Pumphouse Community Brewery Limited

Data Protection Policy

- **First produced:** **May 2018**
- **This version approved by Board:** **May 2018**
- **To be reviewed no later than:** **May 2019.**

Introduction

Pumphouse Community Brewery Limited (PHCB) is a society registered under the Co-operative and Community Benefit Societies Act 2014 and owned by its members, the majority of whom are residents of the village of Toppesfield. PHCB operates from the Green Man Barn in Toppesfield. PHCB is a socially responsible business committed to commercial success whilst upholding the highest standards with regards to business operations and practices. This policy forms part of those standards of good practice. PHCB collects and administers a range of personal information for the purposes of:

- employing staff;
- maintaining our register of members;
- dealing with customers; and
- marketing and publicity.

PHCB is committed to protecting the privacy of the personal information it collects, holds and administers.

2. General Policy Statement

We are fully committed to comply with the requirements of the General Data Protection Regulations ('GDPR') 2018 (the 'Act'). As a not-for-profit organisation, we are not obliged to register with the Information Commissioner's Office, but we aim to adhere to the principles which are the foundation of the Act, namely that all data which is covered by the Act (which includes not only computer data but also personal data held within a filing system) is:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than is necessary;
- processed in accordance with the data subject's rights;
- secure;
- not transferred to countries without adequate protection;
- where applicable, held with the consent of and for purposes authorised by the individual.

PHCB has adopted the following principles contained as minimum standards in relation to handling personal information. PHCB will:

• Collect only information which the organisation requires for its primary functions;

• Ensure that stakeholders are informed as to why we collect the information and how we administer the information gathered;

• Use and disclose personal information only for

- our primary functions;
- directly related purpose;
- for another purpose with the person's consent; or
- as required by law.

• Store personal information securely, protecting it from unauthorised access; and

• Provide stakeholders with access to their own information, and the right to seek its correction.

3. Data Protection Policy

3.1. Responsibilities

The Company Secretary is responsible for:

• ensuring that PHCB adheres to the GDPR and meets the requirements of the Information Commissioner's Office

• PHCB maintains this policy by for monitoring changes in Privacy legislation, and for advising on the need to review or revise this policy as and when the need arises.

At PHCB we hold sensitive and valuable personal information which must be kept safe, failing which there could be serious repercussions for PHCB. Our policy is to protect the information we hold from all threats, whether internal, external, deliberate or accidental.

It is our policy to ensure that:

• information is protected against unauthorised access;

• information is kept confidential;

• the integrity of information we hold is maintained;

• regulatory and legislative requirements are met;

• anyl breach of information security, actual or suspected is reported and investigated; and

• business and individual requirements for the availability of information and information systems are met.

We maintain the security and confidentiality of the information we hold as well as our information systems and applications by:

• ensuring that all involved with the operations are aware of the information security policies and procedures applicable in theiractivities and fully understand their own responsibilities;

• creating and maintaining within PHCB a level of awareness of the need for information security and data management as an integral part of our day to day business;

• having in place up to date contingency and recovery plans;

• having in place measures to ensure data is secured against loss and unauthorised access;

3.2 Use and Disclosure

PHCB will:

• Only use or disclose information for the primary purpose for which it was collected or a directly related secondary purpose

• For other uses, unless disclosure is required by law, we will obtain consent from the affected person.

3.3 Data Quality

PHCB will:

• Take reasonable steps to ensure the information the organisation collects is accurate, complete, up to date, and relevant to the functions we perform.

3.4 Data Security and Retention

PHCB will:

• Safeguard the information we collect and store against misuse, loss, unauthorised access and modification.

3.5 Openness

PHCB will:

• Ensure stakeholders, including employees, are aware of our Data Protection Policy and its purposes.

• Make this information freely available in relevant publications and on the organisation's website.

3.6 Access and Correction

PHCB will:

• Ensure individuals have a right to seek access to information held about them and to correct it if it is inaccurate, incomplete, misleading or not up to date.

• Individuals who wish personal data to be removed & deleted from PHCB records have the right to do so.

3.7 Anonymity

PHCB will:

• Give stakeholders the option of not identifying themselves when completing evaluation forms or opinion surveys.

3.8 Making information available to other organisations

PHCB:

• Will only release personal information about a person with that person's express permission, unless required by law. For personal information to be released, the person concerned must send permission in writing.

• Will not release information to third parties where it is requested UNLESS required by law to do so.

3.9 Information Assets

We annually assess our assets to ensure that appropriate procedures are in place to mitigate the risks. This process is the responsibility of the Management Committee . The register below lists the society's key information assets and identifies the risks to these assets, their likelihood and impact and how we ensure they are protected

Asset	Risk	Likelihood	Impact	Security Measures
Business plan	Low	Low	High	On Google Drive
Business Continuity Plan	Low	Low	High	All information kept in Google Drive and restricted to Directors and Secretary
Financial information	Medium	Medium	High	All information kept in xero accounting package with access to Directors and Secretary
Accounts information	Medium	Medium	High	Maintained on Xero and in the office. Access only Directors and Secretary Copies of accounts held by external accountants.
Staff records	Medium	Medium	High	All information kept online secure server
Complaints information & on	Low	Low	High	Complaints information kept locked in office Google Drive . Access restricted to Directors.
Money laundering	Low	Low	High	All information kept in Google Drive and restricted to Directors/Secretary
Shareholder details	Medium	Medium	High	Records are stored digitally on Google drive
Board minutes and papers	Medium	Medium	High	These documents are kept kept & backed up on Google Drive

3.10 Access controls

Google Drive:

the administrator is a nominated Director. S/he is responsible for creating access to the Directors documents.

Xero:

the administrator is a nominated DirectorRequests for new accounts or requests by existing users for amendments or adjustments to access rights must be made to the Company Secretary.

Employees' user rights generally cease upon termination of their employment contract.

User accounts shall only be used by the person (or persons) it was issued to.

Each user is responsible for the appropriate use of their accounts.