**BOURNEMOUTH EAST ALLOTMENT SOCIETY LIMITED**

**ACCESS TO ELECTRONIC INFORMATION AND CLOUD STORAGE POLICY**

*First adopted on December 2019. Last reviewed on 22nd November 2023 and adopted at AGM on 6th December 2023*

**BACKGROUND INFORMATION**

Originally registered as a Friendly Society in 1935 under the Industrial and Provident Societies Act (1893), Bournemouth East Allotment Society Ltd was re-registered in 2018 under the Co-operative and Community Benefit Societies Act 2014. It is affiliated to the National Allotment Society, previously the National Society of Allotment and Leisure Gardeners Ltd. The allotment sites are leased from Bournemouth, Christchurch & Poole Council and managed by an elected committee.

1. **Purpose**
   To set out the arrangements for access to information stored electronically for Committee Members, including Cloud storage and ensure that data is protected and only accessed by authorised users.

2. **Scope**
   The policy and guidance applies to all Committee Members, co-opted Committee Members or designated users such as volunteer administrators or suppliers. Any exceptions to this must be documented and approved by the Committee. Related document: Data Protection (GDPR) Policy.

3. **Definition**
   For clarity, Cloud storage refers to any third party online storage such as OneDrive, Dropbox, Google Drive or similar file storage. Sharing via Cloud storage gives us much more flexibility and allows convenient access to files and data from a number of different devices and confidence that we are looking at the latest information. However, it is essential that all Committee Members follow the guidance in this policy to protect the data.

4. **Confidentiality**
   All Committee Members must have access to any information available to enable them to carry out their role and responsibilities. This information must be accessed and used sensitively to ensure that data remains confidential where appropriate and in accordance with the Data Protection (GDPR) Policy.

5. **Data Stored**
   For clarity the data stored on members is limited to title, name, address, telephone number(s) and email address. Personal details such as date of birth or bank details are not required for our purposes.

6. **Guidance**
   - 6.1 New Committee Members will be given the required passwords and induction into our system for storing and accessing files, with guidance on which documents can be shared on the Cloud.
   - 6.2 If a member leaves the Committee their access will be removed and for further security all passwords will be changed.
   - 6.3 The main BEAS computer, held by the Secretary, contains all current and archived documents concerning the membership, finance, policy documents and other relevant BEAS business documents. These are stored on the hard drive, with a number of identified key documents also available on OneDrive with links being shared with Committee Members as appropriate.

6.4 For ‘business continuity’ purposes, the BEAS Computer is ‘backed-up’ up each month onto a separate, portable Hard Drive.
6.5 The Software Package is Microsoft 365 and all documents must be shared from the computer so that ownership is clearly retained by BEAS.
6.6 MacAfee Security Software is used on each BEAS Computer.
6.7 Where documents are made available for information purposes only, they will be in read only format.
6.8 Committee Members with responsibility for updating information will have permission to edit.
6.9 Committee Members should not download documents or files that include member details and retain them on their personal computers unless authorised to do so by the Committee.
6.10 The Cloud can be used for collaborative working, for example, when comments are requested on a document or others are required to contribute to different sections (e.g. the newsletter). Finalised documents will be read only, with only the author having editing rights.
6.11 Only the latest versions of documents will be shared in Cloud storage. For example, the most recent Data Protection Policy will be shared, with any previous versions being deleted or archived as appropriate.

7. **Email addresses**

All Committee Members will be assigned a BEAS email address to use for Committee business. This email address can be used for official contact and correspondence for Committee business as it enables an automatic record to be retained where appropriate. This provides a more professional ‘face’ for the society and protects the Committee Member’s personal email from wider circulation.

Note that it is acknowledged that a lot of correspondence is likely to be of a ‘chatty’ and friendly variety as the normal day-to-day business is done. Emails that do not need to be retained can be deleted and more official correspondence retained or filed as appropriate.

The email address is provided on the following basis:

- The assigned email address for the relevant Committee post must be the one that is published for that Committee Member on official BEAS communications.
- A password will be provided to enable that email box to be accessed from a personal computer or mobile device.
- When a person ceases to be a Committee Member, the email box will be disabled from personal devices.
- For added security all passwords will be changed by BEAS.

8. **Further Guidance for Creating and Storing Documents**

To ensure that there is clarity on the final version of documents, the following guidance should be observed when creating and finalising documents:

- It is acceptable and practical that Members may create and save documents relating to a project or work for the Society on their personal computers. However, where it is necessary that the document should be retained by the Society for future reference, then the finalised document must be sent to the administrator who will ensure it is saved on the BEAS Computer as a BEAS document.
- Data for BEAS Members should not be downloaded and stored on personal PCs.
- Where a Committee Member is asked to contribute to or edit a document that is shared, that is the document they must work on so that the latest version is always available. For example the monthly reports.

- All report titles must clearly say whether it is a draft or a final version e.g. ***Minutes 29 Jan 2018 final***. In these cases, all previous versions or draft versions must be deleted to avoid confusion.
- In the case of Policy Documents, or other documents that are reviewed or updated regularly, the version number and date must be clearly stated and all previous versions archived for our records e.g. ***Health & Safety Policy V4 2018***. The version number and date should also appear on the footer of each page of the document.

I have read and understood what is required in accessing IT systems and information about BEAS and their Members in my role as Committee Member.

Signed …… Date …….