Data Protection Policy (Including Home Working)

Version: 4 – June 2025

Document Control

Version 5 Effective Date: 1st June 2025

Review Dates

Linked Policies

Safer Recruitment Policy
Disciplinary Policy
Password Policy

Person Responsible for the Policy
Managing Director

Name
Tony Higgins

Signature

Policy Statement

All organisations that process *personal data* are required to comply with data protection legislation. This includes in particular the Data Protection Act 1998 (or its successor) and the EU General Data Protection Regulation (together the 'Data Protection Laws'). The Data Protection Laws give individuals (known as 'data subjects') certain rights over their *personal data* whilst imposing certain obligations on the organisations that process their data.

The Company collects and processes both *personal data* and *sensitive personal data*. It is required to do so to comply with other legislation. It is also required to keep this data for different periods depending on the nature of the data.

This policy sets out how the Company implements the Data Protection Laws.

Definitions

In this policy the following terms have the following meanings:

'***consent***' means any freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the *processing* of persona data relating to him or her;

'***data controller***' means an individual or organisation which, alone or jointly with others, determines the purposes and means of the *processing* of *personal data*;

'***data processor***' means an individual or organisation which processes *personal data* on behalf of the *data controller*;

'***personal data***'* means any information relating to an individual who can be identified, such as by a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'***personal data breach***' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, *personal data*;

'***processing***' means any operation or set of operations performed on *personal data*, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'***profiling***' means any form of automated *processing* of *personal data* consisting of the use of *personal data* to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

'***pseudonymisation***' means the *processing* of *personal data* in such a manner that the *personal data* can no longer be attributed to an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational

measures to ensure that the *personal data* are not attributed to an identified or identifiable individual;

'*sensitive personal data*'* means *personal data* revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the *processing* of genetic data, biometric data, data concerning health, an individual's sex life or sexual orientation and an individual's criminal convictions.

* For the purposes of this policy we use the term '*personal data*' to include '*sensitive personal data*' except where we specifically need to refer to *sensitive personal data*.

'*Supervisory authority*' means an independent public authority which is responsible for monitoring the application of data protection. In the UK the *supervisory authority* is the Information Commissioner's Office (ICO).

All of these definitions are italicised throughout this policy to remind the reader that they are defined terms.

Data processing under the Data Protection Laws

The Company processes *personal data* in relation to its own staff, work-seekers and individual client contacts and is a *data controller* for the purposes of the Data Protection Laws. The Company has registered with the ICO and its registration number is Z1862361**.**

The Company may hold *personal data* on individuals for the following purposes:

- Staff administration;
- Advertising, marketing and public relations
- Accounts and records;
- Administration and *processing* of work-seekers' *personal data* for the purposes of providing work-finding services, including *processing* using software solution providers and back office support
- Administration and *processing* of clients' *personal data* for the purposes of supplying/introducing work-seekers

1. The data protection principles

The Data Protection Laws require the Company acting as either *data controller* or *data processor* to process data in accordance with the principles of data protection. These require that *personal data* is:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specified and legitimate purposes and not further processed in a manner that is in-compatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and kept up to date; every reasonable step must be taken to ensure that *personal data* that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept for no longer than is necessary for the purposes for which the *personal data* are processed;
6. Processed in a manner that ensures appropriate security of the *personal data*, including protection against unauthorised or unlawful *processing* and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and that
7. The *data controller* shall be responsible for, and be able to demonstrate, compliance with the principles.

2. Legal bases for processing

The Company will only process *personal data* where it has a legal basis for doing so (see Annex A). Where the Company does not have a legal reason for *processing personal data* any processing will be a breach of the Data Protection Laws.

The Company will review the *personal data* it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date.

Before transferring *personal data* to any third party (such as past, current or prospective employers, suppliers, customers and clients, intermediaries such as umbrella companies, persons making an enquiry or complaint and any other third party (such as software solutions providers and back office support)), the Company will establish that it has a legal reason for making the transfer.

3. Privacy by design and by default

The Company has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all *processing* activities. This includes implementing measures such as:

- data minimisation (i.e. not keeping data for longer than is necessary);
- *pseudonymisation*;
- anonymization
- cyber security;

Rights of the individual

The Company shall provide any information relating to data *processing* to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. The Company may provide this information orally if requested to do so by the individual.

1. Privacy notices

Where the Company collects *personal data* from the individual, the Company will give the individual a privacy notice at the time when it first obtains the *personal data*.

Where the Company collects *personal data* other than from the individual directly, it will give the individual a privacy notice within a reasonable period after obtaining the *personal data*, but at the latest within one month. If the Company intends to disclose the *personal data* to a third party then the privacy notice will be issued when the *personal data* are first disclosed (if not issued sooner).

Where the Company intends to further process the *personal data* for a purpose other than that for which the data was initially collected, the Company will give the individual information on that other purpose and any relevant further information before it does the further *processing*.

2. Subject access requests

The individual is entitled to access their *personal data* on request from the *data controller*.

3. Rectification

The individual or another *data controller* at the individual's request, has the right to ask the Company to rectify any inaccurate or incomplete *personal data* concerning an individual.

If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to rectify the *personal data* unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

4. Erasure

The individual or another *data controller* at the individual's request, has the right to ask the Company to erase an individual's *personal data.*

If the Company receives a request to erase it will ask the individual if s/he wants his *personal data* to be removed entirely or whether s/he is happy for his or her details to be kept on a list of individuals who do not want to be contacted in the future (for a specified period or otherwise). The Company cannot keep a record of individuals whose data it has erased so the individual may be contacted again by the Company should the Company come into possession of the individual's *personal data* at a later date.

If the Company has made the data public, it shall take reasonable steps to inform other *data controllers* and *data processors processing* the *personal data* to erase the *personal data*, taking into account available technology and the cost of implementation.

If the Company has given the *personal data* to any third parties it will tell those third parties that it has received a request to erase the *personal data*, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

5. Restriction of *processing*

The individual or a *data controller* at the individual's request, has the right to ask the Company to restrict its *processing* of an individual's *personal data* where:

- The individual challenges the accuracy of the *personal data*;
- The *processing* is unlawful and the individual opposes its erasure;
- The Company no longer needs the *personal data* for the purposes of the *processing*, but the *personal data* is required for the establishment, exercise or defence of legal claims; or
- The individual has objected to *processing* (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of the Company override those of the individual.

If the Company has given the *personal data* to any third parties it will tell those third parties that it has received a request to restrict the *personal data*, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

6. Data portability

The individual shall have the right to receive *personal data* concerning him or her, which he or she has provided to the Company, in a structured, commonly used and machine-readable format and have the right to transmit those data to another *data controller* in circumstances where:

- The *processing* is based on the individual's *consent* or a contract; and
- The *processing* is carried out by automated means.

Where feasible, the Company will send the *personal data* to a named third party on the individual's request.

7. Object to *processing*

The individual has the right to object to their *personal data* being processed based on a public interest or a legitimate interest. The individual will also be able to object to the *profiling* of their data based on a public interest or a legitimate interest.

The Company shall cease *processing* unless it has compelling legitimate grounds to continue to process the *personal data* which override the individual's interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

The individual has the right to object to their *personal data* for direct marketing.

8. Enforcement of rights

All requests regarding individual rights should be sent to Tony Higgins, Funding & Development Director.

The Company shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability or objection or automated decision-making processes or profiling within one month of receipt of the request. The Company may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

Where the Company considers that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature the Company may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

9. Automated decision making

The Company will not subject individuals to decisions based on automated *processing* that produce a legal effect or a similarly significant effect on the individual, except where the automated decision:

- Is necessary for the entering into or performance of a contract between the *data controller* and the individual;
- Is authorised by law; or
- The individual has given their explicit *consent*.

The Company will not carry out any automated decision-making or *profiling* using the *personal data* of a child.

10. Recording of meetings

Employees do not have the legal right to record an internal meeting, whether meetings are video calls, Zoom meetings or take place in person with portable recording devices.

Our policy is that recordings are not normally permitted unless all attendees agree to the meeting being recorded and this is evidenced at the beginning of the meeting. Any unauthorised recording will be viewed as serious misconduct and a breach of this policy would be grounds for disciplinary action. Recordings are personal data and as such are covered by the data protection act.

11. Recordings

Recordings should be stored securely on the servers with access limited only to those who have a need to access the recordings. The company Data Protection Policy must be complied with at all times. The recordings must be retained for a reasonable period after the meeting or hearing. For meetings, it would be reasonable to retain the recording until the minutes have been accepted. Staff must be aware that any recordings of meetings or hearings will be subject to the Freedom of Information Act and Data Protection Act, where relevant, subject to the standard exemptions from disclosure under those pieces of legislation. Where it relates to a dispute, copies of recordings may be shared with relevant parties as part of the normal disclosure process. Disposal - All recordings must be securely disposed of at the end of the retention period.

Personal Data Breaches

Reporting *personal data* breaches

All data breaches should be referred to Tony Higgins (Funding & Development Director, SP Training).

1. *Personal data breaches* where the Company is the *data controller*:

Where the Company establishes that a *personal data breach* has taken place, the Company will take steps to contain and recover the breach. Where a *personal data breach* is likely to result in a risk to the rights and freedoms of any individual the Company will notify the ICO.

Where the *personal data breach* happens outside the UK, the Company shall alert the relevant *supervisory authority* for data breaches in the effected jurisdiction.

2. *Personal data breaches* where the Company is the *data processor*:

The Company will alert the relevant *data controller* as to the *personal data breach* as soon as they are aware of the breach.

3. Communicating *personal data breaches* to individuals

Where the Company has identified a *personal data breach* resulting in a high risk to the rights and freedoms of any individual, the Company shall tell all affected individuals without undue delay.

The Company will not be required to tell individuals about the *personal data breach* where:

- The Company has implemented appropriate technical and organisational protection measures to the *personal data* affected by the breach, in particular to make the *personal data* unintelligible to any person who is not authorised to access it, such as encryption.
- The Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise.
- It would involve disproportionate effort to tell all affected individuals. Instead, the Company shall make a public communication or similar measure to tell all affected individuals.

Home Working

Background

When staff are required to work from remote locations, they shall ensure that sensitive data is not put at risk. The purpose of this policy is to inform staff about their own and the company's responsibilities regarding remote working and the use of mobile computer equipment or data storage devices outside company premises. Wherever staff are working, they must adhere to the same level of data protection as would be expected on company premises as set out in our Data protection Policy.

Policy

As a default staff will work from home via a VPN but, by exception, for staff to access company information from home, the home router/firewall must have the following configurations made (unless the company has provided VPN access to all the company data) to comply with our cyber security requirements:

i) Do not allow the router/firewall configuration pages to be accessible over the internet
ii) Do not allow the router/firewall to advertise services over the internet that terminate on the work or personal computer that is used for accessing company information.
iii) Change the default password of the home router/firewall as per the Password Policy.
iv) Ensure the router/firewall is changed promptly when the Internet Service Provider (ISP) sends out updated models and ensure the first 3 steps above are followed again.
v) If there is a suspected breach of the firewall credentials, the user must report this to the company's IT department and be familiar with how to change the password – or, at least, know who to ring to help facilitate this (this may be the ISP themselves or the Company's technical support team).
vi) Only use the computer and/or mobile device that has been provided by the company to access business information (unless your personal devices have been approved by the company).

Mobile computer equipment is any device that can store and process information electronically. This includes laptop computers as well as smaller handheld devices such as smart phones, USB devices and memory cards.

i) If computer equipment is removed from company premises for any length of time, it must be stored securely in a locked cupboard.
ii) Such equipment should never be left unattended in a staff member's car or on public transport.
iii) Non-members of staff or unauthorised persons must not be given the use of company owned computer equipment or storage devices.
iv) Always ensure that any device used in remote or home working, is not set up to automatically remember login details and passwords. The option to remember login information on browsers must not be used in case the device is stolen.

v) Log out of systems if computers are left unattended (computers must be protected by passwords in line with our Password Policy).
vi) Staff making use of any third-party equipment to access sensitive data must ensure the network is secure and not public.
vii) Any company owned computer equipment must be used responsibly. This includes not adding/removing software without authorisation and changing security controls.

When discussing business in person or on the phone, ensure that no sensitive information can be heard or seen by a third party.

i) Paper documents containing sensitive data must be securely locked away when not in use. Any such documents that are disposed of must be destroyed in line with our Disposal and Destruction Policy.
ii) You must not use personally owned devices for remote working or data storage.
iii) Staff must not use any third-party equipment to access sensitive data unless they are sure of its security.
iv) Staff must adhere to our Data Protection Policy when deciding what data should be encrypted.

At all times, staff must take measures to secure sensitive data while working outside the business premises.

This requires that staff:

i) Log out of systems if computers are left unattended (computers must be protected by passwords in line with our Password Policy.
ii) Employees must ensure that sensitive information is not on view to people nearby [See the company's Data Protection Policy]. For example, this could include notes stuck to computer screens, minutes of meetings, financial reports and other items deemed sensitive by the company.
iii) When printing sensitive documents, always ensure they are immediately collected from printers, fax machines or photocopiers.
iv) In no circumstances must personal computers be used for remote or home working without the relevant authorisation.

Compliance:

This policy forms part of the company's induction and ongoing security awareness programme. If there is anything within this policy that is not clear, or has not been understood, then you must inform your line manager or policy owner to seek further clarification.

Failure to comply with this policy, in whole or in part, may lead to disciplinary action.

The Human Rights Act 1998

All individuals have the following rights under the Human Rights Act 1998 (HRA) and in dealing with *personal data* these should be respected at all times:

- Right to respect for private and family life (Article 8).
- Freedom of thought, belief, and religion (Article 9).
- Freedom of expression (Article 10).
- Freedom of assembly and association (Article 11).
- Protection from discrimination in respect of rights and freedoms under the HRA (Article 14).

Complaints

If you have a complaint or suggestion about the Company's handling of *personal data* then please contact Tony Higgins, Managing Director, System People Ltd.

Alternatively, you can contact the ICO directly on 0303 123 1113 or at https://ico.org.uk/global/contact-us/email/

This policy is approved and endorsed by the System People Ltd Board and will be reviewed on a bi-annual basis.

Signed: 

By Whom: Tony Higgins, Managing Director **Date: June 2025**

Annex A – legal bases for processing personal data

a) The lawfulness of *processing* conditions for *personal data* are:

1. *Consent* of the individual for one or more specific purposes.
2. *Processing* is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual to enter into a contract.
3. *Processing* is necessary for compliance with a legal obligation that the controller is subject to.
4. *Processing* is necessary to protect the vital interests of the individual or another person.
5. *Processing* is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the *data controller*.
6. *Processing* is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of the individual which require protection of *personal data*, in particular where the individual is a child.

b) The lawfulness of *processing* conditions for *sensitive personal data* are:

1. Explicit *consent* of the individual for one or more specified purposes, unless reliance on *consent* is prohibited by EU or Member State law.
2. *Processing* is necessary for carrying out data controller's obligations under employment, social security or social protection law, or a collective agreement, providing for appropriate safeguards for the fundamental rights and interests of the individual.
3. *Processing* is necessary to protect the vital interests of the individual or another individual where the individual is physically or legally incapable of giving *consent*.
4. During its legitimate activities*, processing* is carried out with appropriate safeguards by a foundation, association, or any other not-for-profit body, with a political, philosophical, religious or trade union aim and on condition that the *processing* relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without the *consent* of the individual.
5. *Processing* relates to *personal data* which are manifestly made public by the individual.
6. *Processing* is necessary for the establishment, exercise, or defence of legal claims or whenever courts are acting in their judicial capacity.
7. *Processing* is necessary for reasons of substantial public interest on the basis of EU or Member State law which shall be proportionate to the aim pursued, respects the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the individual.
8. *Processing* is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Member State law or a contract with a health professional and subject to the necessary conditions and safeguards.
9. *Processing* is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the individual, in particular professional secrecy.
10. *Processing* is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard fundamental rights and interests of the individual.