POLICY DOCUMENT

Breach Notification Policy

1. Introduction

Albatross Bus & Coaches Ltd is committed to protecting personal data and ensuring compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. As part of this commitment, the organisation recognises its legal obligation to respond promptly and effectively to any personal data breach.

Under UK GDPR requirements, certain types of personal data breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, those affected must also be informed without undue delay.

This policy sets out the approach Albatross Bus & Coaches Ltd will take to identify, manage, report, and learn from data breaches, including those involving operational systems.

2. What is a Data Breach?

2.1 Personal Data Breach

A personal data breach refers to a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Such breaches can occur through human error, technical failures, or deliberate actions.

A personal data breach is not limited to the loss of data; it also includes any incident that compromises the confidentiality, integrity, or availability of personal data. This may involve unauthorised access to booking information within the System, accidental deletion or alteration of customer records, or system failures that restrict or prevent access to personal data, where such incidents may have an impact on the rights and freedoms of individuals.

3. What breaches do we need to notify about?

Albatross Bus & Coaches Ltd will assess every data breach to determine whether it meets the threshold for reporting to the ICO. A breach must be reported within 72 hours if it is likely to result in a risk to individuals rights and freedoms. Where the risk is considered high, affected individuals must also be informed directly.

In assessing risk, the organisation will consider the nature of the data involved, the potential consequences and the likelihood of harm. This includes situations involving customer booking data, driver information, or any personal data processed through the Albatross Bus & Coaches ltd.

Where Albatross Bus & Coaches Ltd acts as a data processor, it will notify the relevant data controller without undue delay. Similarly, where third party processors are involved, contractual arrangements ensure that breach notifications are communicated promptly to support compliance obligations.

Examples of risks include:

- Financial loss or identity theft
- Damage to reputation
- Loss of confidentiality
- Emotional distress or discrimination

4. Information we MUST provide to the ICO in the event of a breach

In the event that a breach is reportable, Albatross Bus & Coaches Ltd will ensure that all required information is provided to the ICO in a clear and timely manner. This includes a description of the nature of the breach, the categories and approximate number of individuals and records affected, and the likely consequences of the incident.

The organisation will also provide details of the person responsible for managing the breach and outline the measures already taken or proposed, to address the breach and mitigate its impact. Where all information is not immediately available, an initial report will still be submitted within 72 hours, followed by further updates as necessary.

Information to be included:

- Nature and scope of the breach
- Categories and volume of data affected
- Contact details of responsible person
- Likely consequences
- Actions taken or planned

5. Data Breach Response Stages

To ensure an effective and consistent response, Albatross Bus & Coaches Ltd follows a structured process when managing data breaches. This approach ensures that incidents are handled quickly, risks are minimised, and compliance obligations are met.

The response process begins with identifying the breach and understanding its nature, followed by immediate containment and recovery actions. A detailed risk assessment is then conducted to determine the severity and whether notification is required. Finally, the organisation reviews the incident to identify lessons learned and implement improvements.

Core stages include:

- Identification of the breach
- Containment and recovery
- Risk assessment
- Notification (ICO and individuals)
- Review and improvement

6. Breach Response Plan

6.1 Identification and Reporting

All employees are responsible for identifying and reporting suspected data breaches promptly. The organisation ensures that staff receive appropriate training and understand their responsibilities in relation to data protection.

Any breach must be reported immediately to the designated Data Protection Lead, who will take responsibility for managing the incident. Accurate and detailed information must be recorded at the earliest stage to support investigation and decision-making. This includes breaches involving digital systems.

Information to record includes:

- Date and time of the breach and its discovery
- Method of discovery and reporting
- Systems and data affected
- Nature of the incident
- Supporting evidence

6.2 Contain the breach and instigate recovery

Once a breach has been identified, immediate steps must be taken to contain it and minimise its impact. This may involve isolating affected systems, restricting access, or recovering lost data. The Data Protection Lead will coordinate the response and involve IT support where necessary.

Prompt containment is critical to reducing the potential harm to individuals and limiting organisational risk. Recovery actions will be implemented as quickly as possible to restore normal operations.

Key actions include:

- Securing affected systems
- Preventing further unauthorised access
- Recovering data where possible

- Engaging IT support immediately

6.3 Risk Assessment

Following containment, a thorough risk assessment will be carried out to determine the potential impact on individuals. This assessment will evaluate both the likelihood and severity of harm, taking into account the type of data involved and the circumstances of the breach.

Special consideration will be given to sensitive data and the potential for misuse, particularly where customer or driver information is involved.

Factors considered include:

- Nature and sensitivity of the data
- Security measures in place
- Potential misuse of data
- Number of individuals affected
- Possible consequences

6.4 Notification of a breach

The decision to notify the ICO and affected individuals will be based on the outcome of the risk assessment. The Data Protection Lead will ensure that all required information is gathered and that notifications are made within the required timeframe.

Where individuals are informed, communication will be clear and transparent, providing details of the breach, its potential impact, and any steps they should take to protect themselves. Senior management, including Directors, will be informed of all significant breaches.

Notification actions include:

- Informing Directors
- Reporting to the ICO within 72 hours (if required)
- Communicating with affected individuals
- Managing public relations if necessary

6.5 Evaluation of breach, the response and Improvement

After the breach has been resolved, Albatross Bus & Coaches Ltd will conduct a full review of the incident to identify any weaknesses in processes, systems, or controls. This review will assess the effectiveness of the response and determine whether improvements are required.

Lessons learned from the incident will be used to strengthen data protection practices, including updates to policies, additional staff training, and enhancements to system security, including the Icabbi platform where relevant.

Post-incident actions include:

- Reviewing response effectiveness
- Updating policies and procedures
- Enhancing security measures
- Providing additional staff training

7. Roles and Responsibilities

Albatross Bus & Coaches Ltd ensures that clear roles and responsibilities are assigned for managing data breaches. The Data Protection Lead is responsible for coordinating the response and ensuring compliance with reporting obligations, while Directors provide oversight and strategic direction. All staff members have a responsibility to report suspected breaches immediately.

8. Documentation and Record Keeping

The organisation maintains a record of all data breaches, regardless of whether they are reportable to the ICO. This record includes details of the breach, its impact, and the actions taken in response. Maintaining such records is a legal requirement under UK GDPR and supports accountability and continuous improvement.

9. Review and Approval

This policy will be reviewed annually, or sooner if there are significant changes in legal or regulatory requirements. The Data Protection lead is responsible for ensuring that the policy remains up to date and effective.

Approved by

Managing Director: _____

Signature: _____

Approval Date: 15 April 2026

Revision / Amendment Register

Issue No.	Date of issue	Section / Clasue	Description of Change	Approved by
1			Initial Issue	