JOHN WORTH GROUP (JWG)
EMPLOYEE PRIVACY NOTICE

OVERVIEW

John Worth Group is committed to data protection and data privacy. With the General Data Protection Regulation (GDPR) becoming enforceable from 25 May 2018, we have undertaken a GDPR readiness programme to review our entire business, the way we handle data and the way in which we use it to provide our services and manage business operations.

We hold personal data on all our employees to meet legal obligations and to perform vital internal functions. This notice details the personal data we may retain, process and share with third parties relating to your employment and vital business operations. We are committed to ensuring that your information is secure, accurate and relevant. To prevent unauthorised access or disclosure, we have implemented suitable physical, electronic, and managerial procedures to safeguard and secure personal data we hold.

INTRODUCTION

We have issued this notice to describe how we handle personal information that we hold about our staff and job applicants (collectively referred to as "you"). For the purposes of this notice, the term "employee" includes temporary and contract workers, independent contractors, consultants, professional advisors

We respect the privacy rights of individuals and are committed to handling personal information responsibly and in accordance with applicable law. This notice sets out the personal data that we collect and process about you, the purposes of the processing and the rights that you have in connection with it.

If you are in any doubt regarding this notice, please contact Sian Coley on 01455 271202.

TYPES OF DATA WE COLLECT

During your employment with us, or when making an application for employment, we may process personal data about you and your dependents, beneficiaries and other individuals whose personal data has been provided to us.

The types of personal information we may process include, but are not limited to:

- Identification data – such as your name, gender, photograph, date of birth, staff member IDs.
- Right to work data/Anti money laundering /health and safety legislation – photocopy of passport or driving licence
- Health questionnaire on induction.
- Copies of driving licences for all employees who drive company vehicles or drive on behalf of the company
- For relevant employees we conduct annual health surveillance examinations
- Contact details – such as home and business address, telephone/email addresses, emergency contact details.
- Employment details – such as job title/position, office location, employment contract, performance and disciplinary records, grievance procedures, sickness/holiday records.
- Background information – such as academic/professional qualifications, education, CV, criminal records data (for vetting purposes, where permissible and in accordance with applicable law). E.g. DBS certification number for client safeguarding purposes

- Spouse & dependents information, marital status.
- Financial information – such as banking details, tax information, withholdings, salary, benefits, expenses, allowances, stock and equity grants.
- IT information – information required to provide access to our IT systems and networks such as IP addresses, log files and login information.
- If you are a temporary employee, contract worker or consultant, the type of personal information we process is limited to that needed to manage your specific work assignment.
- References relating to previous roles and employment conduct may be undertaken prior to commencement of employment. We will only gather references from referees provided to us by the employee, or prospective employee.

John Worth Group are required to hold the details of an emergency contact for all employees and contractors. **It is the employee's responsibility to gain explicit consent to share the emergency contact details with JWG.**

Sensitive personal data ('special categories of personal data' under the General Data Protection Regulation) includes any information that reveals your racial or ethnic origin, religious, political or philosophical beliefs, genetic data, biometric data for the purposes of unique identification, trade union membership, or information about your health/sex life. Generally, we try not to collect or process any sensitive personal information about you, unless authorised by law or where necessary to comply with applicable laws. In some circumstances, we may need to collect some sensitive personal information for legitimate employment-related purposes: for example:

- data relating to your racial/ethnic origin, gender and disabilities for the purposes of:
- equal opportunities monitoring;
- to comply with anti-discrimination laws; and
- for government reporting obligations;
- data relating to your physical or mental health to:
- provide work-related accommodations,
- health and insurance benefits to you and your dependents; or
- to manage absences from work.

PURPOSE FOR PROCESSING DATA

Recruitment

If you are applying for a role with us then we collect and use this personal data for recruitment purposes – in particular, to determine your suitability for a specific role. This includes assessing your skills, qualifications and verifying your information, carrying out reference checks or background checks (where necessary) and to generally manage the hiring process and communicate with you about it.

If you are accepted for a role with us, the data collected during the recruitment process will form part of your ongoing employee record.

Employment

We collect and process personal data relating to our employees to meet our obligations under the employment contract and to comply with our legal obligations. We take the security of your data seriously and are committed to being transparent about how we collect and use that data and to meeting our data protection obligations.

Once you become an employee, we collect and use this personal information for managing our employment or working relationship with you – for example, your employment records and contract information (so we can manage our employment relationship with you), your bank account and salary details (so we can pay you), your equity grants (for benefits plan administration) and details of your spouse and dependents (for emergency contact and benefits purposes).

Where we process special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that we use for these

purposes is anonymised or is only collected with the express consent of employees, which can be withdrawn at any time.

We have policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed without authorisation and only accessed or used for specific legal purposes.

You have some obligations under your employment contract to provide the organisation with data. You may also have to provide the organisation with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide this data may mean that you are unable to exercise your statutory rights.

We process our employees' personal information through a third party, who helps us to administer employee compensation and benefits. The third party is based in the United Kingdom and adopts stringent security requirements to ensure that all appropriate security controls are in place to protection personal information.

Legitimate business purposes

We may also collect and use personal information when it is necessary for other legitimate purposes, such as to help us conduct our business more effectively and efficiently – for example, for general IT security management, accounting purposes or financial planning. We may also process your personal information to investigate violations of law or breaches of our own internal policies.

The IT Department will record and monitor usage of all our IT equipment, user activity, voice traffic, email and Internet usage as deemed necessary. The IT Department will observe the strictest confidentiality when undertaking these activities. They will make their report directly to Directors who will determine the actions that may need to be taken in any particular case.

Our site(s) is/are protected by circuit television (CCTV) systems throughout its premises as deemed necessary and employees should expect all areas (other than those where use would contravene common decency) to be visible on a television monitoring system. Any information obtained from systems will be used with strict adherence to the GDPR. Information will be used for the prevention and detection of crime and to ensure compliance with our policies and procedures and our legal obligations. This may include using recorded images as evidence in disciplinary proceedings.

We provide services to organisations who have safeguarding policies in place to protect vulnerable individuals. It is a requirement to provide a DBS certification number for all JWG employees working on these sites.

Legal purposes

We may also use your personal data where we consider it necessary for complying with laws and regulations, including collecting and disclosing employee personal information as required by law (e.g. for tax, health and safety, anti-discrimination laws), under judicial authorisation, or to exercise or defend our legal rights.

LEGAL BASIS FOR PROCESSING PERSONAL DATA

Our legal basis for collecting and using the personal data described above will depend on the personal data concerned and the way we collect it. We will normally collect personal data from you only where we need it to perform a contract with you (i.e. to manage the employer/employee relationship), where we have your freely given consent to do so, or where the processing is in our legitimate interests and only where this interest is not overridden by your own interests or fundamental rights and freedoms. In some cases, we may also have a legal obligation to collect personal information from you or may otherwise need the personal information to protect your vital interests or those of another person.

Any processing based on consent will be made clear to you at the time of collection or use – consent can be withdrawn at any time by contacting Sian Coley on 01455 271 202.

WHO WE SHARE YOUR DATA WITH

We take care to allow access to personal data only to those who require such access to perform their tasks and duties, and to third parties who have a legitimate purpose for accessing it. Whenever we permit a third party to access personal information, we will implement appropriate measures to ensure the data is used in a manner consistent with this notice and that the security and confidentiality of the data is maintained.

We share employee's names, business contact details, photographic identification and DBS certification number to organisations to who we deliver services who require this documentation for safeguarding purposes.

Business contact details are listed on office desks and walls, access to the offices is restricted to the employees and contractors.

Transfers to third-party service providers

In addition, we make certain personal data available to third parties who provide services to us. We do so on a "need to know basis" and in accordance with applicable data protection and data privacy laws.

For example, some personal data will be available to our employee benefit plans service providers and third-party companies who provide us with employment law advice, health and safety support, insurance providers, payroll support services, expenses, tax and travel management services.

Transfers to other third parties

We may also disclose personal data to third parties on other lawful grounds, including:

- To comply with our legal obligations, including where necessary to abide by law, regulation or contract, or to respond to a court order, administrative or judicial process
- In response to lawful requests by public authorities (including for national security or law enforcement purposes)
- As necessary to establish, exercise or defend against potential, threatened or actual litigation
- Where necessary to protect the vital interests of our employees or another person
- In connection with the sale, assignment or other transfer of all or part of our business; or
- With your freely given and explicit consent

TRANSFER OF PERSONAL DATA ABROAD

We may need to transfer personal data to countries outside of the United Kingdom. When we export your personal data to a different country, we will take steps to ensure that such data exports comply with applicable laws. For example, if we transfer personal data outside the European Economic Area (EEA), such as to the United States, we will implement an appropriate data export solution such as entering into contracts with the data importer that contain EU model clauses or taking other measures to provide an adequate level of data protection.

DATA RETENTION

Personal data will be stored in accordance with applicable laws and kept for as long as needed to carry out the purposes described in this notice or as otherwise required by law. Generally, this means your personal information will be retained until the end or your employment, employment application, or work relationship with us plus a reasonable period of time thereafter to respond to employment or work-related inquiries or to deal with any legal matters (e.g. judicial, insurance claims or disciplinary actions), document the proper termination of your employment or work relationship (e.g. to tax authorities), or to provide you with ongoing pensions or other benefits.

For more information, please see our GDPR Policy, which outlines our current document retention schedule.

YOUR RIGHTS

You may exercise the rights available to you under data protection law as follows:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws. You can read more about these rights at:

https://ico.org.uk/for-the-public/is-my-information-being-handled-correctly/

To exercise any of these rights, please write to Data Protection Officer

ISSUES AND COMPLAINTS

We try to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention if they think that our collection or use of information is unfair, misleading or inappropriate. We would also welcome any suggestions for improving our procedures.

This notice was drafted with clarity in mind. It does not provide exhaustive detail of all aspects of our collection and use of personal information. However, we are happy to provide any additional information or explanation needed.

If you want to make a complaint about the way we have processed your personal information, you can contact the Information Commissioner's Office in their capacity as the statutory body which oversees data protection law – www.ico.org.uk/concerns.

UPDATES TO THIS NOTICE

This notice may be updated periodically to reflect any necessary changes in our privacy practices. In such cases, we will inform you. We encourage you to check this notice periodically to be aware of the most recent version.