

Whitchurch and District u3a Compliance with General Data Protection Regulation (GDPR)

Whitchurch and District (W&D) u3a needs to keep personal data about its members in order to carry out its activities.

To comply with the law, personal information must be collected and used fairly; stored safely and not be disclosed unlawfully. These rules apply however such data is acquired, stored or used.

This document states how W&D u3a will comply with the law and follow good practice, protect the rights of members, be open about how it stores and uses individual's data, and will protect data from unintended disclosure.

All personnel with access to members' data must observe this policy, and related procedures. The W&D u3a committee is ultimately responsible for ensuring this policy is upheld.

~~oOo~~

W&D u3a will collect, store, use, amend, share, destroy or delete personal data only in ways which protect people's privacy and comply with the general data protection regulation (GDPR) and other relevant legislation.

To this end:

W&D u3a will only collect, store and use the minimum amount of data that is needed either for legal reasons, or for clear u3a purposes for which the individual has given explicit consent.

W&D u3a will store personal data securely and not share this data with third parties without the explicit consent of the individual unless legally required to do so.

W&D u3a will endeavour to keep personal data up to date and accurate. On request from the relevant individual W&D u3a will provide details of the data held on them, and amend or delete such data if requested unless required to keep it for legal reasons.

~~oOo~~

To uphold this policy, W&D u3a will maintain the following set of data protection procedures.

Electronic data will be kept securely on the u3a Beacon management system.

Members of W&D u3a and any others acting for or on behalf of W&D u3a must at all times respect the privacy and security of all confidential and private data (personal data) to which they have access whether in paper, electronic or other forms. This means they only use such personal data for W&D u3a purposes and for no other purposes whatsoever. They must take all reasonable care to ensure they do not make any inadvertent or unauthorised disclosures of any personal data.

Wherever possible, the Beacon membership management system should be used to record and contact members.

Any downloaded personal data should contain the minimum information necessary for the intended activity. If required for ongoing purposes this must be stored securely. Otherwise it must be securely destroyed or deleted as soon as the activity is complete.

Personal data should not be shared (either informally within a group or outside the u3a) unless prior consent for specific and agreed reasons is given by the data subject.

Personal data held on a computer or other electronic device must be encrypted with a strong password for access.

Members must not allow any other person to use or have access to their Beacon system account.

A shared computer must not be used to access a Beacon system account unless the user has a personal logon for the shared computer.

Access to the Beacon system via a public computer, e.g. in a public library, is strictly prohibited.

The security procedures and systems on any electronic device used to access the Beacon system should be kept updated to the latest version.

~~~~~