



# Jays Logistics (South West) Ltd

## JAYS LOGISTICS (SOUTH WEST) LTD

## DATA PROTECTION & UK GDPR POLICY

### Policy Statement

Jays Logistics (South West) Ltd is committed to protecting the privacy and security of personal data and ensuring compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and any other applicable data protection legislation.

During the course of your employment, you may have access to confidential personal information relating to employees, customers, suppliers, contractors, and other individuals. This may include names, addresses, telephone numbers, email addresses, payroll information, vehicle and driver records, health information, and other personal data.

All employees are required to handle personal information responsibly and in accordance with this policy. Failure to comply may result in disciplinary action, including dismissal, and may expose both the individual and the company to legal action and financial penalties.

The Company's designated Data Protection Lead is:

**Graham Hewlett**  
**Finance Manager**  
**Jays Logistics (South West) Ltd**

Any questions regarding data protection or requests relating to personal data should be directed to the Data Protection Lead.

---

## Scope

This policy applies to:

- All employees
- Agency workers
- Contractors
- Consultants
- Temporary staff

|                    |                         |
|--------------------|-------------------------|
| Version: Jays SC 1 | Review Date: 01-01-2027 |
| Reviewer: S GUMM   | Approver: M.Beavan      |



- Anyone processing personal data on behalf of Jays Logistics (South West) Ltd

The policy applies to both electronic and paper records.

---

## What is Personal Data?

Personal data means any information relating to an identified or identifiable living person.

Examples include:

- Name
- Home address
- Telephone number
- Email address
- National Insurance number
- Driving licence details
- Vehicle tracking information
- Payroll information
- Employment records
- Photographs
- CCTV images

## Special Category Data

Some personal data requires additional protection under UK GDPR.

This includes information relating to:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data used for identification
- Physical or mental health
- Sexual orientation or sex life

Criminal conviction and offence data is also subject to additional legal protections.

|                    |                         |
|--------------------|-------------------------|
| Version: Jays SC 1 | Review Date: 01-01-2027 |
| Reviewer: S GUMM   | Approver: M.Beavan      |



## UK GDPR Principles

All employees must comply with the following UK GDPR principles.

### 1. Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and transparently.

The company will only process personal data where there is a valid legal basis, including:

- Employment obligations
- Contractual necessity
- Legal compliance
- Legitimate business interests
- Consent (where required)

### 2. Purpose Limitation

Personal data shall only be collected for specified, explicit and legitimate purposes and shall not be used in a manner incompatible with those purposes.

### 3. Data Minimisation

Only personal data that is necessary, relevant and adequate for business purposes shall be collected and retained.

Personnel files and business records will be reviewed periodically to ensure unnecessary or excessive information is not retained.

### 4. Accuracy

Personal data must be accurate and kept up to date.

Employees are responsible for notifying management promptly of changes to:

- Home address
- Telephone number
- Emergency contacts
- Bank details
- Driving licence information
- Other relevant personal details

|                    |                         |
|--------------------|-------------------------|
| Version: Jays SC 1 | Review Date: 01-01-2027 |
| Reviewer: S GUMM   | Approver: M.Beavan      |



The company cannot be held responsible for inaccuracies where employees fail to notify relevant changes.

## 5. Storage Limitation

Personal data shall not be retained longer than necessary.

Typical retention periods include:

| Record Type                                   | Retention Period                                      |
|-----------------------------------------------|-------------------------------------------------------|
| Employee personnel files                      | 6 years after employment ends                         |
| Payroll records                               | 6 years                                               |
| Recruitment records (unsuccessful applicants) | 6 months                                              |
| Health and safety records                     | As required by law                                    |
| Driver and transport records                  | In accordance with legal and operational requirements |

Where data is no longer required, it will be securely deleted or destroyed.

## 6. Integrity and Confidentiality (Security)

Appropriate technical and organisational measures shall be taken to protect personal data against:

- Unauthorised access
- Unlawful processing
- Accidental loss
- Destruction
- Damage
- Disclosure

Security measures include:

### Physical Security

- Personnel files stored securely.
- Restricted access to authorised personnel only.
- Secure disposal of confidential records.

### Electronic Security

- Password-protected systems.
- Access controls based on job role.

|                    |                         |
|--------------------|-------------------------|
| Version: Jays SC 1 | Review Date: 01-01-2027 |
| Reviewer: S GUMM   | Approver: M.Beavan      |



- Multi-factor authentication where available.
- Encryption where appropriate.
- Regular software updates and security patches.
- Secure backups and disaster recovery procedures.

The Company currently utilises Microsoft cloud-based services and implements security controls appropriate to the nature of the data processed.

## 7. Accountability

Jays Logistics (South West) Ltd is responsible for demonstrating compliance with UK GDPR requirements.

Employees must:

- Follow company procedures.
  - Report data protection concerns immediately.
  - Cooperate with investigations and audits.
  - Complete any required data protection training.
- 

## International Transfers

Personal data will not be transferred outside the United Kingdom unless:

- Adequate safeguards are in place; and
- The transfer complies with UK GDPR requirements.

Where cloud service providers process data internationally, appropriate contractual and legal safeguards will be implemented.

---

## Data Subject Rights

Individuals have the following rights under UK GDPR:

### Right to be Informed

To know how their personal data is being used.

### Right of Access

To obtain a copy of personal data held by the company.

|                    |                         |
|--------------------|-------------------------|
| Version: Jays SC 1 | Review Date: 01-01-2027 |
| Reviewer: S GUMM   | Approver: M.Beavan      |



## Right to Rectification

To have inaccurate information corrected.

## Right to Erasure

To request deletion of personal data where appropriate.

## Right to Restrict Processing

To request limitations on how personal data is used.

## Right to Data Portability

To receive personal data in a usable electronic format where applicable.

## Right to Object

To object to certain types of processing.

## Rights Relating to Automated Decision-Making

To challenge decisions made solely by automated means where applicable.

---

# Subject Access Requests (SARs)

Employees and other individuals may request access to personal data held by the company.

Requests should be submitted in writing to the Data Protection Lead.

The company will normally respond within one month of receiving a valid request.

No fee will normally be charged for a Subject Access Request unless the request is manifestly unfounded or excessive.

---

# Data Breaches

Any employee who becomes aware of:

- Loss of personal data
- Unauthorised disclosure
- Cybersecurity incidents
- Accidental deletion
- Suspected data breaches

must immediately report the matter to the Data Protection Lead.

|                    |                         |
|--------------------|-------------------------|
| Version: Jays SC 1 | Review Date: 01-01-2027 |
| Reviewer: S GUMM   | Approver: M.Beavan      |



Failure to report a known breach may result in disciplinary action.

The company will investigate all incidents and, where legally required, notify the Information Commissioner's Office (ICO) within the required timescales.

---

## Employee Responsibilities

Employees must:

- Keep personal information confidential.
- Only access information required for their role.
- Verify the identity of anyone requesting personal information.
- Never disclose personal data to unauthorised individuals.
- Ensure personal information is transmitted securely.
- Lock computers when unattended.
- Keep passwords confidential.
- Follow company data retention and disposal procedures.
- Report suspected breaches immediately.

Employees must not:

- Access records without authorisation.
- Share passwords.
- Remove confidential records without permission.
- Store personal data on unauthorised devices or systems.
- Disclose personal information to family members or third parties without appropriate authority.

Unauthorised access to personal data may constitute gross misconduct and may result in dismissal.

---

## Employee Consent and Processing

Jays Logistics (South West) Ltd processes employee personal data primarily because it is necessary:

- To perform the employment contract;
- To comply with legal obligations;
- For legitimate business purposes.

The company will only rely on employee consent where UK GDPR requires consent to be obtained.

|                    |                         |
|--------------------|-------------------------|
| Version: Jays SC 1 | Review Date: 01-01-2027 |
| Reviewer: S GUMM   | Approver: M.Beavan      |



Employees will be informed separately of how their personal data is processed through the Company's Employee Privacy Notice.

---

## Complaints

Any concerns regarding the handling of personal data should be raised initially with:

**Graham Hewlett**  
**Finance Manager / Data Protection Lead**

If an employee remains dissatisfied, the matter should be raised through the Company's Grievance Procedure.

Individuals also have the right to lodge a complaint with the Information Commissioner's Office (ICO):

**Information Commissioner's Office**  
[www.ico.org.uk](http://www.ico.org.uk)

---

## Policy Review

This policy will be reviewed periodically and updated as necessary to ensure continued compliance with UK GDPR, the Data Protection Act 2018 and applicable regulatory requirements.

**Version: 2026**

**Approved By**

**Matthew Beavan, Operations Director Jays Logistics (South West) Ltd**

**Review Date: 01/01/2027**

|                    |                         |
|--------------------|-------------------------|
| Version: Jays SC 1 | Review Date: 01-01-2027 |
| Reviewer: S GUMM   | Approver: M.Beavan      |