

Data Protection Policy

Introduction

Burrenbeo Trust are committed to upholding privacy and data protection rights. The following document outlines the organisation's application of the eight data protection principles. The policy applies to all personal data processed by the organisation, including members data, third party data and employee data.

Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal data, in both paper and electronic format. The Data Protection Acts 1988 and 2003 (the "Data Protection Acts") lay down strict rules about the way in which personal data and sensitive personal data are collected, accessed, used and disclosed. The Data Protection Acts also permit individuals to access their personal data on request, and confer on individuals the right to have their personal data amended if found to be incorrect. This document outlines Burrenbeo Trust's policy to help ensure that we comply with the Data Protection Acts along with The General Data Protection Regulation (GDPR) under the EU Data Protection Directive.

Inquiries about this Data Protection Policy should be made to: Data Protection Co-Ordinator, Burrenbeo Trust, Glebe Road, Kinvara, Co. Galway.

Data Protection Policy

Purpose of this policy

This policy is a statement of Burrenbeo Trust's commitment to protect the rights and privacy of individuals in accordance with the Data Protection Acts.

Collecting information.

We collect and use information to provide the following services:

- To communicate with members.
- To undertake advertising, marketing, direct marketing and public relation exercises.
- To perform accounting and other record-keeping functions.
- To provide personnel and payroll administration services.
- To verify attendances should insurance issues arise.

Data Protection Principles

We shall perform our responsibilities under the Data Protection Acts in accordance with the following eight Data Protection principles:

Rule 1: Fair obtaining:

- Individuals are made aware of the uses for the information at the time of collection.
 - A tickbox is included on online & printed forms
- We will not disclose information to any third parties.

Rule 2: Purpose specification

- We clearly outline why data is held in our Data Protection Statement.
- The Trust Coordinator has responsibility for maintaining a list of all data sets and the purpose associated with each.

The data we currently hold is listed below;

Data	Contains	Where	Why
Current Membership Database	Name, Address, Email, Phone	Laptop, Cloud	Correspondence & accounting
Lapsed Membership Database	Name	Laptop, Cloud	Membership number continuity
BCV List	Name, Email	Laptop, Cloud	Correspondence & insurance
Past walk, talk, event attendees	Name, Email	Hard copy	Insurance
Past LLS attendees	Name, Address, Email, Phone	Laptop, Cloud	Correspondence
Local School Details	School, Address, Email	Laptop, Cloud	Correspondence
Past event contributors	Name, Email	Laptop, Cloud	Correspondence
CSR contacts	Name, Company, Email	Laptop, Cloud	Fundraising
Snapshot mailing list	Name, Email	Mailchimp	Correspondence & advertising
Images	Name, Image	Laptop, Cloud	Promotion
Media contacts	Name, Email	Laptop, Cloud	Correspondence
Staff details	Name, Address, Email	Laptop, Cloud	Correspondence

Rule 3: Use and disclosure of information

- Data should only be used for the uses set out above.
- All staff are aware of these rules.

Rule 4: Security

- Computers and databases are password protected.
- Encryption is not necessary.

Rule 5: Adequate, relevant and not excessive

- We collect all the information we need to serve our purpose effectively, and to deal with individuals in a fair and comprehensive manner.
- The information we collect is relevant, and not excessive, for our specified purpose.
- If an individual asked to view their records they can be provided within a reasonable timeframe.

Rule 6: Accurate and up-to-date

- We routinely check our data for accuracy. The data held is not generally time-sensitive.

Rule 7: Retention time

- We delete personal data as soon as the purpose for which we obtained the data has been completed.

Data	Time to be retained
Current Membership Database	Until membership lapses
Lapsed Membership Database	Name & Corresponding number held in case of re-joining
BCV List	Until 5 years of inactivity (Name will be retained for numbers)
Past walk, talk, event attendees	7 years for insurance purposes
Past LLS attendees	As long as necessary
Local School Details	As long as necessary
Past event contributors	As long as necessary
CSR contacts	As long as necessary
Snapshot mailing list	As long as necessary
Images	As long as necessary
Media contacts	As long as necessary
Staff details	4 years after ending employment

Rule 8: The Right of Access

- The Trust Coordinator is responsible for dealing with requests for access to data.
- An application can be submitted in writing, via email or by post with a request for the data required. This will be processed in a timely fashion.