



DOWNHAM MARKET & DISTRICT U3A DATA PROTECTION POLICY

Statement Principle

This policy complies with the guidance from the Third Age Trust and the eight principles within current UK data protection legislation.

The Data Protection Act obliges everyone to process personal data in accordance with the law. Its aim is to balance the rights of individuals with regard to how their information is processed with the legitimate need of organisations to use information.

Practice Principles

Downham Market & District U3A applies the following principles to the management and storage of members' data

1. Information is held securely in the Beacon Online Management System and is not shared on a routine basis
2. Beacon users will comply with the conditions in Appendix A.
3. Information held by Downham Market & District U3A is only used for the purposes that will:
 - 3.1. facilitate the function of Downham Market & District U3A i.e. the maintenance of membership lists and financial records
 - 3.2 update the national database of the U3A Trust.
4. Downham Market & District U3A will from time to time publicise the work of the U3A both locally and with the Third Age Trust and this may include photographs of U3A activities. The Committee seeks individual consent at the time of joining to use images in this way according to the imagery policy. Members give consent on the membership form and may withdraw consent at any time by contacting the Membership Secretary.
5. Committee members of Downham Market & District U3A only have information relating to members if they need such information to complete the duties required by their role. Committee members are required to destroy any information (including digital and audio) they hold when they cease to serve on the Committee.
6. Information held by Downham Market & District U3A which is supplied by members is held at the discretion of that member and remains their property.
7. Personal data is deleted as soon as is reasonable after a member resigns from Downham Market & District U3A, with the exception of gift aid data that has to be kept for a minimum of six years.
8. Group Leaders are asked to keep records up to date and to delete digital/filed/audio information relating to members who have left their group.

Should any member of Downham Market & District U3A believe that their rights in respect of personal data have been infringed they may outline their concerns in writing to the Business Secretary or Chairman of the Committee who will try to address the concerns raised. If the member feels that their concerns have not been fully addressed they can request that the matter be referred to the Regional Trustee for investigation. The outcome of any investigation will be conveyed to the member in writing.

This policy will be reviewed every two years or sooner in the event of changes to the UK protection policy.

Signed:

John Cowin, Chairman of the Downham & District U3A.

August 2021



Downham Market and District U3A Data Protection Policy

APPENDIX A

Responsibilities for security: BEACON SYSTEM

- 1) Downham Market and District U3A is responsible for deciding which members may have a BEACON users account, and the privileges they shall be allocated.
- 2) Downham Market and District U3A is responsible for ensuring that its BEACON users keep to the following conditions:
 - a) Access to data within a Beacon account is controlled by the user's name, password and the privileges allocated by the U3A.
 - b) 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.
 - c) On any computer used by a user to access Beacon, it is the user's responsibility to ensure that suitable security measures have been taken to keep that computer free of viruses and other malware which might enable unauthorised access to Beacon.
 - d) Users should not allow anyone else to use their Beacon account.
 - e) When using a shared computer, users are recommended to only use a Beacon account within a personal logon on the shared computer.
 - f) 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.
 - g) Users should always logout of their account when finished.

I have read and agree to comply with Downham Market & District U3A Data Protection Policy and the responsibilities for security when using the Beacon system.

*Signed:	*Date:
*Name: Please print	