

The Hull Community Pub Society Limited (the Society)

DATA PROTECTION POLICY

1. Purpose and Scope

1.1 This policy outlines how the Society will comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 in handling personal data of members, employees, customers, and other stakeholders.

1.2 The policy applies to all Directors, employees, and volunteers who process personal data on behalf of the Society.

2. Definitions

2.1 **Personal Data:** Data about a living individual who can be identified from those data (or from those and other information either in our possession or likely to come into our possession).

2.2 **Usage Data:** Data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (e.g., the duration of a page visit).

2.3 **Cookies:** Small pieces of data stored on a user's device.

2.4 **Data Controller:** A person or entity that determines the purposes for which and the manner in which any personal data are, or are to be, processed. The Society is a Data Controller.

2.5 **Data Processor (or Service Provider):** Any person (other than an employee of the Data Controller) who processes data on behalf of the Data Controller. The Society may use third-party service providers to process data.

2.6 **Data Subject:** Any living individual who is the subject of Personal Data.

2.7 **User:** The individual using the Society's services. The User corresponds to the Data Subject, who is the subject of Personal Data.

3. Data Collection and Processing

3.1 The Society collects personal data for:

- Membership administration
- Financial transactions
- Staff and volunteer management
- Customer engagement and marketing (with consent)

3.2 The Society ensures that personal data is:

- Collected for specified, explicit, and legitimate purposes
- Kept up-to-date and accurate
- Processed securely

4. Information Collection and Use

4.1 Types of Data Collected:

- **Personal Data:** Email address, first name, last name, address, cookies, and usage data.
- **Usage Data:** Includes IP address, browser type, pages visited, time spent on pages, and diagnostic data.

4.2 The Society may use personal data to:

- Provide and maintain services
- Notify users of changes
- Allow participation in interactive features
- Provide customer support
- Improve service offerings
- Detect and prevent fraud or technical issues
- Send marketing communications (with opt-out options)

5. Data Security and Retention

5.1 Personal data is securely stored and protected against unauthorized access, alteration, or disclosure.

5.2 Data is retained only for as long as necessary, with regular reviews to ensure outdated data is securely deleted.

5.3 Usage data is generally retained for shorter periods unless required for security, legal, or analytical purposes.

6. Data Transfers

6.1 Personal data may be transferred and maintained on computers located outside of the UK where data protection laws may differ. By providing data, users consent to such transfers.

6.2 The Society will ensure appropriate safeguards are in place to protect data during transfers.

7. Disclosure of Data

7.1 The Society may disclose personal data if required to do so by law or in response to valid legal requests by public authorities (e.g., courts or government agencies).

7.2 Personal data may be disclosed to:

- Protect and defend the rights of the Society
- Prevent or investigate possible wrongdoing
- Protect the personal safety of users or the public

8. Individual Rights

8.1 Individuals have the right to:

- Access their personal data
- Request correction or deletion
- Withdraw consent for data processing
- Object to processing

8.2 Requests must be submitted in writing to the Society's Data Protection Officer.

9. Cookies and Tracking

9.1 The Society uses cookies and tracking technologies to monitor service usage and improve user experience.

9.2 Users can refuse cookies by adjusting their browser settings, though some features may be impacted.

10. Data Breaches

10.1 Any suspected data breach must be reported to the Data Protection Officer immediately. The Society will assess the breach and, where necessary, report it to the ICO within 72 hours.