**Data Protection Policy**

**Introduction**

At Women Of Our Time, we are committed to being transparent about how we collect and use the personal data of our employees and to meeting our data protection obligations.

This policy sets out (and simplifies) the Company’s commitment to data protection, and individual rights and obligations in relation to personal data.

**Who is it for?**

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, and former employees, referred to as HR-related personal data.

**When should it be used?**

* Daily by all employees irrespective of level or title.
* During the storage, deletion, transfer or administering of any data internally and externally.
* To train and onboard employees and managers.

**What do we mean?**

Throughout this policy, we may use abbreviations to refer to Women Of Our Time or our employees as outlined below:

* Us, We, Our, The Company = Women Of Our Time
* You, Your = the client

**Data Protection Explained**

GDPR has been a buzz word over the last few years as the law changed and we have more rights around our personal data. This extends to your data at work and the data of the Company. Data protection laws mean we must treat data in a certain way and ensure we store and process it in line with the legislation and the data protection act.

**Data Protection Definitions**

Data protection and the terms outlined in legislation can be complex, so we’ve broken this down below to hopefully make the reading of this policy easier:

* **"Personal Data"** “is any information that relates to an individual who can be identified from that information.
* **“Processing”** is any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.
* **"Special Categories of Personal Data"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.
* **"Criminal Records Data"** means information about an individual's criminal convictions and offences, as well as information relating to criminal allegations and proceedings.

**Data Protection Principles**

We always process personal data in accordance with the following data protection principles:

* Lawfully, fairly and in a transparent manner.
* Only for specified, explicit and legitimate purposes.
* Only where it is adequate, relevant, and necessary for the purposes of processing.
* Personal Data that is accurate and is rectified or deleted without delay when inaccurate.
* Only for the period necessary for processing.
* Appropriate measures are taken to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

We will always tell you (and those outlined in the scope of this policy) the reasons for processing their personal data, how we use the data and the legal basis for processing it. We will not process personal data of individuals for other reasons. If we need to start processing personal data for other reasons, individuals will be informed of this before any processing begins.

**Data Processing**

* Personal data will not be shared with third parties, except as required for the proper administration of our duties for example, for processing of payroll or pension.
* Where we rely on legitimate reasons for processing data, we will always carry out an assessment to ensure that those reasons are not overridden by the rights and freedoms of individuals.
* Where the Company processes special categories of personal data or criminal records data to perform obligations, to exercise rights in employment law, or for reasons of substantial public interest, this is done in accordance with relevant legislation.
* We will update personal data promptly if an individual advises us that their information has changed or is inaccurate.
* Personal data gathered during the individual's time with the business is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which we hold personal data is in line with the relevant legislation.
* We keep a record of our processing activities in respect of personal data in accordance with the requirements of the UK GDPR.

**Individual Rights**

As a data subject, individuals have a number of rights in relation to their personal data:

***Subject Access Requests***

You have the right to ask an organisation whether or not they are using or storing your personal information. You can also ask them for copies of your personal information, verbally or in writing. This is called the right of access and is commonly known as making a subject access request or SAR.

If you make a subject access request, we will tell you:

* whether the data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected personally.
* to whom your data is or may be disclosed, including to recipients located outside the UK and the safeguards that apply to such transfers.
* for how long your personal data is stored (or how that period is decided).
* your rights to rectification or erasure of data, or to restrict or object to processing.
* your right to complain to the Information Commissioner if you think the organisation has failed to comply with your data protection rights; and
* whether we carry out automated decision-making and the logic involved in any such decision-making.
* We will also provide you with a copy of your personal data undergoing processing. This will normally be in electronic form. If you request paper-based copies, we will charge a fee, which will be based on the administrative cost of providing the paper copies.
* To make a subject access request, you should send the request to the Data Protection Officer (as named at the end of this Policy). In some cases, we may need to ask for proof of identification before the request can be processed.
* We will usually acknowledge receipt of your request within 2 weeks and will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the request is complex, we may need up to three months to respond from the date the request is received. We will always let you know of our intended timescales.
* If a subject access request is manifestly unfounded or excessive, we are not obliged to complete it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded if it is made with the intention of harassing the Company or causing disruption, or excessive where it repeats a request to which we have already responded. If you submit a request that is unfounded or excessive, we will notify you if this is the case and whether it will respond to it.

**Other rights**

You have a number of other rights in relation to their personal data. You can require the Company to:

* rectify inaccurate data.
* stop processing or erase data that is no longer necessary for the purposes of processing.
* stop processing or erase data if your interests override the organisation's legitimate grounds for processing data.
* stop processing or erase data if processing is unlawful.
* stop processing data for a period if data is inaccurate or if there is a dispute about whether your interests override our legitimate grounds for processing data.

To ask us to take any of these steps, you should send the request to the Data Protection Officer (as named at the end of this Policy).

**Data Security**

We take the security of personal data seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

**Third Parties**

Where we engage third parties to process personal data on our behalf, such parties are under a duty of confidentiality and are obliged to comply with all data protection laws, of which Women Of Our Time will check during tendering. An example of a third party in this instance may be a HR System provider or payroll provider.

**Data Breaches**

If we discover that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery or sooner where possible. We will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

**International data transfers**

Women Of Our Time will not ordinarily transfer personal data to countries outside the UK. Sometimes we may use providers whose servers or cloud-based systems sit outside of the UK. Where this occurs, we will always ensure they meet the requirements for data retention, storage, and transfer as outlined in this policy data protection laws as part of our tendering process.

**Individual Responsibilities**

Individuals are responsible for helping us keep their personal data up to date, for example if your address or bank details change.

Some employees may have access to the personal data of other individuals and clients in the course of their employment, for example Human Resource employees. Where this is the case, we rely on individuals to help meet our data protection obligations and may carry out more in-depth checks on hiring.

Employees who have access to personal data are required:

* to access only data that they have authority to access and only for authorised purposes;
* not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
* to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
* not to remove personal data, or devices containing it from our premises/and systems without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
* not to store personal data on local drives or on personal devices that are used for work purposes;
* to keep upto date on legislation and changes in data protection; and
* to report data breaches of which they become aware of immediately

**Training**

We will provide training to all individuals about their data protection responsibilities as part of the induction process [and at regular intervals thereafter]. Employees whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

**Data Protection Officer**

Our appointed Data Protection Officer is Karen Powell, as the person with responsibility for data protection compliance within the organisation.

**Our Policies**

Our policies are adopted on a non-contractual basis and Women Of Our Time reserves the right to change them at any time.

*Policy Last Updated: March 2025*