Platform Resourcing Permanent | Temporary | Onsite	Data Protection Policy
Doc No: PRL0001	Author: David Rowlands

Purpose

To set out Company policy with respect to Data Protection. This policy aims to ensure that all employees are aware of their rights and obligations concerning personal data processed by the Company, and to set out how the Company intends to comply with the provisions of the Data Protection Act 1998.

Scope

The policy applies to all employees of Platform Resourcing Limited

Responsibilities

- The overall responsibility for ensuring the policy is implemented, maintained, monitored and communicated to all employee's rests with the Human Resources Department.
- The Company inevitably processes personal data about employees in the normal course of its business only for the purposes of processing and maintaining records in relation to employment.
- The Company expects all employees to fully comply with the Data Protection Policy and the principles of the Data Protection Act. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures following from this policy.
- All employees will be responsible for:
    - Ensuring that any information they provide to the Company in connection with their employment is accurate and up-to-date
    - Informing the Company of any errors or changes to information which they have provided (e.g. change of contact details)
    - Checking the information that the Company holds about them from time-to-time for accuracy
- Depending on their job role, employees may also come into contact with, and use, confidential personal information about people, and they are expected to handle such information in line with the provisions of this policy. If an employee is ever in any doubt about disclosing confidential information they should seek advice from their line manager or the HR Director.

Data Protection Principles

"Data" refers to any information relating to an individual where the structure of the data allows information about the individual to be readily accessed. Almost all information about individuals that is processed on computer or held in a highly structured manual filing system is covered by the Act.

All personal data must be processed (handled) in accordance with the eight Data Protection Principles:

- Be processed fairly and lawfully;
- Be processed for limited purposes and not in any manner incompatible with those purposes;
- Be adequate, relevant and not excessive in relation to the purpose for which they are processed;
- Be accurate and, where necessary, kept up-to-date;
- Not be kept for longer than is necessary;
- Processed in accordance with the rights of the data subjects;
- Be protected by appropriate technical and organisational measures against unauthorised or unlawful processing, against accidental loss or damage;
- Not transferred to a country or territory outside the European Economic area unless that country or territory shows an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Data Security

The Company has defined Confidential Information in the contract of employment. All such Confidential Information remains the property of the company at all times. In particular employees must not use, copy, or destroy any Confidential Information without the authorisation of the Company's management, express or implied.

Employees must not disclose either directly or indirectly any Confidential Information to any other person, firm or Company for any reason whatsoever without the express authority of the management of the Company.

Employees are referred to the E-Mail and Internet Policy for policy and guidelines relating to the use of computers, e-mail and the internet.

Employees could be made criminally liable and fined if they knowingly or recklessly disclose personal information in breach of this policy. As a minimum, any breaches of this policy in relation to personal data security will result in disciplinary action and, in serious cases, may result in dismissal.

Conditions for Processing

Personal data must not be processed unless one of certain conditions is met. The employee must give their consent to the processing or alternatively the processing must be necessary for one of certain other reasons.

The Act also distinguishes between personal data and "sensitive personal data" which relates to racial or ethnic origin, political or religious beliefs, trade union membership, physical or mental health (medical data), or criminal records. In these cases, more stringent conditions must be met in the processing of sensitive personal data.

General Guidelines

Storing Personal Data

Personal data must always be held securely. In the case of manual data, this could be in filing cabinets, locked cupboards / drawers or rooms with restricted access. In the case of electronic information, access should be subject to reasonable controls such as passwords. Reasonable steps should be taken to detect and prevent unauthorised access. Particular care should be taken when laptops or PCs are used to process personal data away from the Company.

Managers should ideally ensure that HR holds copies of any personal data they hold on an employee, whether in electronic or manual form. The HR department should be able to say to an employee without hesitation that the information they have provided from their files is the total of personal data held concerning that employee.

Employees must notify changes of name, address, telephone number, bank and marital status to the HR department as soon as possible. The HR department will periodically ask employees to confirm any such personal data held by them.

Disclosing Personal Data

In most cases, personal data must not be disclosed to third parties (including family members, friends, government bodies) without the permission of the individual concerned, unless disclosure is exempted from the Data Protection Act or by other legislation. If in doubt, please see advice from the Data Protection Officer. The sender and recipient or personal data must enter into a written contract in which the recipient undertakes to keep the personal data confidential and to ensure that it is protected whilst in the recipient's hands.

Strict care and attention must be taken when transmitting personal data by e-mail or fax, and particularly when transmitting it outside of the EEA.

Disposal of Personal Data

All records are retained for periods in line with the recommendations of the Information Commissioner. Beyond this, personal data will be disposed of when no longer effectively required for its purpose. The method of disposal must be appropriate to the sensitivity of the data. Disposal may include transfer to an appropriate confidential archive system, shredding or confidential disposal. Employees must be aware that when disposing of printed confidential data, this must be shredded and not placed in the office recycling bins.

Ideally, electronic data should be destroyed by reformatting or overwriting. Note that "deleting" a computer file does not equate to destroying the data – such data can often be recovered.

Employees' Rights

Employees have the right to be given a description of all personal data held about them, and the personal data itself, together with the purpose for which it is being processed, the recipients and the source of the data (where the data is held in a "relevant filing system" as defined by the legislation).

The HR department will handle any such requests from employees or other individuals about whom the Company holds personal data.

Where the provision of information would reveal the identity of a third party, the information will not be provided unless the third party has given their consent or if it is deemed reasonable to proceed without their consent.

Procedure to Request Information

Employees must put their request in writing and forward to the HR representative, accompanied by the appropriate fee, as detailed in the table below:

Computerised Records (view only)	£Nil
Computerised Records (printed copy)	£5.00
Manual Records (view only)	£5.00
Manual Records (printed copy)	£10.00
Computerised & Manual Records (view only)	£10.00

The HR department will acknowledge receipt of all requests, and will arrange an appropriate date and time with the employee within 14 days. The appropriate fee will be deducted direct from the employee's salary.

Computerised Records

Requests to view computerised records will be dealt with by "walking" employees through each screen of the Human Resources software system and explaining the details held therein.

Employees may view the computerised records once per calendar year. If any employee makes more than one request per year, then a fee of £5.00 will be charged for each request.

Whilst viewing the data, should an employee find any information which is inaccurate, the employee has the right to request that the data is corrected or erased.

Penalties

Use or disclosure of personal data outside the terms registered with or notified to the Data Protection Commissioner is a criminal offence, as is the unlawful obtaining or disclosure of personal data. On conviction, both the Company and individuals responsible may be liable for a fine of up to £5,000.

Queries and Amendments

Any queries should be addressed to the Human Resources Department. Any amendments will be notified by revision of this document.

Please sign and date below to confirm that you have read, understood the above policy, and will adhere to the content.

Name: _____Signature:_____

Service Centre/Site: _____Date:_____