Ashfield U3A Policy Document

Beacon and the role of the Beacon Administrator

Pre-amble:

Beacon is the Cloud-based Administration system for U3As. The system is run through a website, not an application on someone’s PC and all data is securely stored in the Cloud. By adopting Beacon, we have effectively accepted that the Third Age Trust ensures that data security meets all GDPR requirements other than those controlled by the access we give to users. It can be used to manage most aspects of membership, groups and finances. It can also be used to contact members by email if they have an email address. Members’ personal data is not shared by processes in Beacon unless a system user deliberately does so.

Policy:

1. Allocation of access to the Beacon System.

Committee members and others (e.g. group co-ordinators) can be given access to different aspects of Beacon by the Administrator as agreed by the committee. In order to gain access, U3A members must submit, in writing, their perceived needs. The committee, advised by the administrator, will agree minimum access needed for the member to fulfil any legitimate needs.

2. Advice to users.

Users of Beacon will be advised that they must not save members’ data to their own storage device or print unless it is a list of group members’ names plus, if members have agreed, telephone numbers and emergency contact details (this must be in writing, for example on a register).

Non-compliance with this would contravene GDPR and leave the Beacon user liable to prosecution. Beacon users must consult the Ashfield U3A GDPR document to ensure that they understand and do not contravene it.

Users of the Beacon system must not share their ID and password with anyone else. If a second person, for example assistant group leader, needs the same access, they must apply to the committee for their own access. Contravention of this could result in the loss of access to the system.

If Beacon is used on a shared computer, each user should have their own computer login account.

Beacon must not be accessed via a public computer, e.g. in a public library.

Users of the Beacon System must ensure that their computer has adequate protection against viruses and mallard which might enable unauthorised access to the Beacon system.

3. The Beacon Administrator.

The Beacon Administrator has almost full control of the Ashfield U3A part of the Beacon system. This is an essential part of being able to administer the system. As such, the administrator should be chosen, wherever possible, from established and trusted U3A members.

The Beacon Administrator must notify the Committee immediately of any personal data breach. The Committee will then immediately advise TATTL in writing.

Policy Date September 2022

Review Date September 2025