Lancaster and Morecambe u3a

In accordance with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018, we require you to sign this Confidentiality Agreement which sets out what you will do with any personal data you use in the course of your activities with us and on our behalf.

The Agreement:

I agree at all times, to respect the privacy and security of all confidential and private data to which I have access within the course of my volunteer duties for Lancaster and Morecambe u3a, whether in paper, electronic or other forms ("the Personal Data"). This means that I will use the Personal Data for the purposes of fulfilling my voluntary role with Lancaster and Morecambe u3a and for no other purposes whatsoever. I will at all times act on the reasonable instructions of Lancaster and Morecambe u3a in relation to the Personal Data. I agree that I will take all reasonable care to ensure that I do not make any inadvertent or unauthorised disclosures of the Personal Data. I also agree that I will return all the Personal Data to Lancaster and Morecambe u3a at its request.

Any Personal Data held by me will be deleted or otherwise destroyed once the reason for holding the data has passed. Personal Data held on a personal computer will be encrypted with a strong password for access.
Personal Data should not be shared (either informally within a group or outside the u3a} unless prior written consent, for specific and agreed reasons is given by the data subject.

In relation to my voluntary role: I agree that my contact details may be made available to group members and the wider membership within Lancaster and Morecambe u3a.

To ensure compliance with data protection regulations it is recommended that the Beacon membership management system is used to contact Interest Group members and record participants. Any downloaded attendance register for use at group meetings should only contain a list of member names.

You must not allow any other person to use or have access to your Beacon system account.

A shared computer must not be used to access a Beacon system account unless you have 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

I understand that it is the user's responsibility to ensure that suitable security measures have been taken to keep any computer used to access Beacon free from Viruses and Malware.

Any computer used for storage of Personal Data must have any critical updates to firmware, operating systems, software and programs installed. *(Firmware is code that is embedded in chips within a computer to provide basic operating functions and communication with software programs. From time to time the coding may be updated by the chip or computer manufacturer to take account of potential security threats.)*

Name.....Membership No.....

Signed.....Date.....

10/5/24 PJ