Date 19/10/2017

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 both the Beacon Terms and Conditions of Use, and the Data Protection Act 1998 (which applies to all personal information about living individuals held either electronically or in a manual filing system). 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
- 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.

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. This data includes the addresses, telephone numbers and email addresses of U3A members, and may store other data related to their activities within the U3A.

In addition, Alsager U3A may be required by law to collect and retain certain types of personal information in order to comply with the needs of government departments.

Most of this data will be held on the Beacon system through the internet, though some data may be held on paper or on individual computers.

4. 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.

5. 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 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.

6. 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 name, 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.

7. 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 U3A's a commercial service level agreement or to have binding response times when issues occur.

As the number of U3A's 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 our support team, which we 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.

8. 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).

9. 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.

10. 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 U3A 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 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.

11. 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).

The role is 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 as set out in this document.

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

12. Use of Data

Alsager U3A holds data and processes personal information for the purpose of managing and administering Alsager U3A, its membership, its activities and its groups. This may include: administering the membership process; managing events; recording membership, managing and monitoring attendance of groups; enabling communications between members of a group; taking payments. Any use will be within the principles of the Data Protection Act.

13. Protection of Data and Compliance with the Principles of the Data Protection Act

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

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.

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'.

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 you seek

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. A Subject Access Request Form is made available for convenience. The form sets out where to send a request as well as the various ways in which you may 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 40 calendar days. 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.

16. Policy Review

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

End