Prestwood Community Association (PCA)
Data Protection Policy

1) Definitions

1. Personal data is information about a person which is identifiable as being about them. It can be stored electronically or on paper, and includes images and audio recordings as well as written information.

2. Data protection is about how we, as an organisation, ensure we protect the rights and privacy of individuals, and comply with the law, when collecting, storing, using, amending, sharing, destroying or deleting personal data.

2) Responsibility

1. PCA is committed to the legal principles of data protection, which include lawfulness, fairness and transparency; purpose limitation and data minimisation; accuracy; integrity and confidentiality of storage; accountability.

2. All volunteers are responsible for observing this policy, and related procedures, in all areas of their work for the group. Overall and final responsibility for data protection lies with the management committee.

3) The Data we will keep

1. PCA needs to keep personal data about its committee, members, volunteers and supporters in order to carry out group activities.

2. The committee needs to be in contact with one another in order to run the organisation effectively and ensure its legal obligations are met. Committee contact details will be shared among the committee. Committee members will not share each other's contact details with anyone outside of the committee, or use them for anything other than PCA business, without explicit consent.

3. PCA will maintain a list of names and contact details of people who wish to receive communications from PCA. When people sign up to the list we will explain how their details will be used, how they will be stored, and that they may ask to be removed from the list at any time. We will only send them messages which they have expressly consented to receive. If using mailing list providers, we shall use providers who store data within the EU.

4. PCA will maintain a list of contact details of our volunteers. We will share volunteering opportunities and requests for help with the people on this list.

5. PCA may from time to time hold surveys of local residents, which may include some personal data.

4) Use and Storage of Data

1. PCA will collect, store, use, amend, share, destroy or delete personal data only in ways which protect people's privacy and comply with the General Data Protection Regulation (GDPR) and other relevant legislation.

2. We will only collect, store and use the minimum amount of data that we need for clear purposes, and will not collect, store or use data we do not need.

3. We will only collect, store and use data for:
• purposes for which the individual has given explicit consent, or
• purposes that are in our our group's legitimate interests, or
• contracts with the individual whose data it is, or
• to comply with legal obligations, or
• to protect someone's life, or
• to perform public tasks.

5) People's Rights relating to their Data

1. We will provide individuals with details of the data we have about them when requested by the relevant individual, and explain how it is being used.
2. We will delete data if requested by the relevant individual, unless we need to keep it for legal reasons.
3. We will endeavour to keep personal data up-to-date and accurate.
4. We will store personal data securely. When it is stored electronically, it will be kept in password protected files. When it is stored online in a third party website (e.g. Google Drive) we will ensure the third party complies with the GDPR. When it is stored on paper it will be filed carefully in a locked filing cabinet.
5. We will keep clear records of the purposes of collecting and holding specific data, to ensure it is only used for these purposes.
6. We will not share personal data with third parties without the explicit consent of the relevant individual, unless legally required to do so.
7. We will endeavour not to have data breaches. In the event of a data breach, we will endeavour to rectify the breach by getting any lost or shared data back. We will evaluate our processes and understand how to avoid it happening again. Serious data breaches which may risk someone's personal rights or freedoms will be reported to the Information Commissioner's Office within 72 hours, and to the individual concerned.

6) Review

This policy will be reviewed every year

Date: 17th December 2025

Signed and approved by:

Karen Pither (Chair)

Robert Gibson (Treasurer)