Towcester Community Fridge Privacy Policy

Approved By: Committee
Status: Approved – 09/02/2026
Next Review Date: [set later]

Purpose:
To ensure that all personal data of volunteers is collected, stored, and processed in compliance with GDPR and internal data protection standards.

Scope:
Applies to all volunteers, committee members, and staff handling volunteer personal data.

Data Controller:
Towcester Community Fridge is the data controller for all volunteer personal data collected and processed under this policy.

Policy Principles:

Data Minimisation:
Only collect personal data necessary for the volunteer role.

Consent:
Volunteers must consent to their data being collected, stored, and processed.

Storage & Security:
Personal data is stored securely (locked cabinet or encrypted digital file). Only authorised officers may access it.

Retention:
Volunteer records and all personal data held by the organisation are kept for the duration of their involvement plus up to 6 years after they leave, to meet legal, safety, and insurance requirements. Records of volunteers who leave are deleted unless retention is required for legal, safeguarding, insurance, or regulatory purposes, in which case the data will be retained only for the minimum period necessary.

Access/Rights:
Volunteers may request access, correction, or deletion of their personal data at any time. Requests must be made in writing (email is acceptable) to the Chair or Administrator using the organisations official contact details

Requests will be responded to without undue delay and within the timeframes required by data protection legislation.

Sharing:
Personal data will not be shared with third parties without consent, except for statutory obligations (e.g., DBS checks, insurance).

Lawful Basis:
The lawful basis for processing volunteer personal data is consent, and where applicable, legitimate interest in order to manage volunteering activities safely and effectively.

Procedure

- Volunteer personal data is collected **only as part of the volunteer onboarding process**.
- Data may be collected **in person at a session** or **electronically (e.g. via email or form)** where appropriate.
- All data collection must use the **approved volunteer data collection form** and include a privacy statement referencing this policy.
- Paper forms must be stored securely in the designated locked safe immediately after collection.
- Electronic records must be stored securely with access limited to authorised persons only.
- Data is stored and retained in line with the retention schedule set out in this policy.
- Any actual or suspected data breaches must be reported to the Chair immediately and assessed promptly in line with GDPR requirements.
- An annual review of data held and retention periods will be carried out by the Committee.
- When a volunteer requests deletion of their personal data, the responsible person must delete it without undue delay in line with GDPR and **confirm in writing to the individual once deletion has been completed**. Where data cannot be deleted due to legal or regulatory requirements, this will be explained to the individual in writing.

Responsibilities:

Session Lead / Duty Lead

- Responsible for collecting volunteer personal data during sessions.

- Responsible for ensuring all paper records are stored securely in the designated locked safe immediately after each session.
- Responsible for handling volunteer data in accordance with this policy.

Committee / Chair

- Responsible for ensuring appropriate systems, roles, and controls are in place to comply with data protection legislation.
- Responsible for overseeing compliance with this policy and addressing any breaches or concerns.

Administrator

- Responsible for drafting and maintaining data protection documentation and policies.
- Responsible for supporting compliance and responding to data protection queries.
- Not responsible for the physical storage, access to, or security of paper records held on site.

All Authorised Persons

- Any individual granted access to volunteer personal data is responsible for complying with this policy and GDPR principles.

Committee: Ensure policy is followed and reviewed annually.