**Dronfield and District u3a**

**Personal Data Management**
**Version 1.2**

**This document is available on the Policies page of the DDu3a website.**

Date Approved: 19 Aug 2024
Next Review Date: No later than July 2026

**Background and Objectives**

This document sets out how Dronfield and District u3a (DDu3a) complies with its legal obligations for the protection of personal data (ie data that could be used to identify, or is related to the identity of an individual) and **MUST** be used in conjunction with the DDu3a Privacy Policy and Legitimate Interest Assessment.

**1. All Members**

a. ANY personal data that you receive as part of your u3a membership MUST be treated as confidential. It is the legal responsibility of each member to do so .

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

c. If you keep personal data on a computing device, you must:

   i. Ensure that the computer is fully up to date with operating system and anti-malware software.

   ii. 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.

d. Lists of members' personal data (email, postal addresses, phone numbers) must not be shared by email. The sharing of an individual's contact details is permitted, but only with the express permission of the individual concerned.

e. 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 (eg through shredding). If you send personal data through the post, you must do so in a sealed envelope.

**2. For Beacon users**

a. 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.

b. On any device used to access Beacon, it is your responsibility to ensure that suitable security measures have been taken to keep that device free of viruses and other malware that might enable unauthorised access to Beacon.

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

d. When using a shared device, you are recommended to only use a Beacon account within a personal logon on the shared device. If you don't have a personal logon, then you should not tick the 'Local computer' checkbox at login, nor should you allow your browser to auto-fill the logon screen

e. NEVER use a Beacon account on a public computer, e.g. in a library

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

**3. For Group Coordinators (GCs)**

a. DDu3a is legally obliged to ensure the personal data it holds is accurate. This becomes harder if it is kept in several places; it is therefore recommended that GCs use the Beacon system, which provides a single source of member data.

b. If for whatever reason you do not use the Beacon system, then you must ensure that the personal data you maintain and use is managed in line with the Privacy Policy, 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 the Privacy Policy.

c. DDu3a is committed to keeping members' personal data private. This means members must not disclose other members' email addresses or other contact information, even to one another, without their explicit permission The best way to ensure this in email is to use "bcc:" (blind copy); the Beacon system automatically uses this on all emails it sends out.

d. Where group members decide to use a group messaging service (WhatsApp or similar) or individually exchange contact details, or use "cc:" in email instead of bcc, this MUST be an individual decision for each member of the group. No individual group member may share anyone else's data with anyone else without their explicit permission.

e. Note that under the DDu3a Privacy Policy, members' personal data must not be used for any purpose other than running DDu3a. Using a group membership list to advertise outside events or promotions, for example, is not allowed.

f. If you cease to be a GC, you must destroy all copies you hold of the group members' personal data outside Beacon; you should not retain historical records of group membership.

**4. For Groups Manager(s)**

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

b. If a GC relinquishes their role, you MUST:

   i. Ask the Systems Administrator to remove the GC's access to Beacon.

   ii. Remind the GC of the legal requirement to destroy all their electronic and paper copies of member records and confirm this has been done.

## 5. For the Membership Secretary

If a member asks to see the personal information DDu3a holds about them, you must:

a. Determine to which groups the member belongs and request any data that might be held by the GCs outside Beacon;

b. Extract the member's details from Beacon;

c. Collate this information and supply it to the member;

d. Make any corrections requested by the member and pass them on to the GCs identified above for them to correct their information.

| **Document History** | | |
|---|---|---|
| **Date** | **Version Number** | **Summary of Changes** |
| 19 Aug 2024 | 1.2 | All urls pointing to DDU3a's old website removed in preparation for website migration to SiteWorks.<br>Reference to DDu3a's Legitimate Interest Assessment added to Background and Objectives. |
| March 2023 | 1.1 | Reformatted and paragraph numbering changed (eg from 1.1 to 1.a) to meet DDu3a's policy standards<br>Change of terminology U3A to u3a<br>Para 1.c.ii and 1 d rephrased.<br>In 4.a reference to a 'Group Coordinators Roles and Responsibilities' form removed. |
| Feb 2019 | 1 | Replacement for Data Management Policy 5.0 (now obsolete); linked to Privacy Policy |