

# GDPR Policy

## Introduction

Rock School Bus CIC needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

## Why this policy exists

This data protection policy ensures Rock School Bus CIC:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

## Data protection law

The Data Protection Act 1998 describes how organisations — including [company name]— must collect, handle and store personal information.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways

## People, Risks and Responsibilities

This policy applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- ...plus any other information relating to individuals

## Data protection risks

This policy helps to protect Rock School Bus CIC from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if thieves successfully gained access to sensitive data.

## Responsibilities

Everyone who works for or with Rock School Bus CIC has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that Rock School Bus CIC meets its legal obligations.
- Amber Sinclair, is responsible for:
  - Keeping the board updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data Rock School Bus CIC holds about them (also called 'subject access requests').
  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
  - Approving any data protection statements attached to communications such as emails and letters.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

## General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from the board of directors.
- **Amber Sinclair will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be disposed of.
- Employees **should request help** from the board of directors if they are unsure about any aspect of data protection.

## Data storage

These rules describe how and where data is safely stored. Questions about storing data safely can be directed to the board of directors.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.

## Data use

Personal data is of no value to Rock School Bus CIC unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- Rock School Bus CIC **will not store any personal data electronically**
- Employees **should not save copies of personal data to their own computers**. Always access and update the central copy of any data.
- Emails **will not be CCd**

## Data accuracy

The law requires Rock School Bus CIC to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Rock School Bus CIC should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.

## Subject access requests

All individuals who are the subject of personal data held by Rock School Bus CIC are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date**.
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the board of directors at [therockschoolbus@gmail.com](mailto:therockschoolbus@gmail.com).

Individuals will be charged £10 per subject access request. The board of directors will aim to provide the relevant data within 14 days.

The board of directors will always verify the identity of anyone making a subject access request before handing over any information.

## Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Rock School Bus CIC will disclose requested data. However, the board of directors will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Signed: Amber Sinclair (Director)  
Signed: Abbi Thompson (Director)  
Signed Jules Jones (Director)

Date: 11th May 2022

Date to be reviewed: 11th May 2023