Ambleside & District u3a

As a u3a participating in Beacon we are responsible for ensuring that our Beacon users keep to the following conditions. The Beacon team reserves the right to suspend or terminate any user's account if they don't abide by these conditions.

1. Access to data within a Beacon account is controlled by the user's name, password and the privileges allocated by the u3a.

2. Rules on password composition are imposed by Beacon, but it is a user's responsibility to ensure that their password is of sufficient strength and to keep it secret from others.

3. On any computer used by a user to access Beacon, it is the user's responsibility to ensure that reasonable security measures have been taken to keep that computer free of viruses and other malware which might enable unauthorised access to Beacon.

4. Users should not allow anyone else to use their Beacon account.

5. When using a shared computer, users are recommended to only use a Beacon account within a personal logon on the shared computer.

6. When using a Beacon account on a public computer, e.g. in a library, users should use the 'In Private mode' (IE) or equivalent, if available, and ensure that form history is not enabled. They should not tick the 'Local computer' checkbox at login so that cookies are not stored.

7. Users should always logout of their account when finished. Beacon will automatically log out users who make no input after 15 minutes.

Frances Green

Beacon Administrator 17/12/2022