Cronfa Gymunedol Fferm Wynt
PEN Y CYMOEDD
Wind Farm Community Fund CIC

Data Protection Policy

Scope of policy	Applies to all PyC CIC activities
Date Approved	22.5.18 V2 (V1 approved 17.2.17)
Review date	June 202

1. Introduction

1.1 Purpose of policy	This Policy ensures that Pen y Cymoedd Wind Farm Community Fund CIC collects and processes data: • lawfully, fairly and in a transparent manner in relation to individuals – obtaining their explicit consent for all personal data stored and used • for specified, explicit and legitimate purposes only • that is adequate, relevant and limited to what is necessary for CIC business activities • that is accurate and kept up to date • in a way that ensures appropriate security of the personal data, The CIC is registered with the Information Commissioner's Office (ICO) and provides training and support for staff who handle personal data, so that they can act confidently and consistently. This policy should be read in conjunction with the CIC's ICT Policy and Document Retention & Disposal Policy.
1.2 General Data Protection Regulation (GDPR)	The GDPR Europe-wide law replaced the Data Protection Act 1998 in the UK in May 2018. It sets out requirements for how organisations must collect, handle and store personal information, whether information is stored electronically or on paper or in any other form. The requirements apply to both PyC CIC as a Data Controller and to Data Processors with whom we have contracts.
1.3 Definitions	• **Personal Data**: all information relating directly or indirectly to an identifiable individual. This includes names; postal and email addresses; images; phone numbers; dates of birth, bank account, driving license and passport details. • **Data Controller**: the CIC Board. The Board determines why and how personal data are processed. • **Data Processor**: any person (other than a CIC employee) who processes personal data on the CIC's behalf. This would include, for example, the contractors who are undertaking Monitoring and Evaluation of the CIC, developing the CRM/Grants database, enabling Anti Money Laundering checks, ICT providers. • **Processing:** any operation performed on personal data. • **Personal Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
1.4 Data Protection Principles	Personal data must be: • Processed and stored fairly and lawfully. • Processed only for specified and lawful purposes. • Adequate, relevant and not excessive for those purposes. • Accurate and kept up to date - data subjects have the right to have inaccurate personal data corrected or destroyed if the personal information is inaccurate to any matter of fact. • Kept for no longer than is necessary for the purposes it is being processed. • Processed in line with the rights of individuals - this includes the right to be informed of all the information held about them, to prevent processing of their personal information for marketing

	purposes, and to compensation if they can prove they have been damaged by a Data Controller's non-compliance. • Secured against accidental loss, destruction or damage and against unauthorised or unlawful processing. • Not transferred to countries outside the European Economic Area - the EU plus Norway, Iceland and Liechtenstein - that do not have adequate protection for individuals' personal information.
2. Data Collection and Retention	
2.1 Data Flows	Details of the data types collected, why these are required and how long they are retained are listed at *Appendix 1*. The CIC collects no sensitive personal data[1].
2.2 Lawful Bases: Consent, Contract, Legitimate Interests	a. **CONSENT:** PyC CIC will process data only with full and explicit consent. • **Contact Database** People on our general mailing list have given their consent to receive general updates. We hold details of their names, job titles and organisations (if they represent an organisation), postal and email addresses and phone numbers. If anyone on the list wishes to stop hearing from us, they can do so at any time. • **New Contacts** When we meet potential applicants and interested parties they will be asked to complete a simple form giving consent before their details are added to the contact database. • **Grants and Loan Applicants** At the outset, applicants are required to read and confirm acceptance of the Privacy Statement at *Appendix 2* and the CIC's Data Protection Policy, before proposals are submitted. We will collect the same basic personal information. We may share some or all of the information with individuals and organisations we consult when assessing applications. These organisations may include those offering support and advice, local authorities and governing bodies. We ensure that they are fully compliant with data protection legislation. Applicants are advised that if they supply personal information relating to third parties (e.g. delivery partners) as part of their applications, they must ensure that they have consent. b. **CONTRACT:** processing necessary to the management of the award contract **c. LEGITIMATE INTERESTS**: the processing is necessary for PyC CIC, Vattenfall and the Welsh Ministers' legitimate interests.
2.3 Retention Period	We will keep details of both successful and unsuccessful applicants until 2041 - for the duration of the Fund. This is in line with the CIC's contract with our funder, the wind farm company Vattenfall, and Vattenfall's contract with Welsh Government Ministers.

[1] Sensitive personal data categories: 1. racial or ethnic origin 2. political opinions; 3. religious beliefs or beliefs of a similar nature; 4. Trades union membership; 5. physical or mental health; 6. sexuality; 7. commission or alleged commission of an offence; 8. Biometric and Genetic Data

3. Responsibilities	
3.1 Directors	Have overall responsibility for ensuring that the organisation complies with its legal obligations, supported by a Board Data Protection Champion.
3.2 Data Protection Officer	The Executive Director is the Data Protection Officer. Their responsibilities include: • Briefing the board on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising staff on Data Protection issues • Ensuring that Data Protection induction and training takes place • Ensuring registration with the ICO • Handling subject access requests • Approving unusual or controversial disclosures of personal data • Ensuring that all Data Processors are GDPR compliant before contracts are entered into • Approving all Data Protection statements attached to communications • Ensure marketing initiatives abide by data protection principles
3.3 Staff & Directors	All staff and Directors must read, understand and abide by all policies and procedures that relate to the personal data they may handle during their work.
3.4 Training	Staff and Board members will undertake Data Protection training every two years and will subscribe to ICO best practice updates.
4. Communication	
4.1 Communication with Data Subjects	Data Subjects will be informed about confidentiality via Data Protection statements on our application forms, so that they are as aware as possible about how we use the personal information we hold about them.
4.2 Authorisation for disclosures not directly related to the reason why data is held	These fall into two main categories: those likely to be at the instigation, or in the interests of the Data Subject, and those which are made during official investigations (e.g. by HMRC or the Police). For the first (such as a financial reference request from a bank), consent from the Data Subject is likely to be the normal authorisation. This consent should be recorded. For the second, it may be appropriate for the Data Subject not to be informed. Authorisation should be made by the CIC Chair.
5. Security and Storage	
5.1 Storage	• *Electronic*: data is held on password protected encrypted laptops and backed up on an external encrypted hard drive stored in a locked cupboard. We use Office 365 Cloud storage, which includes enhanced virus protection and Files Restore functionality which can be used to recover lost data due to accidental mass delete, ransomware, file corruption or anything else that might have damaged data. Microsoft also includes ransomware protection to OneDrive, and if cyber attackers are detected, Office 365 subscribers will be notified immediately. Emails are encrypted and protected. • *Grants Database* – our provider has ISO 27001 Information Security Standard accreditation and is fully compliant with data protection legislation • *Paper*: applications and supporting information are held in a filing cabinet in the CIC's office, both of which are locked when staff are away. The CIC uses a company with ISO 9001:2008 Quality Registration and BS EN 15713:2009 for secure destruction of confidential data and recycling services. We are provided with confirming Certificates of Destruction.
5.2 Data Processors	The Executive Director must evaluate any third-party services used by the CIC and obtain full written confirmation and assurance that they are GDPR compliant.

6. Subject Access	
6.1 Responsibility	Individuals have a right to know what information is being held about them. In response to a valid request the Executive Director will provide a permanent, clear copy of all the personal data about that data subject held at the time the request is made. Requests will be acted on without undue delay and at the latest within one month of receipt. No charge will be made.
6.2 Procedure for making request	Subject access requests can be made verbally, in writing or via social media. They do not have to be made to a specific person or contact point, and do not have to include the phrase 'subject access request' or Article 15 of the GDPR, as long as it is clear that the individual is asking for their own personal data. Anything which might be a subject access request will be acknowledged within 3 working days.
6.3 Procedure for granting access	Full details of all requests and responses made will be logged and recorded – including those made by telephone or in person. We will ensure that requests are clearly understood to help avoid later disputes about how they have been interpreted. We will encourage individuals to complete the PyC CIC Subject Access form but will make it clear that it this is not compulsory. The required information will be provided in either a hard copy or email or recording. If appropriate, supervised access in person will be permitted.
7. Personal Data Breach Reporting and Management	
7.1 Definition	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
7.2 Risk Areas	The main risk areas are: • breaches of confidentiality - information about individuals being disclosed through poor security or inappropriate disclosure of information • individuals or organisations being harmed through data being inaccurate or insufficient • data being held and used without explicit consent All these are mitigated by the measures set out above. Human error will always be a risk, and this will be minimised by having: - Regular training and updates - a clear and regularly reviewed and updated IT policy As PyC CIC electronic data is encrypted, and given the limited personal data held, the impact of any data breach is unlikely to be significant.
7.3 Responsibility	The CIC's Executive Director is responsible for all notifications about and management of data breaches. They will: - Assess the severity and potential impact of the breach - Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in any containment actions - Establish what can be done to recover any losses and limit damage - Where appropriate, inform the police. - Keep clear logs of all incidents and action taken
7.4 Action	If the breach is likely to adversely affect personal data or privacy, those affected will be notified promptly. They will be given: - the Executive Director's name and contact details - the estimated date of the breach - a summary of the incident - the nature and content of the personal data - the likely effect on the individual - any measures taken to address the breach; and - how they can mitigate any possible adverse impact.

8 Changes to this Policy

This policy will be reviewed annually. Any changes will be published clearly on our website and all those whose data we hold will be informed.

Appendix 1 – Data Collected

	Type	Data Held	Reason	Storage & Security	Comments
1.	Contact Database	• Applicant Name • Job Title • Organisation • Address (Home/Work) • Email address • Phone numbers	Programme and event updates	• Spreadsheet • CRM • One Drive • Back-up external encrypted hard drive	In April 2018 all database contacts were asked to confirm their willingness to remain and receive updates and news from the CIC and the database was updated accordingly. All responses were recorded and saved. Contacts will be asked again every two years to confirm their willingness to remain on the mailing list. All general emails issued by the CIC contain an 'unsubscribe' option.
2.	Grant & Loan Applicants	• Name • Job Title • Organisation • Address (Home/Work) • Email address • Phone numbers	Grant assessment	• Spreadsheet • CRM • Locked filing cabinet • One Drive • Back-up external encrypted hard drive	Details of both successful and unsuccessful applicants will be kept for the duration of the Fund / CIC in tandem with the CIC's contract with Vattenfall and Vattenfall's contract with the Welsh Ministers. Applicants are made aware of and explicitly assent to the CIC's Data Protection Policy Statement before they access the CRM application portal, or when they submit a paper application.
3.	Grantees	As 2 above – also: - DoB for main contact - Organisation / business bank account details - Photographs / films	- AML checks - Grant contract management - Grant payments *Data required for identity verification checks in relation to the grant / loan contract – no credit checks are undertaken. Data is destroyed once a verification check has taken place.* Project reporting and monitoring.	• Spreadsheet • CRM • Locked filing cabinet • One Drive • Back-up external encrypted hard drive	Details of successful applicants will be kept for the duration of the Fund / CIC in tandem with the CIC's contract with Vattenfall and Vattenfall's contract with the Welsh Ministers. Model consent forms required.

Appendix 2 – Privacy Statement

Data Protection Policy

It's very important that you read and accept our Data Protection Policy and the Privacy Statement below before you start the grant registration process. By continuing, you are confirming your acceptance of the Policy and the ways in which we will use the information you give us. You can read the whole policy **here.** If you have any queries at all about it, please give us a call.

Thank you.

Privacy Statement

In order to keep in touch with people and to assess grant proposals and make funding awards, Pen y Cymoedd CIC needs to collect information – not only about the activities and projects themselves, but also about the individuals submitting grant applications. Our Policy sets out how we will use that personal information. It aims to be open, fair and transparent, and to meet the requirements of the General Data Protection Regulation (2016/679).

We will collect information about you when you:

- sign up to our Contact Database to receive updates on our activities and programmes.
- apply for a grant or loan

If any information you've given us changes at any time, please tell us and we'll amend our records.

1. Contact Database

People on our general mailing list have given their consent to receive general updates. We hold details of their names, job titles and organisations (if they represent an organisation), postal and email addresses and phone numbers. If anyone on the list wishes to stop hearing from us, they can do so at any time.

2. Grants and Loan Applicants

We will collect the same basic personal information. We may share some or all of the information you give us with individuals and organisations we consult when assessing applications. These organisations may include those offering support and advice, local authorities and governing bodies. We ensure that they are fully compliant with data protection legislation.

If you supply personal information relating to third parties (e.g. delivery partners) as part of your application, you must make sure that you have their consent.

3. When a Grant or Loan is Awarded

- *Verification checks:* in order to verify that lead applicants are who they say they are, we ask for dates of birth. In exceptional circumstances, we may also need driving license numbers and dates of issue, and/or passport numbers and full registered names. This information will be destroyed once the checks have been carried out. Again, we ensure that the organisations we use to help us carry out these checks are fully compliant with data protection legislation.

  If you provide false or inaccurate information in your application or at any point in the life of any funding we award to you and fraud is identified, we will provide details to fraud prevention agencies, to prevent fraud and money laundering.

- *Bank Accounts:* we will also need details of group, business or individual bank accounts for grant or loan payment purposes.

- *Monitoring & Evaluation:* we are likely to share some or all of the information you give us with individuals and organisations we work with to administer and monitor the outcomes and impacts of the Community Fund. Again, we ensure that these organisations are fully compliant with data protection legislation.

4. How we store and protect your information

- *Electronic*: we hold data on password protected encrypted laptops, and back these up on an external encrypted hard drive stored in a locked cupboard. We use Office 365 Cloud storage, which notifies subscribers immediately if cyber attackers are detected. Emails are encrypted and protected
- *Grants Database* – our provider has ISO 27001 Information Security Standard accreditation and is fully compliant with data protection legislation
- *Paper copies*: applications and supporting information are held in a filing cabinet in the CIC's office, both of which are locked when staff are away.

5. How long your information is kept

We will keep details of both successful and unsuccessful applicants until 2041 - for the duration of the Fund. This is in line with the CIC's contract with our funder, the wind farm company Vattenfall, and Vattenfall's contract with Welsh Government Ministers.

6. Changes to this Policy

This policy will be reviewed annually. Any changes will be published clearly on our website and we will contact you directly to let you know about them.

If you have any questions at all about your privacy or this Policy, please contact us:
enquiries@penycymoeddcic.cymru / 01685 878785