

Pertemps Network



Data Protection Policy

Date of Issue: 30th April 2012

Author: Paul Horn

Document Version: 5

Last Review: January 2026

Next Review: January 2027

Definition

The Company: Refers to Pertemps Network Administration Limited and all of its subsidiary and associated companies.

Purpose

The Company is committed fully to compliance with the requirements of the Data Protection Laws covering the judicial state. Data Protection Laws covering the UK and EU judicial state applies to all companies that process data to their employees, as well as to others e.g. customers and clients. It sets out principles which should be followed by those who process data; it gives rights to those whose data is being processed.

To this end, the Company endorses fully and adheres to the 7 Principles of data protection, as set out in the Data Protection Laws covering the UK and EU Judicial state. In summary these state that personal data shall:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

As a Company that processes or uses personal information we will ensure that we follow these principles at all times. Therefore, through appropriate management and strict application of criteria and controls, the Company will:

- observe fully the conditions regarding the fair collection and use of information
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements
- ensure the quality of information used
- ensure that the information is held for no longer than is necessary
- ensure that the rights of people about whom information is held can be fully exercised under the Data Protection Laws covering the judicial state (i.e. the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information)
- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred abroad without suitable safeguards.

Status of Policy

The Policy does not form part of the formal Contract of Employment for Employees but it is a condition of employment that Employees will abide by the rules and policies made by the Company from time to time. Any failure to follow the Data Protection Policy may lead, therefore, to disciplinary proceedings.

Data Protection Officer

Employees or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself should raise the matter internally with HR or with Tracy Evans our Data Protection Officer, who can be contacted via email: tracy.evans@pertemps.co.uk or telephone: 01676 525000.

Employee Responsibilities

All Employees are responsible for:

- checking that any information that they provide to the Company in connection with their employment is accurate and up to date.
- informing the Company of any changes to information that they have provided, e.g. changes of address, either at the time of appointment or subsequently. The Company cannot be held responsible for any errors unless the employee has informed it of such changes.
- Adhering to the User Responsibilities: Information Security Policy as it cover the use and transfer of any data where it may be of a personal or sensitive nature.

Data Security

All Employees are responsible for ensuring that:

- any personal data that they hold is kept securely.
- personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Employees should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases. Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Subject Consent

In many cases, the Company can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the Data Protection Laws (and to which special rules apply), express consent must be obtained. Agreement to the Company processing some specified classes of personal data are condition of employment for Employees. This includes information about previous criminal convictions. Therefore, the application forms that all prospective Employees are required to complete will include a section requiring consent to process the applicant's personal data. A refusal to sign such a form will prevent the application from being processed.

Subject Access

An employee may request details of personal information which we hold about him or her under the Data Protection Laws. If an employee would like a copy of the information held on him or her, they are required to complete the Data Access Request Form (available on the Company Intranet site or via the HR department). The requested information will be provided within 30 days.

If an employee believes that any information held on him or her is incorrect or incomplete, then they should write to or email the HR Function as soon as possible, at Meriden Hall. The Company will promptly correct any information found to be incorrect.

Version Control

Version	Date	Author	Amendment
v01	30/04/2012	Paul Horn	Information captured
v5	16/04/2024	Megan Farley	Transferred information onto a company standard template