

Bristol u3a – Data Protection Guidance for Group Leaders

1. Don't Misuse Data

You should only use u3a data for running your group. You must make sure that your group members have explicitly agreed to share their contact details within the group: you can keep this simple by circulating an email (blind copy) or a sign-up sheet to obtain consent (and including consent to share across the group). It follows that you must delete people's details as soon as they leave your group.

2. Minimise Data Extraction, Use and Retention

Our membership records are securely stored on Beacon, and this is generally the safest place to keep them. If you must store data outside Beacon then you should only do so for as long as you need it to run your group. Once you no longer need it you must delete it, leaving only the Beacon records.

You may not share personal data with anybody unless you are authorised to do so and unless you have their explicit consent. For this reason it will be necessary to carefully consider whether group emails should be sent "blind copy". Groups can function better when members are in touch with each other, so you will want to obtain explicit consent to sharing email addresses across your group.

3. Store Data Securely

If you have to store personal data outside Beacon then you must keep it securely. In a domestic situation you should take steps to ensure that only you have access to the relevant data, by using password protection and, where appropriate, encryption. You should not put personal data onto social media platforms or allow such platforms to harvest our data, nor should you put data onto "cloud" storage unless you know that it will meet EU (or post-Brexit) standards. It is extremely poor practice to use USB sticks to store members' details and you should not do this.

4. Sending Data

Email is not a secure means of exchanging personal data, such as names, addresses and contact information. You must ensure that any data sent in this way is available only to the recipient(s). This might be done by sending the data as a password protected attachment or encrypting it.

You must send a password using a different method to the method you used to send the data (for instance by SMS text message). Good password practice uses a strong password with a minimum of 8 characters which includes a combination of lower and uppercase letters and numbers and characters such as "?" or "!". It might also be useful to include spaces in passwords.

5. Hardcopy Data must also be protected

Hardcopy data must be securely stored so that only you can access it. Once it is no longer required it must be destroyed. This might mean using a crosscut shredder or even a professional confidential waste service provider. (There is at least one in Avonmouth which provides a retail service).

6. Photographs

Photographs of group members are personal data. Photographs of individuals should not be published without the explicit consent of that individual. Where group photographs are being taken and may be circulated members should be asked to step out of shot if they do not wish to be in the photograph.

7. If there's an issue

All data breaches and any Subject Access Requests must be reported immediately to the Bristol u3a Data Protection Officer. Currently this responsibility is vested in the Secretary who can be contacted at secretary@bristolu3a.org.uk.

More information on GDPR compliance can be found on the Members' Info section of the Bristol u3a website.

Last updated 25th July 2022