

DATA PROTECTION POLICY

INTRODUCTION

The Data Protection Act 1998 (DPA 1998) was introduced in response to an EC directive and has been amended in many important respects by the Data Protection Act 2003. It covers the control of manual records and sets conditions for processing personal data, which strengthen individuals' rights.

In order to comply with the requirements of the Data Protection legislation, PETA Ltd sets out the following Policy, which is communicated to all employees.

POLICY

The Data Protection legislation requires PETA Ltd to maintain strict security in relation to personal data held which relates to individuals, whether these individuals are employees, volunteers, learners, customers or suppliers.

In order to carry out the contract of employment, we hold and use personal data including sensitive personal data relating to our employees, which includes names and addresses, bank details and health records. We require this information so that we can contact and pay our employees, comply with our obligations under Health and Safety legislation and generally do the things we need to do as employers.

For the purposes of the Data Protection legislation, the Company needs to specify how it will use that information. PETA Ltd will only use it for legitimate purposes, which include:

- ▲ Complying with our obligations to our employees (e.g. paying them)
- ▲ Complying with our obligations under the general law (e.g. in relation to taxation, social security, or law enforcement)
- ▲ Providing information about employees to those who require it in connection with services that they provide to us (e.g. pension providers)
- ▲ The prosecution or defence of any legal proceedings
- ▲ Assessing employees, their performance and suitability for particular roles
- ▲ Doing anything for the benefit or welfare of employees, their families or dependants

Personal data will not be held other than for the purposes above and PETA Ltd will abide by the following rules:

1. Personal data will be kept secure and confidential and will not be disclosed outside the Company unless expressly permitted by the Director
2. Staff who have access to, or control over, personal data held by the Company, for example employee records or list or details relating to customers must ensure that it is stored securely (locked filing cabinets, and offices, password protected computers) and that access to it within the company is strictly on a "need to know" basis
3. Employees requested to transfer personal data to recipients outside the company (e.g. giving out a home telephone number of an employee) should check with the Director that such a transfer of information is authorised. Where there is any doubt, the Director will offer to telephone the employee concerned and ask them to contact the person requesting such information

4. Employees should be aware that it is a criminal offence to access or disclose personal data held by PETA Ltd without authority
5. Employees and volunteers should be aware that sharing personal data relating to a learner, other than for legitimate work related reasons, and to recognised partner agencies or approved third parties, is strictly forbidden. Where there is any doubt, this should in the first instance be discussed with your Line Manager. Any failure to ensure learner data confidentiality will result in disciplinary action, which may lead to dismissal and reporting to the Local Safeguarding Authority and/or the Police
6. Any failure to respect and handle personal data as set out in this policy will result in disciplinary action, which may lead to dismissal

RIGHTS OF ACCESS

The Data Protection legislation gives employees the right of access to their personal manual records, as well as computerised records. Employees have a right to a copy of any information held about them. By law, the company must provide this within 40 days of the request, and are entitled to make a charge. PETA Ltd will not make a charge, except when a request for information exceeds one request per annum.

Procedure for Employee Requiring Access to Personnel File

This procedure is to ensure that individual employees are aware of their right to access their personnel file and of the procedure to be adopted for such access.

Employees' personnel files contain a substantial amount of personal and private information and need to be treated confidentially. The Director has overall responsibility for such files and for ensuring their safekeeping.

An employee's personnel file will only be made available to:

- ▲ The individual concerned
- ▲ The person to whom they report
- ▲ Management senior to the person to whom they report
- ▲ Medical advisors to the company
- ▲ Management Services staff for updating purposes only

Should an employee wish to inspect his/her file, they should make a written request to this effect to their Manager, who will then forward this request to the Director. Inspection will normally be available within 14 days of the request being received by the Manager. Any delay over and above this period will be kept to a minimum.

The inspection must take place within Management Services in the presence of the Director or his nominated deputy. All papers, etc. should be kept in the same order in which they appear in the file and no paper or data, may be removed or copied without the permission of the Director or his nominated deputy.

PETA Ltd reserves the right to remove those items from personal files to which employees do not have the right of access for examples those parts of documents which identify other individuals who have not consented to being identified in this way (e.g. references).

Should an employee disagree with an item being included in their file, they should notify the Director so that a decision regarding the item may be made. Should the request to remove/amend a file be refused the employee will be notified in writing of the reasons for such a decision. If they do not agree with the decision, the matter can be pursued under PETA's Grievance Procedure and Appeals Procedure.

Associated policies in place within PETA Ltd are:

[Email Policy](#)

[Guidelines on Passwords](#)

[Internet Usage and Security Policy](#)

[Software Policy](#)

[Remote Access Policy](#)

Any questions regarding these policies should be directed to the ICT Systems Engineer.