Data Protection Policy

Part I: Policy Overview

Scope and Purpose

Rock School Bus takes the protection of Personal Data very seriously. Personal Data is any information from which a living individual (a Data Subject) can be identified. This does not include anonymised data. Personal Data can be simple, such as a name, address, or telephone number, but may also include opinions, preferences, or, under GDPR, an IP address.

As a business, we are required to comply with the UK Data Protection Laws, including the Data Protection Act 2018 and the UK GDPR. Compliance is critical to protect individuals' rights and maintain our reputation. Everyone covered by this policy, including employees, contractors, and other individuals handling Personal Data on behalf of Rock School Bus, must ensure that all Personal Data is handled securely and lawfully.

This policy sets out how Rock School Bus handles Personal Data of customers, suppliers, business contacts, staff, shareholders, and other individuals. It is an internal policy and may be updated periodically. It is not part of an employment contract, and Rock School Bus reserves the right to amend it at any time.

Key Terms and Definitions

To aid understanding, key terms from Data Protection Laws are defined here. Automated Decision Making refers to decisions made solely by automated means, without human involvement. Consent is freely given, specific, informed, and unambiguous agreement from the Data Subject to process their Personal Data. A Data Controller is the entity responsible for determining how Personal Data is processed, whereas a Data Processor carries out processing tasks on behalf of the Data Controller under written instructions. Personal Data includes any information identifying a living individual, and Special Categories of Personal Data include sensitive information such as health, racial or ethnic origin, religious beliefs, trade union membership, sexual orientation, or biometric data. Processing encompasses all actions involving Personal Data, including collection, storage, use, disclosure, and deletion. Profiling refers to automated processing to evaluate certain aspects of a Data Subject, such as behaviour, preferences, or location.

Part II: Data Protection Responsibility

Compliance and Accountability

All employees, directors, contractors, and similar roles are required to comply with Data Protection Laws and this policy. Breaches may result in disciplinary action. Rock School Bus has appointed Amber Sinclair as the Data Protection Officer (DPO) or Data Protection Manager (DPM), responsible for overseeing compliance. They can be contacted via info@rockschoolbus.org.uk or 07939 266321. You should contact the DPO/DPM with any questions, concerns, or suspected breaches, or before undertaking new or unusual processing activities.

Accountability Principle

Rock School Bus must demonstrate compliance with Data Protection Laws. Measures include adopting this policy, providing staff training, implementing data protection by design and default, maintaining contracts with third-party processors, recording all processing activities, ensuring appropriate security, reporting breaches, conducting Data Protection Impact Assessments (DPIAs), and regularly reviewing all measures.

Record Keeping

The DPO/DPM maintains comprehensive records of all processing activities. Where acting as a Data Controller, records include contact details, purposes of processing, categories of Data Subjects, types of data processed, recipients, retention periods, transfers outside the EEA, and technical and organisational security measures. When acting as a Data Processor, additional records include the identity of the Data Controller, categories of processing undertaken on their behalf, and safeguards for transfers outside the EEA. All staff must notify the DPO/DPM before initiating new processing activities to ensure records remain up to date.

Part III: Data Protection Principles

Lawfulness, Fairness, and Transparency

Personal Data must be processed lawfully, fairly, and transparently. Lawful reasons include consent, contractual necessity, legal obligations, protection of vital interests, and legitimate interests that do not override Data Subjects' rights. Consent must be informed, freely given, and verifiable. Processing Special Categories of Data requires an additional lawful basis, such as explicit consent or legal obligations. Transparency requires providing a clear and accessible privacy notice to Data Subjects.

Purpose Limitation

Data must only be collected for specific, explicit, and legitimate purposes. Processing for additional purposes requires consultation with the DPO/DPM, who will advise on compliance and update records.

Data Minimisation

Only data necessary for the purpose should be collected and processed. Unnecessary or unrelated data must not be collected.

Accuracy

Personal Data must be accurate and kept up to date. Staff must regularly verify and, where necessary, correct or delete inaccurate data.

Storage Limitation

Data must not be retained longer than required. Retention periods are set out in Rock School Bus retention policy, which staff must follow. When data is no longer needed, it should be securely deleted or destroyed according to the company's destruction policy.

Security, Integrity, and Confidentiality

Personal Data must be processed securely, protecting against unauthorized access, loss, destruction, or damage. Extra safeguards are required for sensitive or special category data. Staff must follow the Information Security Policy or other relevant policies and report any security concerns to the DPO/DPM.

Part IV: Rights and Obligations

Data Subject Rights

Data Subjects have multiple rights under GDPR, including access, rectification, erasure, restriction, data portability, objection to processing, objection to automated decision making, and withdrawal of consent. Staff must immediately inform the DPO/DPM upon receiving any request, who will verify the requestor's identity and handle the request appropriately.

Disclosure and Sharing of Personal Data

Personal Data may only be shared if permitted under Data Protection Laws. Disclosure to third parties, including cloud providers, must meet conditions of necessity, consent, contractual safeguards, security assurances, and compliance with EEA transfer rules. Staff must contact the DPO/DPM before sharing data or engaging new service providers.

Part V: Personal Data Breaches

A data breach is any accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to Personal Data. Examples include misdirected emails, stolen records, unauthorized system access, or cyberattacks. Any suspected breach must be reported immediately to the DPO/DPM, along with any relevant documentation. The DPO/DPM investigates breaches, decides on reporting to the ICO and Data Subjects, and maintains a register of all breaches.

Part VI: Data-Protection-Related Matters

Data Protection by Design and Default

Data protection must be integrated from the outset of any project or system and throughout its lifecycle. Personal Data should be automatically protected, accessed only by those with a business need, and limited to necessary processing.

Data Protection Impact Assessments (DPIAs)

A DPIA must be conducted for any high-risk processing, including large-scale processing of sensitive data, profiling, new technologies, or projects affecting vulnerable individuals. The DPIA assesses the scope, necessity, compliance measures, risks, and mitigating measures. Staff must contact the DPO/DPM for guidance.

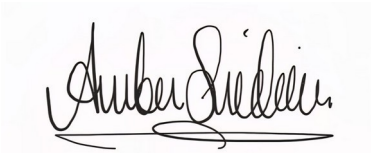
Automated Decision Making and Profiling

Automated decisions with legal or similar effects are prohibited unless based on contractual necessity, explicit consent, or legal authorization. Use of sensitive data requires explicit consent or substantial public interest justification. The DPO/DPM must be consulted before undertaking such processing, and appropriate safeguards must be implemented, including the ability for human intervention.

Direct Marketing

Direct marketing must comply with data protection and marketing laws. Data Subjects can opt out at any time. Marketing records must reflect preferences, and staff must contact the DPO/DPM before initiating campaigns to ensure compliance.

If you have any questions or require guidance on this policy, contact the DPO/DPM at the provided contact details.

Signed: 

Author Name & Job Title: Amber Sinclair, Director

Date: 01 December 2025

Next Review: Dec 2026