Site Builder Privacy and Data Protection Policy

This policy applies to the work of the Third Age Trust's Site Builder Team. The policy sets out the approach of the Team in managing personal information for: Team management purposes, for the delivery of the Site Builder 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 the principles of good data protection and specifically the General Data Protection Regulation.

This policy is effective 25 May 2018 and should be read in tandem with the Site Builder Terms and Conditions. The policy will be reviewed on an ongoing basis by the Team Coordinator to ensure that the Team remains compliant.

Terms used in this Document

- Author - The specified member of a Client U3A authorised by their Committee to create their website on Site Builder. In this process the Author becomes the original site Administrator and may remain the sole Administrator or may create others.
- Administrator - A member of a Client U3A who operates their website using Site Builder, including managing accounts for all types of editor, including other Administrators.
- Site Builder Team - A Team of volunteers which delivers Site Builder as a Service to Client U3As on behalf of the Third Age Trust.
- Client U3A - A U3A which has agreed to the Site Builder Terms and Conditions and thereby has a contract with the Third Age Trust.
- Supplier- A commercial organisation contracted to provide services to the System under direction of the Site Builder Team (see below for details).
- 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 Processor - A person who (either alone or jointly or in common with other persons) is responsible for processing personal data on behalf of a Data Controller.
- Data subject - An individual who is the subject of personal data.
- Editor - One of the members of a Client U3A responsible for creating/amending/removing web pages, including uploading documents and images to their website.
- Oversights - The Site Builder companion site that displays data drawn from individual sites
- System - The Site Builder System comprising the operating system, application code, data storage and support services and materials for individual websites and Oversights.
- Team Coordinator - A specified member of the Site Builder Team.

- U3A - A University of the Third Age organisation for a locality, affiliated to the national Third Age Trust.

Purpose

This data protection policy shows how the Team:

- Complies with data protection law and follows good practice.
- Protects the rights of data subjects (including Team members and potential members, editors and other members of Client U3As).
- Is open about how it stores and processes personal data.
- Protects itself and the System 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 Site Builder Team's lawful bases for processing are:

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

In providing the Site Builder Service, the system will capture personal contact information for the Site Author as part of the initial site registration process. A copy of this information is then used to create the initial Administrator account and the original Site Author data is deleted. Thereafter this account and all other personal data submitted to the site, including in the accounts for other Administrators and Editors, contact details for use behind the Contact pages of the website and as part of the content of web pages and uploaded documents and images is managed by the relevant U3A as the Data Controller. The Site Builder Team then acts as the Data Processor for any personal data submitted by those Administrators and editors.

The Oversights part of Site Builder displays aggregate data drawn from individual U3A sites published using Site Builder itself and provides specialised search functions for particular site content (for example Groups in Kent with “Walking” in the title).

Site Builder also offers an email based support service to all Editors where issues relating to their particular site or more generally with the System are addressed. This is achieved using generic Team email addresses and does not involve revealing the contact details of individual Team Members. It may involve the use of the personal email address of the Editor (rather than an account based on the U3A domain name) if they choose to use that for raising support queries.

The Team acts as Data Controller in so far as it operates a small team whose contact details are held and shared within the team.

Processed for Specified, Explicit and Legitimate Purposes

Client U3As act as the Data Controller for Client U3As members’ personal data, so subjects will be informed by the Client U3A as to how their information will be used by the U3A. The Data Controller shall also seek to ensure that data is not used inappropriately and otherwise to fulfil the terms of their U3A Privacy Policy.

Site Builder shall only use personal data uploaded to the System by U3As in order to communicate with Administrators and Editors in order to give pro-active support on the use of the system and the investigate apparent failings as detailed in the Terms & Conditions.

Where Site Builder acts as a Data Controller appropriate use of information provided by Team members will include:

- Communicating with Team members about the Team’s activities and distribution of work.
- Communicating with Team members information about Third Age Trust policies.

The Team Coordinator shall ensure that Team members are made aware of what would be considered appropriate and inappropriate communication. Inappropriate communication would by anything other than directly supporting the use of Site Builder. For example include sending U3A Editors promotional materials from external service providers would be inappropriate.

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 by the Team to provide information that is relevant the delivery of support to the users of the Site Builder Service. This will include:

- A Team member's name.
- A Team member's email address.

Where additional information may be required, 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.

Client U3As are responsible for decisions regarding the submission and processing of the personal data of their Administrators and any other Editors and for any Contacts that are held within the System and any other personal data held on their U3A website pages or in uploaded documents.

Where the System has responsibility for processing Client U3As' personal data, there are two levels of access:

- Super Users. There are a very small number of people who have ongoing access to all data across all U3As in the database. This level of access is required to maintain the System.
- Ordinary Volunteers. A small number of additional Site Builder helpers. These are people who may have limited-period occasional access to data for individual U3As as part of their role in answering individual support queries. Special web based tools are provided by the System in order to facilitate these functions, that limit access to only the data required.

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 in their role as Data Controller. Team Members' personal information shall be reviewed and validated annually or when policy is changed. Team Members are required to let the Team Coordinator know if any of their personal information changes.

Client U3As are responsible for the accuracy and currency of the personal data of their Administrators and any other Editors and for any Contacts that are held within the System and any other personal data held on their U3A website pages or in uploaded documents.

Subject Access Request

Team Members 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 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.

The Team will respond to Subject Access Requests made by Client U3As' members by providing details of any communications with that member (if they requested support as an Administrator or other Editor or were the recipient of bulk mailings).

The System supports Subject Access Requests made to the individual U3A by their members in that it provides facilities for Administrators to view details of all editors' account information, as well as the contact details if the member is registered as a Contact on the website.

The Team will also support U3As in responding to Subject Access Requests made to the individual U3A by providing help with searching the pages and any uploaded documents on the website to locate any personal data.

Accountability and Governance

The Team Coordinator is responsible for ensuring that the Team remains compliant with data protection requirements and providing evidence that it has done so.

The Team Coordinator shall ensure that new members joining the Team receive an induction into how data protection is managed within the Team. 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 Site Builder Team has a responsibility to ensure that data is both securely held and processed.

Site Builder will only accept instructions regarding personal data on any site from the authorised Administrators. Sole Administrators who do not have their own account will need to be validated by at least two senior U3A Committee members before an account can be created for them by Site Builder.

Data handling security measures within the Team will include but are not limited to:

- Team members using strong passwords to access Site Builder management tools.
- Team members not sharing passwords for access to System facilities.
- Using password protection on laptops and PCs that contain or access personal information.
- Using password protection or secure cloud systems when sharing personal data between Team members.
- Ensuring firewall security is active on Team members' laptops or other devices.
- Not sharing personal data outside of the Team unless with prior consent of the Team Coordinator and/or for specific agreed and documented reasons.

Where the System has responsibility for processing Client U3As' personal data, it:

- Requires Client U3A Administrators and other Editors to use unique login names and passwords to access the System.
- Limits access to Editors login names and passwords to those with the full Administrator role
- Stores all Administrator and Editor passwords only in encrypted form.
- Offers Client U3As a "protected" documents folder (where documents containing personal data may be stored) where access is restricted by means of usernames and passwords.
- Stores the "protected" folder passwords in encoded form with the encoding key stored outside the System.
- Enforces HTTPS mode of access to all System and Client U3A website pages.
- Insulates public access to U3A website pages by means of an external third party firewall.
- Hides Contact details behind a web form for U3A members to reach a member of their U3A via email. (Unless the U3A decides to use the "Mailto:" form of addressing where such details are potentially exposed on the web page.)
- Anonymises any personal data taken from the live server before using it for volume testing.

Where Team members are required to view or manage data in the System for support purposes, access is secured in one of the following ways, by using:

- A username and password over SFTP to access facilities provided by the web host ISP
- A username and password over SFTP to access a set of special Team web forms
- A username and password over SSH to access the System's servers directly
- A username and password over SFTP to access the filing system of System's servers

Access to the System's servers via unsecured Telnet or FTP is blocked.

In terms of securing data against loss, the System provides three levels of backup, viz.:

- A parallel database on the live server – from which individual web page elements that have been accidentally deleted by a website Administrator or other Editor may be restored.
- Nightly dumps of the live database of Client U3As' and System web pages to the file system on the live server, stored indefinitely. This may be used to restore the entire System and all Client U3A web pages, or individual web site pages.
- Nightly archives of the dump file of the live database of Client U3As' and System web pages stored both on the live server and offline for a rolling 30 days, This may be used to restore the entire System and all Client U3A web pages.
- Nightly archives of Client U3As' uploaded documents and images stored offline for a rolling 30 days, that may be used to restore all Client U3A uploaded files and image.

Service Providers

The Team Coordinator has scrutinised the Terms and Conditions of each Site Builder supplier listed below and assessed the state of compliance with the GDPR.

TSOHost are in the process of issuing a new Data Protection and Privacy policy before 25 May 2018 to set out the terms of its compliance with the provisions of the GDPR.

Sucuri are in the process of issuing a new Data Protection and Privacy policy before 25 May 2018 to set out the terms of its compliance with the provisions of the GDPR.

All Amazon Web Services (AWS) are already fully compliant with the terms of the GDPR.

The Google Maps API provides geographical mapping and does not handle personal data.

As regards the issue of transferring personal data outside the EU, it has been established that servers for the main web hosting service TSOHost are located wholly within the UK at Maidenhead, Milton Keynes and Slough.

Use of email services from Amazon SES is limited to the EU based servers located in the Republic of Ireland. Amazon Web Services (AWS) - of which Amazon Simple Email Service (SES) is a part – is in any case covered by the EU-US Privacy Shield Framework.

Use of the Content Distribution Network (CDN) servers by for the Sucuri firewall may result in caching of uploaded documents outside the EU. Web page caching for Site Builder is switched off globally. CDN servers used by website visitors from within the EU are also based in the EU located in London, UK and Frankfurt in Germany.

For cases where access to Site Builder from outside the EU results in documents being cached on servers outside the EU, case Media Temple Inc. of which Sucuri is a part is covered by the EU-US Privacy Shield Framework.

Data Breach Notification

Should a suspected data breach be detected by the Team, the System or be reported by an Administrator or Editor of a Client U3A, the Team will investigate. If a data breach has in fact occurred the Team shall seek to address the cause of the breach as soon as they reach an understanding of how any breach occurred, in order to prevent any further breaches. The Team Coordinator shall then contact senior National Office management within one working day if a breach is confirmed, advising them of details of the breach.

Following a discussion between the Team Coordinator and National Office as to the seriousness of the breach and action taken, the Information Commissioner's Office will be notified where necessary. The Team Coordinator shall also contact the relevant data subjects (if Team Members) or the owning U3A (if U3A members) to inform them of the data breach and actions taken to resolve the underlying cause.

If a data subject or a Client U3A contacts the Team Coordinator to report a data breach by a member of the Team, the Team Coordinator will ask them to provide details by email. The Team Coordinator shall in such cases provide details to senior National Office management within one working day of the alleged breach occurring. The alleged breach will then be investigated by Team members who are not in any way implicated in the breach. The Team member or Client U3A shall be informed that they can report their concerns direct to the National Office if they do not feel satisfied with the response from the Team.

Allegations of breaches by Team members will be subjected to a full investigation, records will be kept and those involved notified of the outcome.