THE LLANDYRNOG COMMUNITY SHOP LIMITED

(Hereafter 'the Business')

Data Protection Policy

1. Definitions

1.1. **GDPR** – the General Data Protection Regulation

1.2. **Responsible Person** – the person responsible for data protection within the Business

1.3. **Register of Systems** – a register of all systems or contexts in which the Business processes personal data

2. Data Protection Principles

2.1. The Business is committed to processing data in accordance with its responsibilities under the GDPR.

2.2. Under Article 5 of the GDPR, the Business will ensure that personal data is:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, or statistical purposes is not considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. General Provisions

3.1. This policy applies to all personal data processed by the Business.

3.2. The Responsible Person will take responsibility for the Business's ongoing compliance with this policy.

3.3. This policy will be reviewed at least annually.

3.4. The Business will register with the Information Commissioner's Office as an organisation that processes personal data.

4. Lawful, Fair and Transparent Processing

4.1. To ensure that its processing of data is lawful, fair and transparent, the Business will maintain a Register of Systems.

4.2. The Register of Systems will be reviewed at least annually.

4.3. Individuals have the right to access their personal data and any such requests made to the Business will be dealt with promptly.

5. Lawful Purposes

5.1. All data processed by the Business must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO website for more information).

5.2. The Business will note the appropriate lawful basis in the Register of Systems.

5.3. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent will be kept with the personal data.

5.4. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent must be clearly available and systems must be in place to ensure such revocation is reflected accurately in the Business's systems.

6. Archiving/Removal

6.1. To ensure that personal data is kept for no longer than necessary, the Business will put in place an archiving policy for each area in which personal data is processed and will review this process annually.

6.2. The archiving policy will consider what data should/must be retained, for how long and why.

7. Security

7.1. The Business will ensure that personal data is stored securely using modern software that is kept up to date.

7.2. Access to personal data will be limited to personnel who need access and appropriate security must be in place to avoid unauthorised sharing of information.

7.3. When personal data is deleted this must be done safely, such that the data is irrecoverable.

7.4. Appropriate back-up and disaster recovery solutions must be in place.

8. Breach

8.1. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, the Business will promptly assess the risk to people's rights and freedoms and, if appropriate, report this breach to the ICO (see ICO website for more information).