



Blue Flamingo Community Hub CIC

GDPR & Data Protection Policy

Policy Owner: Blue Flamingo Community Hub CIC

Date policy approved: 10.02.2026

Introduction

Blue Flamingo Community Hub CIC is committed to protecting the privacy and rights of our members, volunteers, and staff. Data we collect is held in compliance with the UK General Data Protection Regulation (UK GDPR).

The Six Principles of Data Protection

We ensure that all personal data is:

1. **Lawful, fair, and transparent:** We tell people why we need their data.
2. **Purpose-limited:** We only use data for the reason it was collected (e.g., emergency contacts).
3. **Data minimisation:** We only ask for what we actually need.
4. **Accuracy:** We keep records up to date.
5. **Storage limitation:** We don't keep data longer than necessary.
6. **Integrity and confidentiality:** We keep data secure.

How We Use Member Data

We collect data primarily to ensure the safety and wellbeing of our members. This includes:

- Emergency contact details.
- Dietary requirements.
- Consent for photography and social media.
- Email addresses to keep members informed of news and events. Every year, we send out an email asking individuals if they would like us to remove them from our list. Anyone can ask at any time for their information to be deleted from mailing list which will be completed immediately.
- Phone numbers and home addresses are collected from members, volunteers and staff. We collect this information to send occasional correspondence, such as condolence cards, or to perform a welfare

check if we are concerned about an individual's wellbeing (e.g., if an individual has been absent for over 2 months without notice and we haven't been able to reach them by any other means and this is unusual for them).

- Mobile phone numbers are collected when a person requests to be added to our closed WhatsApp groups.
- We keep an attendance record for each session. We use this information to collect data on the number of service users access our services which we then use to apply for grants, create impact reports and for grant monitoring purposes. This information is only accessible by the ED and SCs. This information is saved as a Google sheet which is password protected. We will retain this information for up to seven years for reference purposes, after which time it is deleted.

Volunteer Responsibilities

- **Confidentiality:** Never discuss member details (names, health status, or personal stories) outside of the Hub.
- **No Personal Storage:** Volunteers must not store member phone numbers or addresses on their personal devices without explicit authorisation from the ED.
- **Paper Records:** New Member Forms are collected by the ED. Whilst on-site, these forms must be kept in a locked Hub folder and never left unattended on tables. The ED will be the only authorised person to hold a key for the locked folder; in her absence they key will temporarily be given to another member of staff or designated lead volunteer.
- **Digital Security:** Data from paper forms is transferred promptly to the official Blue Flamingo Gmail account. This account is password-

protected and access exclusively by the ED. Once data is securely digitized, paper copies containing sensitive data are shredded.

Data Breaches

A breach occurs if personal data is lost, stolen, or shared with the wrong person (e.g., sending a member list to the wrong email).

- **Action:** Any potential breach must be reported to the **Executive Director immediately**.
- **Reporting:** We are legally required to report significant breaches to the ICO within 72 hours.

Right to Access (Subject Access Requests)

Anyone we hold data on has the right to see that data. If a member or volunteer asks to see their records, please refer them to the Executive Director immediately.