Data Protection, Privacy and Retention Policy

WHAT IS THE PURPOSE OF THIS DOCUMENT?

The Company is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the Data Protection Act 2018. It applies to all employees, clients and contractors.

The Company is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice at your request.

This notice applies to current and former employee's, clients and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

DATA PROTECTION PRINCIPLES

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). There are "special categories" of more sensitive personal data which require a higher level of protection.

We will collect, store, and use the following categories of personal information about you where required:

1. Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
2. Date of birth.
3. Gender.
4. Next of kin and emergency contact information.
5. National Insurance number.
6. Bank account details, payroll records and tax status information.
7. Salary, annual leave, pension and benefits information.
8. Start date.
9. Location of employment or workplace.
10. Copy of driving licence and car insurance details where required.
11. Recruitment information (including copies of CVs and cover letters, right to work documentation, passports, and references).
12. Employment records (including job titles, work history, working hours, training records and professional memberships).
13. Compensation history.
14. Performance information.
15. Training information
16. Disciplinary and grievance information.
17. CCTV footage where used
18. Photographs.

We may also collect, store and use the following "special categories" of more sensitive personal information:

1. Information about your race, national and ethnic origin for the purpose of equal opportunities.
2. Information about your health, including any medical condition, health and sickness records.

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about employees and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract, we have entered with you.
2. Where we need to comply with a legal obligation.
3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest.

SITUATIONS IN WHICH WE WILL USE YOUR PERSONAL INFORMATION

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases, we may use your personal information to pursue legitimate interests of our own or those of third parties provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

1. Making a decision about your recruitment or appointment.
2. Determining the terms on which you work for us.
3. Checking you are legally entitled to work in the UK (Legal).
4. Paying you and, if you are an employee, deducting tax and National Insurance contributions.
5. Liaising with your pension provider.
6. Administering the contract, we have entered with you.
7. Business management and planning, including accounting and auditing
8. Conducting appraisals, performance reviews, managing performance and determining performance requirements.
9. Making decisions about salary reviews and compensation.
10. Assessing competency for a job or task.
11. Gathering evidence for possible grievance or disciplinary hearings.
12. Making decisions about your continued employment or engagement.
13. Planning for the termination of our working relationship.
14. Education, training and development requirements.
15. Contacting you for legitimate business purposes.
16. Dealing with legal disputes involving you, or other employees, clients and contractors, including accidents at work .
17. Ascertaining your fitness to work..
18. Managing sickness absence.
19. Complying with health and safety obligations.
20. To prevent fraud.

21. To monitor your use of our information, computer and communication systems to ensure compliance with our IT policies.
22. For security purposes too ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
23. To conduct data analytics studies to review and better understand employee retention and attrition rates.
24. Equal opportunities monitoring and dealing with our regulators and quality assurance.
25. Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

IF YOU FAIL TO PROVIDE PERSONAL INFORMATION

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

CHANGE OF PURPOSE

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent;
2. Where we need to carry out our legal obligations;
3. Where it is needed in the public interest, such as for equal opportunities monitoring;
4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

OUR OBLIGATIONS AS AN EMPLOYER

We will use your particularly sensitive personal information in the following ways:

1. We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
2. We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
3. We will use information about your race or national or ethnic origin to ensure meaningful equal opportunity monitoring and reporting.

DO WE NEED YOUR CONSENT?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

THIRD PARTIES

We may have to share your data with third parties, including third-party service providers and other entities in the group. We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

WHY MIGHT YOU SHARE MY PERSONAL INFORMATION WITH THIRD PARTIES?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

WHICH THIRD-PARTY SERVICE PROVIDERS PROCESS MY PERSONAL INFORMATION?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our company. The following activities are carried out by third party service providers: pension administration, IT services.

HOW SECURE IS MY INFORMATION WITH THIRD-PARTY SERVICE PROVIDERS AND OTHER ENTITIES IN OUR GROUP?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

DATA SECURITY

Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.

Communications sent by post / courier or using electronic means.

We have put in place measures to protect the security of your information. Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Workstation Security

Protecting your workstation area - is an important duty all JOS Structures Ltd Users should take very seriously.

- **It is your workstation.** That means that only you should be using it, and primarily, for business purposes only. Allowing other JOS Structures Ltd employees to use your workstation is strictly prohibited, do not let anyone have unsupervised access to your workstation. Imagine another employee using your workstation, accessing the Internet and possibly downloading unsuspected malware, sending unprofessional e-mails, or any other unwanted action. It can and has happened with companies, and you don't want to be blamed for something you didn't do, so do not share your workstation rights.

- **Use strong passwords**. Passwords are used as a means to secure your workstation, and the software that runs on it, from any unauthorised access. It is important to make your passwords unique, do not use any personal information as your password. Use letters, numbers and symbols within your password, that way it will make it complex and secure. It will very likely be that

your password for your IT workstation, software logins and so on, will have been already generated and allocated to you.

- **Security Updates.** Make sure your workstation has all the required security updates for the operating system and all other applications running. This also means having anti-virus running at all times and conducting periodic scans. Additionally, the use of anti-spyware may also be required as it provides additional layers of protection. especially during Internet use.

- **Do not alter security settings.** Your workstation has been configured for maximum security along with performance, so it is strongly advised that you do not attempt to disable or modify the configuration settings to the operating system or any other applications. By doing so you may increase security vulnerabilities that would ultimately allow malicious files and other harmful scripts reside on your workstation.

- **Do not install any unapproved software.** Your workstation has also been configured for providing you the necessary tools in performing daily roles and responsibilities, which means no additional software is needed. Do not download or install into any of the drives or ports, additional software that has not been approved as it may contain malicious files, and could consume additional resources, or is simply not professionally suitable for the work environment.

- **Removable storage devices.** They're easy-to-use, inexpensive, and a great way for transferring information, yet they can also pose a serious threat when the wrong information is stored on them and in the wrong hands. Having said that, USB ports, thumb drives, external drives and other removable storage and memory devices should never hold and highly sensitive and confidential information such as Personally Identifiable Information (PII), or any other data deemed privileged. Such information should be transferred over the network using approved protocols and residing on Company servers only.

- **Use caution with E-mail.** Be careful when opening e-mails from unknown parties, especially attachments. If an e-mail looks suspicious, then do not open it under any circumstances. Additionally, avoid clicking on links or banner advertisements sent to you as these often contain spyware, malware, etc.

- **Be mindful of Instant Messaging.** The use of Instant Messaging software on Company IT systems is expressly forbidden.

- **Handle privileged information with care.** From e-mails containing sensitive information to hard copy documents for contracts, trade secrets, or any other type of confidential data, treat it with the utmost care and professionalism, making every effort to protect its confidentially and integrity. Do not divulge such information to unintended parties and never leave items (i.e. in coffee shops, training seminars, conferences, etc).

- **Report security issues immediately.** Remember, if you see something, say something - and immediately. You have a responsibility for helping protect the

Company, which means being aware of your surroundings and reporting suspicious activity to authorised personnel - immediately. From seeing a door ajar that shouldn't be, to finding sensitive documents lying in a common office area.

- **Shut down and protect your workstation.** When leaving your workstation area at the end of each day, make sure that you completely shut down and turn off all computers and related devices. Additionally, pick up and store any documents, electronic media, or any business and/or professional items that should not be left unattended. Use your judgement by asking yourself the following simple question - "what risk or security danger is there is there for leaving something not securely locked up and put away.

Laptop Security

Securing your laptop at all times is extremely critical, and it requires comprehensive measures regarding its physical security, while also protecting all electronic data residing on it. From travelling for meetings to connecting to open public wireless access points, your laptop is a constant target for malicious activity, so beware. Take the following precautions for securing what's arguably one of your most important possessions:

- **Use encryption.** The full-disk encryption ensures the safety and security of your data (i.e., user files, swap files, system files, hidden files and so on.) residing on your laptop, especially if it is stolen or misplaced.

- **Use anti-virus**. It's one of the most fundamentally important - and often not used - pieces of security software, so make sure your laptop has anti-virus software running always, along with it scanning for viruses and other malware at regular intervals. Also ensure that the anti-virus software is current and is updated regularly.

- **Turn on your firewall.** Blocking suspicious traffic is essential for laptop security, so turn on and "enable" your default personal firewall or an approved personal firewall software.

- **Use strong passwords.** When turning on your laptop, your initial password should be extremely strong, with a combination of letters, numbers and symbols used. Once your initial password is compromised, the contents of your entire laptop (especially if you are not using full-disk encryption) can be compromised. Do not use terms and phrases for which somebody might find an association with you as your password, such as favourite football team, home address, middle name and so on.

- **It's your laptop.** Therefore, don't let other individuals use it, especially if it is somebody you don't know. When situations arise that require it to be used by someone other than you, create a guest account for their use.

- **Secure it physically.** A good investment is a security cable with a lock for securing your laptop at a workstation on any other that requires such. They're relatively inexpensive and a great deterrent to any thief.

- **Keep a watchful eye.** Don't ever leave your laptop unattended in any public venue or location not considered safe. Being vigilant and watchful always is a must for the safety and security of your laptop, so remember - do not leave it unattended - plain and simple. The best safety measure of all is to carry it with you always.

- **Place your contact information somewhere visible.** Because most people are honest and trustworthy, should your laptop be stolen, misplaced or lost - and then subsequently found by someone - you should clearly display your name, company telephone number, company address and e-mail on the laptop. Such information can be put on a sticker on the cover lid or the bottom of the laptop.

- **And if your laptop is stolen**. Laptops can and do get stolen, so think and act quickly, which means reporting the theft to the Police along with informing Company management team immediately.

Software Licensing and Usage

It's also important to understand the company's general policy on software usage, which includes numerous responsibilities that all employees need to be aware of. Software is used by all of us, each day, as it's vital to performing daily tasks for one's job function. With that said, please be mindful of the following issues:

- **Use only approved software.** Only software approved and purchased for the Company from a reputable software house and retailer should be installed and used on Company IT equipment. This includes your workstation and any other device provided to you by the Company. Unapproved and unlicensed software can contain dangerous or malicious code that can pose a serious threat to the Company's IT infrastructure. Simply stated, only load and use legally approved software on Company computers.

- **Do not duplicate software.** The licensing rights for software are strict and extremely rigid, allowing only a predetermined number of installations for a given data set. This means that you are not allowed to copy or duplicate any Company approved and purchased software - no exceptions. Copyright laws - and other regulations around the World - often place strict guidelines on software usage, so please keep this in mind.

- **Use caution on your own devices.** When using your own personal workstation, laptop, or other device, please consider and be mindful of the software you install, especially when such computing systems are used for accessing the corporate network. While the guidelines on software for your personal computers are less restrictive, you must still exercise extreme caution when loading any type of application onto your devices.

- **Accept updates.** For software to function efficiently and safely, security and patch updates have to be applied on a regular basis, so you must ensure that you accept such updates when they are generated and distributed and also take time to update any software on your personal computers.

- **Downloading from the Internet.** Any software obtained from the Internet is to be considered copyright protected, which means accepting any copyright agreements, and also comprehensively scanning the software to ensure that no dangerous or malicious code exists. The Internet can be an extremely dangerous forum when it comes to software as many products seems harmless, only to contain viruses, and other malicious code that can wreak havoc on IT systems. Think before you start downloading any software online.

DATA RETENTION

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, client or contractor of the company we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

1. Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

2. Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
3. Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
4. Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your situation which makes you want to object to processing on this ground.
5. Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
6. Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Director in writing.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Director. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

CONTACT

The Director will oversee compliance with this privacy notice. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Review

This policy will be reviewed and issued on at least an annual basis.

Legislation: Data Protection Act 2018

Signed *J O Sullivan* Date 23rd August 2024

Signed *A O Sullivan* Date 23rd August 2024