



Jays Logistics

Data protection policy

In the course of your work you may come into contact with or use confidential information about employees, clients and customers, for example their names and home addresses. The Data Protection Act 1998 contains principles affecting employees' and other personal records. Information protected by the Act includes not only personal data held on a computer, tablet or mobile 'phone but also certain manual records containing personal data, for example employee personal files that form part of a structured filing system. The purpose of these rules is to ensure you do not breach the Act. If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from Graham Hewlett the company Finance Manager, has the responsibility for the control of Data under the GDPR act for Jays Logistics.

You can be criminally liable if you knowingly or recklessly disclose personal data, and a serious breach of this act will lead to disciplinary procedures as per company protocol. If you access another employee's personal records without authority, this will constitute as gross misconduct and could lead to dismissal.

During your course of work you many come into contact with or use confidential information about employees, clients and customers, eg their names and home addresses. If anyone is in doubt about what can and can not be disclosed and to whom, refrain from disclosing personal information until further advice has been sought form the company's compliance manager.

There are 8 data protection principles that are fundamental to the act. Everybody employed by Jays Transport must comply with these principles at all times.

- 1) Data should be processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data.

These conditions being that the employee gives consent to the processing, or the processing is necessary for the purposes set out in the act.

Sensitive information consists of;

- Race or ethnic origin
- Political opinions and trade union membership
- Religion or beliefs

Version: Jays SC 1	Review Date: 24-01-26
Reviewer: S GUMM	Approver: M.BEAVAN



- Physical or mental health conditions
 - Sexual life
 - Criminal offences (both committed and alleged)
- 2) Data should only be obtained for one or more specified and lawful purposes, and not in a manner incompatible with those purposes
 - 3) Data should be adequate, relevant, and not excessive. Jays will review personnel files on an annual basis to ensure that do not contain a backlog of out-of-date information and to check that there is a sound business reason for requiring the information to still be held
 - 4) Data should be accurate and kept up to date. If personal information changes, e.g. change of address, employees must inform their line manager as soon as possible so that the company's records can be updated. Jays can not be held responsible for any data errors if we have not been notified of the relevant changes
 - 5) Data should not be kept for longer than necessary, Jays will not keep personal data for longer than 6 years after the termination of employment. Different categories of data will be retained for different periods of time depending on legal, operational and financial requirements. Any data Jays see as not needing to be held for a required period of time will be held for only 6 months and then destroyed. Data relating to unsuccessful applicants will also only be held for a period of 6 months.
 - 6) Data should be processed in accordance with the rights of employees act
 - 7) Data must be secure, technical and organisational measures will be taken against unauthorised and unlawful processing of personal data and against loss or destruction of, or damage to data. Personnel files must be kept confidential and stored in locked filing cabinets, only authorised personal are to have access. Files are not to be moved for their normal place of storage without good reason. Files stored on disk or other removable media should be stored in locked cabinets. Data on computers should be password protected, encrypted and have coding, again only authorised persons are to have access to this data. The company has network backup procedures to ensure that data on computer cannot be accidentally lost or destroyed. All data, that is subject to GDPR, is hosted on Microsoft Azure and currently has the basic firewall in place. We restrict access via passwords.
 - 8)

Version: Jays SC 1	Review Date: 24-01-26
Reviewer: S GUMM	Approver: M.BEAVAN



Data must not be transferred to a country or territory outside the European economic area, unless that country can ensure an adequate level of protection for processing personal data.

Your consent to personal information being held

Jays logistics holds personal data about its employees, by signing your contract of employment, you have consented to your personal data being processed. It is a condition of your employment to agree to Jays holding your personal data. Jays will also hold limited sensitive personal data about its employees, eg sickness absence records, health needs and equal opportunities monitoring etc, again by signing your employment contract you give explicit consent to Jays holding and processing this data.

You right to access personal information

You have the right, upon request, to receive a copy of the personal information the company holds about you, including your personnel file and to demand that any incorrect information be amended or removed.

You have the right to request;

- What data the company holds on you and for what purposes
- To be given a description on the data and to whom it is being disclosed too.
- To have communicated in an intelligible form the personal data concerned, and any information available as to the source of the data.
- The logic involved in the computerized decision making

Upon request Jays will provide you with a statement regarding the personal data held about you. This will state all the information jays holds and processes about you and the reasons for such.

If you wish to access a copy of your personal data, you must make a written request for this. Jays reserve the right to charge a £10.00 processing fee.

If you would like to make a complaint that the rules are not being followed in respect of personal data that Jays holds about you, you should raise this matter with the compliance manager. If the matter is not resolved to you satisfaction, it should them be raised as a formal grievance unt the companies grievance procedure.

Version: Jays SC 1	Review Date: 24-01-26
Reviewer: S GUMM	Approver: M.BEAVAN



Your obligation in relation to personal information

You should ensure you comply with the following guidelines at all times;

- Do not give out confidential information to anyone other than the person specifically requesting it, it should not be given to someone in the same family or any other unauthorised third party, unless the data subject has expressed consent to do this.
- Be aware that sometimes those requesting information can use deception in order to obtain access to it. Always verify the identity of the data subject and legitimacy of the request, particularly before releasing personal information over the phone.
- Only transmit personal information via email if the network is secure, eg encrypted emails
- If you receive a request for personal information about another employee, this should be forwarded to the compliance manager. The compliance manager will then be responsible for dealing with this request.
- Ensure any personal data you hold is kept securely, either in a locked filing cabinet , or if computerised ensure it is password protected.
- Compliance with this act is your responsibility. If you have any concerns or questions about the interpretation of the rules, take this up with the compliance manager.

Signed

Matt Beavan
Operations Director

Date –

Version: Jays SC 1	Review Date: 24-01-26
Reviewer: S GUMM	Approver: M.BEAVAN