Date 14/08/2018 **Alsager U3A**
Data Management Policy
Status: Issued

1. The Purpose and Scope of this Document.

The purpose of this document is to describe how data held by Alsager U3A, including within the Beacon system, will be managed to ensure its security and protection.

The processes and procedures outlined in this document are designed to be compliant with the Beacon Terms and Conditions of Use, the Data Protection Act 1998 (which applies to all personal information about living individuals held either electronically or in a manual filing system) and the General Data Protection Regulation 2018 (GDPR). It sets out the respective responsibilities of the national Beacon Team, Alsager U3A and individual Beacon Users for management of data, including personal data, held on Beacon and elsewhere.

This document covers the following:

- Terminology used in this document
- Type of data held by Alsager U3A
- Development and support of the Beacon system
- Security - Beacon team responsibility
- Security - Alsager U3A responsibility
- System Availability
- Backup - Beacon Team
- Backup - Alsager U3A
- Information Commission
- Use of data
- Protection of data and compliance with principles of Data Protection Act
- Compliance with the GDPR
- Access to data
- Data subject rights
- Role of Information Compliance Officer
- Policy review

2. Terminology used in this document

Beacon: The Beacon System is a computer system developed by the Third Age Trust and operated over the Internet to support the operation and administration of individual U3A organisations. Beacon supports multiple individual U3As, each operating on and viewing only its own data.

Beacon Team: A number of volunteers who run the national Beacon System. They may be supplemented by commercial IT support as required.

Participating U3A: A U3A which is using the Beacon live system, such as Alsager U3A.

Member: A person who is, or has been, a Member of Alsager U3A, and whose membership details are held within the Beacon System.

Data subject: A term used by the Data Protection Act, it refers to a Member whose personal data is held by Alsager U3A.

User: A Member who has been registered as an authorised user of the Beacon live system to perform functions necessary for the effective running of Alsager U3A and who has a password for access to the system. They will have access privileges depending on their role within U3A.

Information Compliance Officer: A Member of Alsager U3A whose responsibility it is to ensure that Alsager U3A is compliant with the provisions of the Data Protection Act. The Information Compliance Office for Alsager U3A will be the Chair of Alsager U3A.

Data Protection Officer: A Member of Alsager U3A whose responsibility it is to ensure that Alsager U3A is compliant with the provisions of the General Data Protection Regulation (2018). The Data Protection Officer will be the Chair of Alsager U3A.

Information Commissioner: A person who is appointed by the Government to consider complaints concerning data protection.

Data Security and Confidentiality Agreement: An Agreement which must be signed by all Beacon Users within Alsager U3A confirming that they have read this document and will comply with its requirements.

3. Type of Data Held by Alsager U3A

The Beacon system stores personal contact data about members of the participating U3As within its database. Only data that is required for the legitimate interests of Alsager U3A will be held.

This data is:

- Forenames
- Surname
- Known as
- Address
- Telephone number
- Email Address
- Gift Aid information

This data will be held on the Beacon system through the internet, though some data may also be held on paper or on individual computers.
The Beacon system provides facilities for Members to view and edit their own personal information. Beacon enables the recording of personal information which is additional to those data items required by Alsager U3A to perform its legitimate interests. Any photographic image or data items entered by a Member that are additional to those described above will not be used by Alsager U3A for any purpose. Consent to store these additional data items will be assumed by virtue that the Member has entered the data.

Photographs of Members

Taking of photographs of Members can occur during trips, group outings or holidays, which may be used subsequently, for example, in newsletters or in the magazine. This gives rise to the issue of consent by Members for their photograph to be taken. It is not possible for Alsager U3A Members or Users to establish that all Members in a group photograph have given their consent before a photograph has been taken.

The policy the Alsager U3A has adopted for the taking, storage and subsequent use of photographic images is that it is the responsibility of the Member, that if they are unwilling to provide consent to the taking of their image for subsequent storage and use, then they ensure that they are not included in any photograph that may be taken during any U3A trip, outing, holiday or other event that may occur..

This policy will be part of the terms and conditions of membership and will be a condition of initial application and renewal of membership.

4. Use of Data

The legitimate purposes for holding and processing personal data within Alsager U3A are as follows:

- to manage annual membership
- to manage membership payments
- to manage gift aid payments
- to enable communications with the membership or subsections of the membership
- to enable communications between group leaders and their group members
- to have available data for HMRC purposes

5. Protection of Data and Compliance with the Principles of the Data Protection Act and the General Data Protection Regulation

Alsager U3A takes the protection of all personal information extremely seriously and is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal information.

All Users of personal information within Alsager U3A must comply with the eight Data Protection Principles. The Principles define how data can be legally processed. Processing includes obtaining, recording, holding or storing information and carrying out any operations on the data, including adaptation, alteration, use, disclosure, transfer, erasure and destruction.

The eight Principles state that:

1. Personal data shall be processed fairly and lawfully

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed

4. Personal data shall be accurate and, where necessary, kept up to date

5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose

6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

8. Personal data shall not be transferred to any country or territory outside of the U.K. unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Following the implementation of the GDPR, Alsager U3A has determined that the legal basis for processing personal data will be Legitimate Interests. This was agreed at the U3A management Committee meeting of 9 May 2018, and is recorded in the document Alsager U3A, Beacon and GDPR v2 (appended as an annex to this document) This mainly requires that we hold only data required for the organisation's legitimate purposes (as set out above in sections 3 and 4), and that this does not unduly compromise the rights and freedoms of individual Members.

If a Member feels that there has been a breach of these obligations then the Member should report this immediately to the Information Compliance Officer so that Alsager U3A may review the circumstances and liaise as necessary with colleagues.

6. Development and Support of the Beacon System.

The Beacon system has been created under the U3A ethos of learning and mutual-help between members and the Beacon Team consists of volunteers who have developed the system and continue to provide IT support. As the number of U3As using Beacon increases, Beacon will bring in additional commercial IT support as required.

7. Security - Beacon team responsibility

Beacon is hosted by a commercial hosting system, which stores the data. Personal contact data is held in encrypted form on these computers. The Beacon system takes a number of security precautions to protect personal data held within Beacon, but is not responsible for the consequences of any unauthorised access to that data.

Beacon makes this data available online to users of the system. The data may also be used by authorised members of the Beacon Team for uploading and making backups of the data, and for investigating system problems.

For each participating U3A, data about that U3A's Members is made available only to Users and Members who belong to that U3A. The U3A may choose to make it available to 1 or 2 supporters from a Regional Support Team during their period of migration and early use.

8. Security - Alsager U3A responsibility

Each participating U3A is responsible for deciding which of its Members may have a Beacon User account, and the privileges they shall be allocated. Note that only current U3A Members already on the Beacon database can be registered for an on-line Beacon account.

The participating U3A is responsible for ensuring that its Beacon Users keep to the conditions set out below.

Alsager U3A Beacon Users must sign a Data Security and Confidentiality Agreement to confirm that they have read and agreed to this Data Management Policy before being registered as a User.

The Beacon Team reserves the right to suspend or terminate any User's account if they don't abide by these conditions.

1. Access to data within a Beacon account is controlled by the User's username, password and the privileges allocated by the U3A.

2. Rules on password composition are imposed by Beacon, but it is a User's responsibility to ensure that their password is of sufficient strength and to keep it secret from others.

3. On any computer used by a User to access Beacon, it is the User's responsibility to ensure that suitable security measures have been taken to keep that computer free of viruses and other malware which might enable unauthorised access to Beacon.

4. Users should not allow anyone else to use their Beacon account.

5. When using a shared computer, Users are recommended to only use a Beacon account within a personal logon on the shared computer.

6. When using a Beacon account on a public computer, e.g. in a library, Users should use the 'In Private mode' (IE) or equivalent, if available, and ensure that form history is not enabled. They should not tick the 'Local computer' checkbox at login so that cookies are not stored.

7. Users should always logout of their account when finished. Beacon will automatically log out users who make no input after 15 minutes.

9. System Availability

Beacon is being developed and supported exclusively by volunteers, all of whom are members of their own U3As with many other things to do in life. It is therefore not possible to give participating U3As a commercial service level agreement or to have binding response times when issues occur.

As the number of U3As using Beacon continues to grow there is an increasing dependence on Beacon to support an increasing U3A Member population. It is probable that Beacon will bring in additional commercial IT resources to supplement the existing Beacon Support and Development team.

In the first 6 months of live use, Beacon did not experience any significant period of non-availability and it is anticipated that disruption of service in the future will be rare. Nonetheless, all software systems suffer failures from time to time and it is to be expected that this will occur at some time for Beacon. How long it will take to get Beacon back up and running will depend upon the availability of the Beacon Team, which they are seeking to strengthen, but in the worst case it could be several days or a week or more.

The Beacon commercial hosting contract is subject to a service level agreement and server and system software failures should therefore be rectified within a few hours. The commercial hosting system on which Beacon runs has an expectation of 99.9% uptime.

10. Backup – National Beacon Team

All Beacon data is automatically backed up daily and kept for a month, with selected backups retained indefinitely. This can be restored following any major server failure. However, participating U3As should be aware that they may lose data changed since the previous backup (i.e. up to a day before), so it is advisable to keep the original data sources (e.g. membership forms) for 24 hours before disposal.

These data backups are intended to protect against major system faults. They cannot be used to recover from mistakes affecting a single U3A. In such cases the Beacon audit log will often allow overwritten or deleted data to be recovered (by re-entry).

11. Backup - Alsager U3A

Alsager U3A will keep all paper documents, such as member application forms and renewal forms, so that in the event of a system failure the data for the previous day can be re-entered on to the Beacon system.

Beacon has a facility to enable Alsager U3A to create a backup of its own data. It would provide a view of the data in an Excel spreadsheet on a local computer, and could be used in an emergency in the event that for any reason Beacon data is lost or corrupted. This would enable data to be viewed in order to answer queries but would not be a source of restoring data. Lost or corrupted data would need to be re-entered.

The current experience of running Beacon has shown that there has not been any significant period of non-availability. It has therefore been decided that Alsager U3A will NOT use this facility.

If a system failure did occur, the National Beacon backup process would be used to restore data, so at the most only 24 hours' data would be missing. In these circumstances Users will be informed and will be asked to check any data they have entered or amended in the previous 24 hours and, as appropriate, re-enter the data.

If for any reason we lose connection to Beacon for a period at a time when people wish to use it, they will be told that Beacon is down and they will be informed when it is back up again.

The decision not to take regular local backups will be reviewed in the light of experience.

12. Information Commission

Alsager U3A does not need to formally register use of data with the Information Commissioner's Office. This registration process is handled by the UK Third Age Trust directly and covers Alsager U3A's registration. Any queries relating to the terms of the notification or other matters on the operation of the Data Protection Policy and Data Protection Act or the General Data Protection Regulation (2018) should be raised with Alsager U3A's Information Compliance Officer.

Should a member need to contact the Information Commissioner's office the contact details are www.ico.org.uk or telephone 03031231113.

13. Role of Information Compliance Officer

The Chair of Alsager U3A also fulfils the role of Information Compliance Officer with regard to the implementation of the Data Protection Act (1998) and also fulfils the role of the Data Protection Officer as required by the General Data Protection Regulation (2018)

The role is to provide oversight of Alsager U3A's policies and procedures for ensuring data protection, and to resolve any issues reported by a member who believes that the use of the Member's data was outside the prescriptions of the Data Protection Act or the General Data Protection Regulation (2018) as set out in this document.

The Information Compliance Officer will receive any such report and request that an investigation into the issue described be carried out by an appropriate member of the committee.

The Information Compliance Officer will review the report and oversee the resolution of the issue between Alsager U3A and the Member.

14. Access to Data

Members are able to use Beacon to access their own personal data, a list of Alsager U3A groups and a calendar of meetings and events. Members are able to access and edit their information online. A link to Beacon is provided on the Alsager U3A web site using the menu item 'Members Portal', which provides information about the information provided on the Beacon system. At the bottom of the page is a link '**Members Portal** click here'.

This will take the member into the Beacon system which requires the Member to provide membership number, Forename, Surname, post code and email address before access to Beacon will be provided.

Beacon Users will have specific access to data, including member's data, to allow the user to perform the functions of the role that they hold. They will have access to the minimum amount of data required to achieve the objectives of their tasks. This access is controlled by the system privileges they are granted, recorded by the database administrator.

Group leaders will be Beacon Users who will only have access to the information of members within their Group. They will be permitted to use and collect data for the purposes of the Group activity only.

Statistics may be produced from member data, which would be depersonalised so individuals cannot be identified. This would therefore be outside the constraints of the Data Protection Act. Therefore, there would be no restriction on the amount of data or the amount of time any statistics could be retained.

15. Data Subject Rights

Under the Data Protection Act 1998 an individual has the right, subject to certain exemptions, to access the personal information that an organisation holds about them. Accessing personal data in this way is known as making a 'subject access request'.

Any Member is able to view or edit their personal data held on Beacon through the Members Portal.

Individuals also have rights to prevent data processing which is likely to cause substantial and unwarranted damage or distress, to prevent processing for the purpose of direct marketing, and to correct inaccurate personal data.

If a Member wishes to make a subject access request to the Alsager U3A , the request must be made in writing to the Information Compliance Officer (this may be in electronic form).

Before Alsager U3A can act on the request, we must:

- be sure of the person's identity
- be supplied with information from the Member in order to locate the information requested

The Member will be entitled:

- to be informed whether his/her personal data are being processed by Alsager U3A
- to have the information constituting the personal data communicated to him/her in a permanent form (usually, this means paper copies)
- to be given a summary of the sources, recipients and purposes of the processing

The Member may apply to access their data in writing in any way they choose. You may be required to provide us with proof of your identity. The Information Compliance Officer (Chair of Alsager U3A) will decide what will be suitable proof of identity. This will normally be a membership card plus a document such as a utility bill, passport, driving license or bank statement.

On receipt of the completed request, verification of identity, and sufficient details to enable us to locate the information, Alsager U3A is obliged to respond within 1 month. The information will be supplied subject to any applicable exemptions. The data will be provided as of the date of receipt of the request.

If the Member has any reason to believe that the Alsager U3A has not dealt correctly with a request, the member should first take the matter up with the Alsager U3A Information Compliance Officer.

If the Member is still not satisfied, he/she should contact the Information Commissioner.

Information Commissioner's Office
www.ICO.org.uk
Telephone: 03031231113

16. Policy Review

This document will be reviewed and amended as necessary to ensure continued compliance with the Data Protection Act 1998 and the General Data Protection Regulation 2018.

Annex: Alsager U3A Beacon and GDPR v2 09-05-2018

Alsager U3A, Beacon and GDPR

v2 9 May 2018

Introduction

The Beacon Project Group was tasked with considering the implications of the General Data Protection Regulation (GDPR) which comes into force on 25 May 2018, and making recommendations to the Alsager U3A Management Committee. The Management Committee met on 9 May 2018 and approved the recommendations (as amended below).

This document sets out the recommendations and summary of deliberations of the Beacon project group with respect to the new GDPR requirements. They are based on Information Commission documents, Third Aid Trust guidance and advice, and the views of various Beacon users as set out on the Beacon Users Forum. In addition, at the MC meeting, we took into account guidance from consultants employed by the Third Age Trust at a conference attended by a MC member, where it was suggested that a third legal basis of processing, Contract, be considered. As a result the primary amendment to this paper is a summary of contract requirements and reasoning for not using this as the legal basis. Recommendation 5 was changed such that information will be included in letters sent out, not on the web, and Recommendation 6 was added.

Recommendations

1 Personal data held in Beacon should be the minimum required to enable management of the membership and group activities (name, contact details, gift aid entitlement). Data which should no longer be requested or held includes title, gender and emergency contact.

2 Terms and conditions will include a requirement for members who do not wish to be included on U3A group photos to take responsibility themselves for being excluded from the photo or, if they discover subsequently they have been included, to request that the photo not be used.

3 The stated and documented legal basis for processing personal data should be legitimate interests. This does not require us to seek consent in relation to personal data.

4 Membership data will be held for 7 years after an individual ceases to be a member (for HMRC purposes) and will then be deleted in its entirity.

5 Suggestions for implementation should be agreed - new enrolment forms for new members and existing members, information statements included in AGM/renewal emails and letters to members.

Reasoning

1 Personal data to be held in Beacon

All decisions need to start with the nature and purpose of the personal data being held in Beacon. Data must be adequate, relevant and limited to what is required. A sample U3A data protection policy document suggests that members of the U3A will only be asked to provide information that is relevant for membership purposes, which will include:

- name
- postal address
- email address
- telephone number
- gift aid entitlement

We have reviewed the data which we currently hold or are requesting which falls outside this list, and believe that the following are not necessary to hold:

Title

No useful purpose - many organisations nowadays avoid this and address communications by full name eg Dear Firstname Surname.

Sex/gender

No useful purpose

Next of kin/emergency contact

There are a number of reasons against holding this information.

- Holding this data would suggest a responsibility which U3A does not have
- In many cases, the information stored on Beacon would not be available in an emergency (eg on a holiday or trip)
- If held, it would probably be necessary to obtain consent of the emergency contact directly

Instead it should be the responsibility of members to carry emergency contact data if they consider it appropriate.

We therefore recommend that this data is no longer collected or held, and that any data currently held in these fields be deleted.

2 Photos

There is no suggestion that photos should be held in Beacon. However, there has been concern about taking group photos and using them for U3A publicity purposes such as in the magazine, on the website or at the open day. This has led to a belief

that we need to seek consent from members about taking photos. However, having tried to think through the process logically, we do not believe that this is necessary.

Suppose that we proceed with requesting consent for using photos, and there are two people who refuse to give this consent, and this is recorded on Beacon. The question arises about how that information is used by U3A. It would have to mean that whenever a U3A group photo is to be used, a U3A official would need to check each one to ensure that neither of the two people refusing consent was included. Apart from the logistical complexity with this, there is no guarantee that U3A officials know what any particular member looks like, and we do not keep photos on the member records. So they would not be able to carry out this duty.

Instead we believe that it is the member's responsibility themselves to ensure that where group photos are being taken they are excluded. This needs to be made clear to members, and included in the terms and conditions of membership.

3 Legal basis for processing

The GDPR requires an organisation to determine what is the legal basis for processing personal data. There are six possible bases, but the three key ones of relevance to U3A are Consent, Legitimate Interests, and Contract.

Consent

Consent is appropriate

- If you can offer people real choice and control over how you use their data - if you cannot do this, consent is not appropriate
- If you would still process the personal data without consent, asking for consent is misleading and inherently unfair
- If you make consent a precondition of service, consent is unlikely to be the most appropriate lawful basis

Legitimate interests

This legal basis can be used if data processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject which required protection of personal data, in particular where the data subject is a child.

The key elements of the legitimate interests provision can be broken down into a three-part test:

- Purpose test - is there a legitimate interest behind the processing?
- Necessity test - is the processing necessary for that purpose?

- Balancing test - is the legitimate interest overridden by the individual's interests, rights or freedoms

We believe that Alsager U3A can easily demonstrate the legitimate interests of the data which we hold:

Purpose

- to manage annual membership
- to manage membership payments
- to manage gift aid payments
- to enable communications with the membership or subsections of the membership
- to enable communications between group leaders and their group members
- to have available data for HMRC purposes

Necessity

All data held is required to achieve the above purposes

Balancing test

No individual's interests, rights or freedoms are overriden if they have voluntarily applied to be a member of Alsager U3A

Contract

Contract is an appropriate lawful basis if we need to process someone's personal data to fulfil our contractual obligations to them and the processing is necessary.

The contract does not have to be a formal signed document, or even written down, as long as there is an agreement that meets the requirements of contract law. Broadly speaking, this means that the terms have been offered and accepted, you both intend them to be legally binding, and there is an element of exchange (such as U3A services for membership fee).

We had already determined that if a prospective member refuses consent to us holding their personal data collected when joining or re-enrolling, then they could not be a member. Recommendations 1 and 2 show that we are only intending to hold the minimum data required for the legitimate purposes of the organisation. This suggests that there is no real choice or control for the member, we would still process the data or it is a precondition of them being a member. In these circumstances, Consent does not seem to be appropriate.

The choice is therefore between Legitimate Interests and Contract. Given that we are a self-help membership organisation we believe that Legitimate Interests will fulfil our requirements. The three tests are easy to understand and they require us to set out

the legitimate purposes for which data is held and processed. This can then form the basis of our privacy statement. We do not think it appropriate to start using the language of contractual services, and believe that we can fully justify Legitimate Interests. We therefore recommend that Legitimate Interests form the legal basis of processing.

We did note that some members choose to receive TAM, a membership magazine from the Third Age Trust. At present this requires Alsager U3A to pass personal member details to the TAT, which would require consent. At the meeting on 9 May it was decided that the magazine for the leaders should be sent to the Secretary for distribution, and that the few members who opt to receive (and pay for) the magazine be given the details for contacting TAT directly to request this.

4 How long to hold personal data

HMRC requires that financial data be held for 7 years. In the absence of any other advice, and given that we propose holding only minimal data, it seems sensible to hold a member's record for 7 years after they cease to be a member, and then delete the record in its entirity.

It would be possible to delete some data (email address, telephone number) once a member lapses, but this is probably unnecessary, and would require discussions of how long a member must be lapsed before this should happen.

Some implementation implications

Enrolment and re-enrolment forms

The forms will be simplified (proposed forms attached), with sections for completion on one side, information for members on the reverse. We have put the privacy statement on the front, mainly for reasons of room, but it also highlights the statement. It is consistent with the list of legitimate purposes noted above.

Online re-enrolment

It is planned to introduce online re-enrolment from November 2018. This is managed through the members portal.

In order to access the members portal a member requires the following data:

- membership number
- name
- email address
- postcode

This means that any changes of name, address or email address should already have been made and members do not need to be asked about changes. [Members can make their own changes to their records via the members portal.]

During online re-enrolment members are asked to confirm the following:

Tick if you pay UK tax and wish U3A to claim Gift Aid on your subscription (if applicable)

The principal difference between the forms and online is that online there is no immediate access to the information on the forms:

- privacy statement
- membership fees
- gift aid
- terms and conditions of membership

One way to manage this would be to include the information when sending out notifications of the AGM and renewal (emails and letters) and ask members to read them. They should be told that renewing online they will be deemed to accept the terms and conditions. At the same time they should be reminded that they can maintain their personal details through the members portal.

Deleting records

There may be some technical issues relating to deleting whole records which would need to be investigated further and resolved.

Beacon Project Group
April 2018

Updated 9 May 2018