

DATA Protection for Beacon users

The Beacon database gives group leaders access to personal information about members of Bridport and district u3a. This information MUST NOT, under any circumstances, be shared with another person whether a member of u3a or not.

The following paragraphs are relevant extracts from the u3a Data Protection Policy.

- Access to data within a u3a site is controlled by the User u3a's Administrator. Usernames, passwords and the privileges associated with each User's role are allocated by the User u3a's Administrator.
- Each User u3a Member is advised that it is essential that their password is kept securely and secret from others.
- The u3a committee will advise each member granted specific access to the Beacon System that access to it is conditional upon having taken adequate and reasonable measures to ensure that their computer is free of viruses and other malware which might enable unauthorised access to the Beacon System.
- The u3a committee will advise any User granted specific access they must not allow any other person to use or to have access to their Beacon System account. In particular, 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

In addition, please log off from Beacon or close your browser when finished