ADDITIONAL DATA PROTECTION GUIDANCE FOR THE BARNSLEY AND DISTRICT U3A

AIMS OF THE DATA PROTECTION ACT

The data protection act obliges everybody to process personal data in accordance with the law, balancing a legitimate need of organisations to use information with the rights of individuals with regard to how their information is processed.

U3As, as not for profit organisations, are exempt from registering with the information Commissioner's office (ICO), provided that:

1. Processing of personal data is only for the following purposes
   - Establishing or maintaining membership.
   - Administration activities for individuals who are members.
2. Data held is for current members only.
3. The only data held is that which is necessary for membership, i.e. names, addresses, and identifiers.

OUR OBLIGATIONS UNDER THE ACT

Even though we as U3As do not have to register, we still have to comply with all other requirements of the act, and we remain subject to penalties for any offences.

THE EIGHT DATA PROTECTION PRINCIPLES WHICH WE MUST ADHERE TO

1. U3A membership shall be processed fairly and lawfully. We can only request information that we legitimately need, and that members would reasonably expect us to have. We cannot use the data for anything unlawful or that would adversely affect a member, and the member *must* be made aware of how their data will be used.
2. Personal data can't be used for any other purpose other than that specified and agreed to by a member. Changes in usage must be done with full disclosure and with their specific consent.
3. Only the *minimal* amount of data required can be kept that enables us to administer U3A membership.
4. Member data has to be kept up-to-date, and we should take all reasonable steps to ensure accuracy of the data we collect.
5. Member data must only be kept as long as necessary for the purposes of administration. We can, for instance, keep data for a short period after membership has lapsed, but only for an agreed fixed time, e.g. for 3 months from the time that membership fees were due. After which time we *must* delete their data from Beacon, and also be vigilant in destroying any physical copies of their data wherever held.
6. We must comply with each member's rights under The Data Protection Act. This means we must provide a copy of the data we hold whenever requested by the member. We must prevent their data being used for direct marketing (outside of our charitable U3A activities). We mustn't allow decisions to be made regarding their membership using purely automated means, for instance, member exclusion because of unpaid membership fees cannot be processed automatically without human intervention.
7. We must ensure that we take appropriate technical and organisational measures to prevent any unlawful processing of our membership's personal data. Any member data held outside of the Beacon system needs to be kept in a suitably secure place such as a locked filing

cabinet, or shredded and disposed of safely. We must also take measures to prevent accidental loss or change to the membership data.

8. Membership data cannot be held or transferred outside of the UK U3A parent organisation. We rely to a great extent on the administrators of the Beacon system to ensure that we comply with where the data can legally be physically held. For this reason, it is very important that we do not use any system, other than Beacon, for membership data retention.

U3A MAIN DATA CONSIDERATIONS

- Any person looking after membership data should be a Barnsley & District U3A committee member.
- We must be very clear on any forms that membership data will be held on computer, and used for contact purposes and to circulate information about the U3A and our activities.
- We must keep the information accurate and up-to-date.
- We must delete and destroy personal information as soon it is administratively possible when a member leaves. However, this should not include gift aid and financial records, which legally have to be retained for a minimum of six years.
- We must keep the number of committee members holding (or accessing) the full membership database to the absolute minimum. As we are using Beacon, all efforts must be taken to ensure access to member data is restricted to only whatever is necessary. When group coordinators require contact information, the best way is for them to request only what is necessary directly from their group members.
- Passwords that protect the membership database must be strong, at least 12, preferably 16 letters, containing upper and lower case, letters and numbers. Avoid the temptation to use recognisable words. This implies that anyone with access to the Beacon system and membership data must have a strong password for access, and they must take all reasonable precautions to keep that password secure.
- Avoid issuing hard copies of membership data.

We can summarise any data protection concerns with regard to using storage within “the cloud” by stating that, we will only be storing membership data within the Beacon system which is administered by the U3A parent organisation.

COMMITTEE MEMBERS

Committee members should ensure that any computer system used in administrating membership information (e.g. used for accessing the beacon system) is kept up-to-date and as secure as possible by having suitable and effective high grade antivirus protection (for example; Bitdefender, ESET NOD32, Kaspersky, or Norton), and by keeping that antivirus protection up-to-date.