LEICESTER U3A DATA MANAGEMEENT POLICY

Introduction

This document sets out how our U3A complies with its legal obligations for protection of personal data.

Policy principles

1. We collect and maintain personal data relating to members for the purpose of administering the activities of the U3A; we will not use this data for other purposes, nor will we share it with other organisations or individuals for other purposes except as specified in our Privacy Policy.

2. The personal data we maintain are: name, address, whether address is shared with another member, email address, telephone numbers, membership of other U3As, payment history and, for trips and other events, contact details of someone who can be contacted in the event of an emergency affecting the member.

3. Personal data are obtained directly from members at the time of joining. We ensure the accuracy of the data by asking members to verify it at least once a year. We also ask members to let us know of any changes to their data.

4. We keep this data only for as long as a person remains a member and for a defined period afterwards; this is in line with our obligation to retain financial records for seven years.

5. In addition to point 3 above, we will give a person who requests it the information we hold about them and, if necessary, give them a chance to correct it.

6. We protect personal data by keeping it within a secure computer system ("Beacon") centrally managed by The Third Age Trust. Access to this system is restricted to specific members authorised by the Committee.

Guidance notes

A) For all members

1. Please advise the Membership Secretary (membership@leicesteru3a.org.uk) as soon as possible of any changes to your personal details.

2. Please ask the Membership Secretary if you would like to see the information we hold about you; you will be able to correct any errors in the details.

3. Note that any personal data that you receive as part of your U3A membership should be treated as confidential.

B) For anyone handling personal data

1. You must not reveal data to anyone who is not entitled to see it under this policy.

2. If someone, even a fellow group member, asks for data belonging to another member (e.g. contact information), you should yourself seek the permission of the member concerned to disclose it before doing so.

3. If you keep personal data on a computing device, you must
   a. ensure that the computer is fully up to date with operating system and anti-malware software;

b. ensure that the personal data is not accessible to anyone else. As a minimum, the device must be secured with a password; this is particularly important in the case of mobile devices – laptops, tablets, and mobile phones. If the device is shared with others, you must ensure that only you are able to access the data; one way of doing this is to keep it within a word processing document or spreadsheet that is itself password-protected.

4. If for any reason you send personal data by email, you should seek the permission of the member(s) involved. Email does not in itself offer a secure means of communication; it is safer to place personal data in a password-protected file and attach this to an email, and to let the recipient know the password via phone or text message.

5. If you keep personal data on paper, you must exercise similar care. When you dispose of it, you must destroy the papers or otherwise make them unreadable (e.g. through shredding). If you send personal data through the post, you must do so in a sealed envelope.

C) For Beacon users

1. Rules on password composition are imposed by Beacon, but it is your responsibility to ensure that your password is of sufficient strength and to keep it secret from others.

2. On any computer used to access Beacon, it is your 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.

3. You must not allow anyone else to use your Beacon account.

4. When using a shared computer, you are recommended to only use a Beacon account within a personal logon. If you do not have a personal logon, then you should **not** tick the 'Local computer' checkbox at login, nor should you allow your browser to autofill the logon screen.

5. A Beacon account must never be accessed on a public computer, e.g. in a library.

6. You should always logout of your account when finished. Beacon will automatically log you out if you make no input for 20 minutes.

D) For Group Convenors

1. You must ensure that the personal data you maintain and use is managed in line with the Policy Principles in Section A on p1 above, even if it's held on paper. You will also need to co-operate with requests from the Membership Secretary to supply what personal data you hold in order to satisfy requests from members under Policy Principle A5 on p1.

2. We are committed to keeping members' personal data private. This means we must not disclose members' email addresses or other contact information, even to one another. The best way to ensure this in email is to use "bcc:" (blind copy).

3. A group or some of its members may decide to share each other's contact details and to use "cc:" in email instead; this makes it easier to have an email discussion among the group, for example. However, this must be done *with the individual agreement of all participating members.*

4. Note that under Policy Principle A1, we must not use members' personal data for any purpose other than running our U3A. Using a member email distribution list to advertise outside events or promotions, for example, is not allowed.

5. If a member of your group is no longer a member of our U3A, then you must destroy any personal data you hold on them.

6. You should advise the Groups Coordinator when people join or leave the group so that group membership may be updated on Beacon.

7. If you cease to be a convenor, you must destroy all copies you hold of the group members' personal data outside Beacon; you should not retain historical records of group membership. [See Deleting Data below.]

E) For Groups Coordinator

1. When a new group is set up or a new convenor is appointed to an existing group, the convenor must be reminded of their obligations under this policy.

2. If a convenor relinquishes their role, they should be reminded of the requirement to destroy all their copies of member records, and confirm that this has been done.

F) For Membership Secretary

1. If a member asks to see the personal information we hold about them, you will need to:
   (a) Determine to which groups the member belongs and request any data that might be held by the convenors outside Beacon;
   (b) Extract the member's details from Beacon;
   (c) Collate this information and supply to the member;
   (d) Make any corrections requested by the member and pass on to the convenors identified in (a) above for them to correct their information.
2. Convenors should be notified when someone is no longer a member of the U3A and reminded that the corresponding personal data should be deleted from their records.

Deleting personal data

The deletion of personal data is an important activity in data protection, given the fifth data protection principle's requirement that "personal data processed for any purpose or purposes shall not be kept for longer than necessary".

1. Any paper records should be shredded, incinerated or otherwise made unreadable before being put into household rubbish, recycled or otherwise disposed of.
2. Any records kept on computer outside Beacon should be deleted. Also, check the Recycle Bin or equivalent and delete any copies that have been kept there.

Approved June 2018
Reviewed November 2021
Next review due November 2024