Conwy Mind

GDPR Policy

Date Created:

Date approved:

Date of Review:

Introduction

This policy provides information about the data protection legislation, including the General Data Protection Regulation ("GDPR") and Data Protection Act 2018 with which Conwy Mind ("we", "our", "us") must comply.

1. People involved

This policy applies to all members of staff, trustees, volunteers and others who do work for us. This policy provides a general overview of the legal requirements. It sets out what we expect from you in general terms when handling personal information, regardless of the format in which it is stored. This includes information about:

- Current or former employees and workers and applicants
- Current or former volunteers and applicants
- Current or former trustees and applicants
- Beneficiaries / clients / users of our services
- Users of our on-line and digital media channels
- Current, former or potential supporters, donors and funders including individuals and representatives of organisations
- People with whom we engage in relation to our campaigning activity
- Representatives of organisations with whom we have partnerships or we are collaborating
- Representatives of our suppliers

You must read, understand and comply with this Policy when handling personal data on our behalf and attend any compulsory training on its requirements. The policy may be supplemented by specific guidance relevant to your role. Your compliance with this Policy is mandatory. Any breach of this Policy may result in disciplinary action.

2. Definitions

The following definitions are used in this policy:

Controller means the person or organisation that determines when, why and how to process Personal Data. We are the Data Controller of all Personal Data used in our organisation for our own purposes. Data Subject means a living, identified or identifiable individual about whom we hold Personal Data. The Data Controller is delegated to the CEO

Data Privacy Impact Assessment (DPIA) means a tools and assessment used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data

Data Protection Officer (DPO)] or Data Protection Lead (DPL means the person with responsibility for data protection compliance within our organisation. The current person is The CEO and Services Manager Community Hub

Personal Data means any information identifying a Data Subject or information relating to a Data Subject from which we can identify (directly or indirectly) a Data Subject whether from that data alone or in combination with other identifiers we possess or can reasonably access.

Personal Data includes Special category Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour

Personal Data Breach means any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach

Privacy by Design means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the data protection legislation

Privacy Notice means a notice setting out information that should be provided to Data Subjects when we collect information about them

Processing or Process means any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Processors means any third parties who we use to Process Personal Data on our behalf

Pseudonymisation or Pseudonymised means replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Special Category Personal Data means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and information relating to criminal offences and convictions.

3. Data Protection Principles

The law requires that Personal Data must be:

• processed lawfully, fairly and in a transparent manner

• collected only for specified, explicit and legitimate purposes

• Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

• Accurate and where necessary kept up to date

• Not kept in a form which permits identification of Data Subjects

• For no longer than is necessary for the purposes for which the data is processed

• processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage

Personal Data must also not be transferred to outside the EEA country without appropriate safeguards being in place. We are required to enable Data Subjects to exercise certain rights in relation to their Personal Data.

We must also comply with particular legal requirements when suppliers that carry out services for us have access to Personal Data and when we are working with organisations and need to share Personal Data.

We are responsible for and must be able to demonstrate compliance with the requirements under the law.

4. Lawfulness and Fairness

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The law restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The lawful bases available when processing non-special category personal data are:

• The Data Subject has given consent to the processing of his or her personal data for one or more specific purposes

• The processing is necessary for the performance of a contract between us and the Data Subject or in order to take steps at the request of the Data Subject prior to entering into a contract

• The processing is necessary for compliance with a legal obligation to which we are subject

• The processing is necessary in order to protect the vital interests of the Data Subject or of another natural person

• The processing is necessary for the performance of a task carried out in the public interest

• The processing is necessary for the purposes of legitimate interests we are pursuing or which a third party is pursuing, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the Data Subject is a child. A range of additional legal requirements apply when processing Special Category Personal Data. Please see the definitions section for the types of information this includes. If your role involves you being required to process Special Category Personal Data, you will receive additional guidance on this.

5. Transparency

The law requires us to provide detailed, specific information about our use of Personal Data to Data Subjects. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them. Whenever we collect Personal Data directly from Data Subjects, we must provide the Data Subject with information including who we are and how and why we will Process, disclose, protect and retain their Personal Data. This is done through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data. When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with the Privacy Notice information as soon as possible after collecting/receiving the data. We must also check that the Personal Data was collected by the third party in accordance with law and on a legal basis which complements our proposed Processing of that Personal Data.

6. Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and there is a legal basis for doing so.

7. Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. You may only collect Personal Data that you require for your duties: you should not collect excessive data. You should ensure any Personal Data collected is adequate and relevant for the intended purposes.

8. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. You should ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You should check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to amend inaccurate or out-of-date Personal Data.

9. Retention

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. We will maintain retention policies and procedures to ensure Personal Data is deleted securely in accordance with this requirement.

10. Security

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. You are responsible for protecting the Personal Data we hold. You may only Process Personal Data when required to do so as part of your role. You cannot Process Personal Data for any reason unrelated to your role. You must ensure that you follow all guidelines issued to you that are designed to protect against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care to protecting Special Category Personal Data from loss and unauthorised access, use or disclosure.

11. Reporting a Data Breach

The law requires Data Controllers to notify any Personal Data Breach to the Information Commissioner's Office (ICO) and, in certain instances, the Data Subject. If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. You should immediately contact the [DPO/DPL]. You should preserve all evidence relating to the potential Personal Data Breach and provide assurance to the [DPO/DPL] as required.

12. Transfer Limitation

The law restricts data transfers to countries outside the European Economic Area (EEA) where they do not have adequate data protection laws. If you need to send Personal Data outside the EEA, you should contact the [DPO/DPL] for advice.

13. Data Subject Rights

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

• Where Processing is based on the legal basis of consent, to withdraw Consent to Processing at any time;

• receive certain information about our Processing activities;

• Request access to their Personal Data that we hold;

• prevent our use of their Personal Data for direct marketing purposes;

• ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

• restrict Processing in specific circumstances;

• challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

• be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms; and

• in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

You must immediately forward any Data Subject request you receive to the [DPO/DPL].

14. Sharing Data

You may only transfer Personal Data to third-party service providers who agree to comply with our policies and procedures and who agree to put adequate security measures in place, as requested. We must have a written contract in place with any such service providers we are using. This contract must contain specific information in line with GDPR requirements and you should liaise with the [DPO/DPL] on this.

In addition, although it is not a legal requirement, it is good practice to agree data sharing arrangements in writing with any partners with which we are working where the relationship involves sharing Personal Data. It is essential that you have a clear legal basis for sharing Personal Data with such partners or any third parties and that you transmit the Personal Data securely.

15. Accountability and Demonstrating Compliance

The law requires us to keep full and accurate records of all our Processing activities. You should ensure that any Processing of Personal Data that you undertake is included in the records by checking with the [DPO/DPL].

We are required to ensure all people who work for us have undergone adequate training to enable them to comply with data privacy laws.

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

We must also conduct DPIAs in respect to high risk Processing. If you believe Processing that you are carrying out is high risk, please speak to the [DPO/DPL]. We must also regularly test our systems and processes to assess compliance. You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data. You should provide any information to the [DPO/DPL] as required.

Document information

Policy author:	Jacky Baldini	Trustee
Version and status:	V1.0	
Date of Creation:	June 2019	
Date of Authorisation:	July 2019	
Published / Review date:	July 2021	

Change Log

Version	Approved By	Changes