Chelveston Wind Farm Community Benefit Fund

Data Protection Policy

The Chelveston Wind Farm Community Benefit Fund ('the Trust') recognises its responsibility to comply with the *General Data Protection Regulations 2018* which regulates the use of personal data. This does not have to be sensitive data; it can be as little as a name and address.

General Data Protection Regulations (GDPR)

The GDPR sets out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how personal information can be collected, handled and used. The GDPR applies to anyone holding personal information about people, electronically or on paper. The Trust has also notified the Information Commissioner that it holds personal data about individuals.

When dealing with personal data, Trustees and staff must ensure that:

- **Data is processed fairly, lawfully and in a transparent manner**
  This means that personal information should only be collected from individuals if staff have been open and honest about why they want the personal information.

- **Data is processed for specified purposes only**
  This means that data is collected for specific, explicit and legitimate purposes only.

- **Data is relevant to what it is needed for**
  Data will be monitored so that too much or too little is not kept; only data that is needed should be held.

- **Data is accurate and kept up to date and is not kept longer than it is needed**
  Personal data should be accurate, if it is not it should be corrected. Data no longer needed will be shredded or securely disposed of.

- **Data is processed in accordance with the rights of individuals**
  Individuals must be informed, upon request, of all the personal information held about them.

- **Data is kept securely**
  There should be protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Storing and accessing data

The Trust recognises its responsibility to be open with people when taking personal details from them. This means that the Trust must be honest about why they want a particular piece of personal information.

The Trust may hold personal information about individuals such as their names, addresses, email addresses and telephone numbers. These will be securely kept at the Trust Clerk's office and are not available for public access. All data stored on the Clerk's computers are password protected. Once data is not needed any more, is out of date or has served its use and falls outside the minimum retention time (see below), it will be shredded or securely deleted from the computer.

The Trust is aware that people have the right to access any personal information that is held about them. Subject Access Requests (SARs) must be submitted in writing (this can be done in hard copy, email or social media). If a person requests to see any data that is being held about them, the SAR response must detail:

- How and to what purpose personal data is processed
- The period the Trust intends to process it for
- Anyone who has access to the personal data

The response must be sent within 30 days and should be free of charge.

If a SAR includes personal data of other individuals, the Trust must not disclose the personal information of the other individual. That individual's personal information may either be redacted,

or the individual may be contacted to give permission for their information to be shared with the Subject.

Individuals have the right to have their data rectified if it is incorrect, the right to request erasure of the data, the right to request restriction of processing of the data and the right to object to data processing, although rules do apply to those requests.

Retention periods

Records are defined as all those documents which facilitate the activities carried out by Trust and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

A small percentage of the Trust records may be selected for permanent preservation as part of the Trust's archives and for historical research.

Responsibilities.

The Trust has a responsibility to maintain its records and record management systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Clerk. The person responsible for records management will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and timely.

Individual staff and Trustees must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with this policy.

Retention Schedule.

The retention schedule refers to record series regardless of the media in which they are stored.

Document	**Minimum Retention Period**	**Reason**
Minutes		
Minutes of Trust meetings	Indefinite	Archive
Finance		
Receipt and payment accounts	6 years	VAT
Bank statements	Last completed audit year	Audit
Cheque book stubs	Last completed audit year	Audit
Paid invoices and grants	Last completed audit year	VAT
Insurance		
Insurance policies	6 years after policy end	Management
General Management		
Trustee contact details	Duration of membership	Management
Email messages	At end of useful life	Management
Consent forms	5 years	Management

Confidentiality

The Trustees and staff must be aware that when complaints or queries are made, they must remain confidential unless the subject gives permission otherwise. When handling personal data, this must also remain confidential.

Adoption.

Version 1 of this policy was adopted by the Trust on 18th June 2018.

Signed: Signed

Chair of the Trustees Clerk to the Trustees

Date: Date: