

## 1. Data Protection Policy

**For *BROMSGROVE MINIBUS APPEAL FUND CHARITY, No 516666***

### **Purpose**

This policy sets out how the charity complies with the UK GDPR and Data Protection Act 2018 when collecting and using personal data relating to passengers, volunteers, staff, and supporters.

### **Scope**

Applies to all trustees, volunteers, drivers, administrators, and anyone handling personal data on behalf of the charity.

### **Principles**

The charity commits to the six GDPR principles:

- **Lawfulness, fairness, transparency**
- **Purpose limitation**
- **Data minimisation**
- **Accuracy**
- **Storage limitation**
- **Integrity and confidentiality**

### **Roles & Responsibilities**

- **Trustees:** overall accountability
- **Data Protection Lead:** GEOFFREY KEARN BOOKINGS MANAGER AND TRUSTEE
- **Volunteer Drivers:** follow procedures and report concerns

### **Types of Data Processed**

- Names, E mail addresses, phone numbers of Group Contact and Invoice Payment representative.
- No Mobility/health information is required or collected by the Charity.
- Emergency contact will be the Group's contact responsible for booking the Minibus as detailed in the booking request.
- Volunteer drivers contact details are contained on a File of Understanding which is signed by the Driver when he/she commences voluntary service with the Charity. As the Drivers have no direct responsibility for the passengers DBS checks are not required.

- CCTV footage. The Minibus is not fitted with CCTV therefore there is no requirement under this category.

### **Lawful Bases**

- Legitimate interests.
- Contract (transport bookings). A Contract is formed between the Charity and the Group via the online booking form.
- Legal obligation (DBS, safeguarding). There are no DBS nor safeguarding requirements as the Drivers responsibility is to safely drive the Minibus, They have no responsibility for the well-being of the passengers.
- Explicit consent (health/mobility data). No health/mobility information nor consent is required by the Charity for the passengers.

### **Security Measures**

- Password-protected devices. Administrators have full access and control of the booking information via the Admin Portal of the Charity's website. Drivers have read only access for emergency purposes only.
- Locked storage for paper records. Paper records including List of Invoice controllers for the Customer held by the Treasurer/Trustee and completed copies of the File of Understanding held by the Bookings Manager /Trustee are held in locked storage at the homes of the respective Trustees.
- Restricted access to health data. No health data is asked for nor retained.
- Encrypted CCTV. CCTV is not used on the Minibus.

### **Data Subject Rights**

The charity will respond to requests within one month, including: access, rectification, erasure, restriction, objection, and portability.

### **Data Breaches**

All breaches must be reported immediately to the Data Protection Lead. Serious breaches may be reported to the ICO within 72 hours.

## **2. Passenger Privacy Notice**

***For passengers using the Bromsgrove Minibus Appeal Fund minibus service***

### **What information we collect**

- Name, email address, phone number of the Group's Contact and Group's Invoice representative.

- Mobility needs (e.g., wheelchair use, assistance required). The Charity collects no data with regards to the passenger's health and mobility.
- Emergency contact details. This is the Group Contact person whose name and personal details are provided via the website booking form.
- Pickup/drop-off locations. These are stated on the online booking form completed by the Group's Contact at the point of booking the Minibus.
- Payment information. This is issued by the Charity's Treasurer to the Group's Invoice representative, via an emailed Invoice. All payment methods, due dates and Charity's Bank Account details are given on the Invoice.

### **Why we collect it**

- To provide safe and accessible transport
- To contact you about bookings
- To ensure your safety in an emergency
- To meet legal obligations

### **Lawful basis**

- Legitimate interests (transport service)

### **Who we share data with**

- The Charity's website Administrators have full access to the booking data provided by the Group and have the authority to amend it as required or instructed. Authorised volunteer drivers, whose access is on a read only basis, have access to the booking form details on the Charity's website
- Emergency services if required
- Data is never sold or shared for marketing or with any third party.

### **How long we keep data**

See retention schedule below.

### **Your rights**

You may request access, correction, deletion, or restriction of your data.

### **Contact**

Data Protection Lead:

GEOFFREY KEARN

Email: [geoffkearn@hotmail.co.uk](mailto:geoffkearn@hotmail.co.uk)

Phone: 07805 400180

### **3. Volunteer Driver Privacy Notice**

#### **Data we collect**

- Name, address, phone, email
- Driving licence details
- Emergency contact
- Incident reports (if involved)

#### **Why we collect it**

- To manage volunteering
- To meet legal obligations
- To ensure safe operation of the minibus

#### **Lawful basis)**

- Contract (volunteer agreement)
- Legitimate interests (service delivery)

#### **How long we keep it**

See retention schedule.

#### **Your rights**

You may request access, correction, deletion, or restriction of your data.

#### 4. Data Retention Schedule

Data Type	Retention Period	Reason
Group booking records	12–24 months	Service administration
Emergency contact details	12 months after last journey	Safety
Volunteer driver records	Duration of service + 6 years	Legal defence
Incident/accident reports	3–6 years	Insurance/legal
Financial records	6 years	HMRC

#### 5. Data Breach Response Plan

##### Definition

A breach is any loss, access, disclosure, or alteration of personal data.

##### Immediate Actions

1. Notify the Data Protection Lead immediately.
2. Contain the breach (recover data, secure accounts, retrieve documents).
3. Assess risk to individuals.
4. Record the breach in the breach log.

##### Reporting to ICO

If the breach risks harm to individuals, the ICO must be notified within **72 hours**.

##### Notifying Individuals

If the breach is high-risk (e.g., health data exposed), affected individuals must be informed.

##### Review

Trustees must review the breach and update procedures.

## 6. Record of Processing Activities (ROPA)

*Required under Article 30 UK GDPR*

<b>Processing Activity</b>	<b>Data Collected</b>	<b>Purpose</b>	<b>Lawful Basis</b>	<b>Retention</b>	<b>Security</b>
<b>Group bookings</b>	Name, contact, email address	Transport service	Legitimate interests, consent	12–24 months	Password protection, locked storage
<b>Volunteer management</b>	Contact details,	Safeguarding, operations	Legal obligation, contract	Service + 6 years	Restricted access
<b>Incident reporting</b>	Names, details,	Legal compliance	Legal obligation	3–6 years	Locked storage