WPWC DATA HANDLING POLICY 2019

1. The Membership Secretary is WPWC's data controller. WPWC membership data, in paper and /or digital form, will be kept securely by the Data Controller. The annual membership list and other files containing personal data will be encrypted using a strong encryption algorithm (e.g. AES). These files may be shared, encrypted, in a limited access Dropbox folder.

2. The Secretary, Treasurer, and Chairman will be made aware of the encryption keys, in order to access the data for the purposes of their legitimate interests in operating the club.

3. All devices used to access WPWC data must meet the following criteria:-

- Have up to date Operating System software.
- Be regularly scanned for Virus and Malware.
- Require a username and password logon.
- Automatically logout when left unused/unattended.

4. WPWC data should not, except when absolutely necessary, be accessed from mobile devices (e.g. Tablets, Mobile Phones etc.). Special care should be taken to ensure all WPWC data is securely encrypted if stored on Laptop computers that are removed from a secure environment.

5. Copies of WPWC files containing personal information held by club officers or any other authorized club member, must be kept encrypted, and should not be stored on portable media (USB drives, USB memory sticks, SD cards CD, DVD etc). Such copies should be retained only as long as necessary to conduct legitimate club business.

6. Encrypted offline backups of WPWC data will be made at regular intervals and stored securely.

7. Personal data which is no longer required for the purposes of the Committee's legitimate interests in operating the club will be securely erased/destroyed.