Office if they don't feel satisfied with the response from the Team. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.

Andy Topp
Beacon Team Coordinator