Data Protection and Retention Policy

The information and guidelines within this policy are important and apply to all Employees, Temporary Employees, Self-Employed Contractors and Suppliers at Ord Industrial Ltd, ("the Company") and all other Company sites that you may be asked to work or study at from time to time.

Data Protection Principles

The Company complies with the Data Protection Act 1998 and the principles of the Act, your personal data will be:

- Fairly and lawfully processed.
- Processed for limited purposes and not in any way incompatible with those purposes.
- Adequate, relevant and will not be excessive.
- Not kept for longer than necessary
- Processed in accordance with your individual rights.
- Not transferred to countries without adequate data protection.

Your Agreement

Certain types of personal data may be processed for particular purposes without the consent of individual data subjects. However, it is the Company's policy to seek express consent whenever practical from individual data subjects for the main ways in which the Company may hold and process personal data concerning them. This is to allow individuals an opportunity to raise any objections to any intended processing of personal data. The Company will consider any such objections but reserves the right to process personal data in order to carry out its functions as permitted by law. Therefore, all Employees, Temporary Employees, and Self-Employed Contractors will be asked to sign a consent form regarding particular types of information which Simply Bathrooms & Heating may in due course hold/process about them. All existing employees will also be asked to sign a consent form (Annexe A)

Your Personal Data

The Company only holds and processes personal data directly relevant to your employment or study for various purposes (for example, the administration of effective provision of welfare services, to record training and to operate the payroll services). This data is collected as and when required, such information includes, but is not limited to:

Third-party employment references:

- Employment reports or assessments, including performance reviews.
- Disciplinary details, including informal or formal warnings.

- Grievance procedures and outcomes.
- Salary reviews, benefits records and expenses claims.
- Health records.
- Training records

This information is only collected to assist the Company in monitoring performance, achievements, health and safety administration etc, and complying with the law on the appointment of staff in regulated activity roles for example. It is also necessary to process information so that staff can be recruited and paid, training organised and legal obligations to government bodies etc complied with.

Your personal data may be disclosed within the Company to those within the company who are required to use it. Your personal data will not be disclosed to your peers or any other employees that do not require access to the data in order to carry out their own roles within the Company.

Maintaining Records

The Company will take all reasonable steps to ensure that personal data held by the Company is accurate and kept up to date. To ensure accuracy the Company will ask employees every 12 months to check that their personal information held by the Company is correct. As an employee you should always contact management should your personal information change for any reason, for example a change of surname, home address or telephone number. Out of date information or information that is no longer required will be deleted (and securely destroyed) by the Company on a regular basis.

Sickness & Health Records

For day-to-day management the Company needs to keep records relating to the personal sickness and health records of each employee. Such personal data will record any periods of sickness or health matters, detailing the length and nature of the issue and the outcome. These records will be used to assess the health and welfare of employees and to highlight any issues that may require further investigation. Such data will only be disclosed to management and will not be disclosed to fellow employees, (except those employees within the company who process such data). If for any reason you do not wish your health records to be kept please contact the management.

Security of Data

The Company is committed to the secure storage and where undertaken the secure transmission of employees personal data. Only management and employees within the company have access to such data. All such data is protected by physical security, such as locks and technical security, such as usernames and passwords to access computer records and data. Such data is only disclosed on a "need to know" basis. To further ensure the security of such records the Company reserves the right to monitor and keep detailed log file and computer data analysis of all accesses

to employees' personal data. The Company also reserves the right to vet all employees who have access to such data in the course of their normal employment within the Company.

If as an employee you have legitimate access to personal data and you pass or transmit the data within the Company to another party or parties who in turn have the right to see such data, the following rules apply:

When sharing personal information, you must ensure the recipient of the information understands the purpose for which the information is being shared and any limits to consent given, i.e., what information may or may not be shared and the circumstances under which it may or may not be shared with other agencies; and the need to ensure that any further handling of the information is fair and secure.

Sharing personal information securely by telephone

Verify the name, job title, department and organisation of the person requesting the information and the reason for the request.

Take a contact telephone number, preferably a main switchboard number. Try to avoid a direct line or mobile telephone number wherever possible. If you are in any doubt, confirm the requestor's identity with their organisation.

Consider whether the information requested can be provided in response to a telephone request and in a telephone conversation. If in doubt, tell the enquirer you will call them back later.

Ensure that your conversation cannot be overheard by anyone who should not hear it.

Provide information only to the person who has requested it (do not leave information as a message or share with another).

Transporting personal information securely by hand (only where completely necessary)

Only where completely necessary, should personal information be taken off site by hand.

Record when you are taking any personal information off site, the reason(s) for doing so and the date when the information was returned, if appropriate.

Paper based information should be transported in a sealed file or envelope.

Electronic information must be protected by appropriate security measures (see section below on using removable electronic devices).

Information should be kept safe and close to hand. Never leave information unattended unless properly secured.

When transferring information by car, ensure it is placed in the boot and is kept locked.

Return the information to your site as soon as possible and file or dispose of it securely.

Sharing personal information securely by post

Confirm the name, department and address of the recipient.

Seal the information in a double envelope, ensuring the packaging is sufficient to protect the contents during transit.

Mark the inner envelope 'Private and Confidential – To be opened by Addressee Only'.

Make sure that there is nothing on the outer envelope that would indicate that it contains personal information.

Ensure a return address is included on both the outer and inner envelopes in case it has to be returned for some reason.

When appropriate send the information by recorded delivery or by locally approved courier;

When necessary, ask the recipient to confirm receipt.

Sharing personal information securely by e-mail

Unencrypted email is not a safe or secure method of transporting personal information. To share securely by email the following measures should be applied.

Confirm the name, department and email address of the recipient.

Ask the recipient to confirm receipt e.g. use delivery and read request settings.

Include the personal information in a document to be attached to the email, save it as "Read Only" and use encryption or electronic document password protection. Inform the recipient of the password by telephone or, once receipt of the document is confirmed, in a separate email.

Clearly mark the subject 'Private and Confidential'.

Save an audit trail of your email communications.

Sharing information securely using removable electronic devices, e.g. USB memory sticks, Blackberrys, IPhones, IPads, CDs etc

These devices are particularly vulnerable to loss or theft.

The following measures should be applied when using such devices:

- The information must be transferred securely
- Care must be taken with the use of any portable electronic devices as they may not provide adequate protection. If it is necessary to use a portable electronic device then the personal information must be securely encrypted or password protected in line our Data Protection Policy
- Ensure any loss or suspected loss is reported immediately.
- After use, the personal information must be securely deleted off the device. It is unacceptable to continue to carry personal information on a portable electronic device beyond the required or necessary time.

Parties with legitimate access to such data should not use third parties without the authority to view the data to send or receive the data on their behalf.

All employees are reminded that unauthorised attempts to gain access to such data or accessing such data are a disciplinary offence and in certain situations may constitute gross misconduct leading to summary dismissal. Such breaches may also constitute a criminal offence under the Data Protection Act 1998.

Benefits Schemes

Where the Company may provide additional benefits such as health insurance and pension schemes the Company will not make use of data collected by third parties administering the schemes where such data is not required for the day-to day operation of the Company. The Company will provide employees with details of what information will be collected by these third parties and how it will be used. Furthermore the Company will seek permission for the collection and use of this data prior to collection.

Equal Opportunities Monitoring

The Company may collect information relating to ethnic origin, sex or disability as part of an equal opportunities policy. The Company will ensure that any questionnaires relating to such information are accurate and that where possible the results will identify employment trends within the Company, and not identify individual employees.

Employee Reviews & Appraisals

The Company will only collect data required for the day-to day operation of the Company.

Data Transfers outside the European Economic Area

If the Company transfers data outside the European Economic Area such data will only be transferred to countries deemed by the European Commission to provide adequate data protection or to countries, which are recognised "safe harbours" for such data. However, the Company may transfer data to other countries where the permission of the employees has been given.

Data Access & Disclosure

All prospective, current or past employees, self-employed contractors, tutors and learners have the right to request access to data directly relating to them, which is held by the Company. The Company is entitled to seek a fee of up to £10 (+ VAT) to deal with each request. Furthermore the Company can request further information from the person making the request in order to provide accurate and relevant results and to check the identity of the person making the request. The Company seeks to provide such information within 40 days of receiving a request. The Company will provide the person making the request with the following information:

Whether they hold any information regarding them, and if they do:

- Descriptions of that information
- What it is used for.
- The type of third party Organisations it is passed to.
- Provide a breakdown of any technical terms or codes.

The information where reasonably possible will be provided in a hard copy or permanent electronic form.

References

The Company will not disclose details of confidential references where to do so would disclose the identity of the author or where it may cause harm or detriment to the author.

External Disclosure Requests

Where employees receive external requests for the disclosure of data the following guidelines should be observed:

- Verify the identity of the person requesting the information.
- Be on the lookout for fraud or deception.
- Seek a written request where possible.
- Check any telephone numbers where an oral request is received.
- Inform Management if any request appears suspicious.

The Management should also be contacted where the party requesting the data states that disclosure is required by law.

Remember that a duty is owed to the employee whose data is to be disclosed, where possible seek their permission, unless doing so would alert them to a criminal investigation.

If the disclosure of the data is non-routine where possible provide the employee in question with a copy of the data disclosed. A record of all non-routine data disclosures should also be kept.

Other Disclosures

Where the Company wishes to disclose employee data for promotional, marketing or other business purposes, (for example incorporated into an advertisement or brochure) the consent of the employee or learner would be sought in advance. The employee or learner would also be told where the data will be published and how widely.

Employee Monitoring

The Company will inform all employees where employee monitoring is introduced or increased. The Company will take reasonable steps to ensure that employee's privacy and autonomy are preserved. The Company will take reasonable steps to ensure that specific details of personal conversations or correspondence are not accessed. However, the Company retains the right to monitor the actual use of Company resources by employees.

Medical Testing

If the Company undertakes any form of medical testing of employees such testing will only be undertaken for clear health and safety reasons, for assessing an employee's medical fitness for continued employment or to assess their entitlement to health benefits, such as sick pay. Prospective employees may be tested for similar reasons. The results of any testing required for a health or pension scheme shall not be given to the Company.

Retention of Records

The Company will retain records for the following periods:

Application Form: for period of employment

- References: 1 year
- Payroll and tax information: 6 years
- Sickness records: 3 years
- Annual leave records: 2 years
- Unpaid/special leave records: 3 years
- Annual appraisal/ assessments: 5 years

- Promotions: 1 year from end of employment
- Transfers: 1 year from end of employment
- Training: 1 year from end of employment
- Disciplinary matters: 1 year from end of employment
- References provided: 5 years from provided or end of employment
- Summary of service: 10 years from end of employment
- Records and reports of accidents (RIDDOR): 3 years after the date of the last entry (or in case of persons under 18, 3 years after their 18th birthday.
- Medical Records kept by reason of the Control of Substances hazardous to health (COSHH 2002): 40 years (general monitoring records 5 years)

The Company will ensure the safe and secure disposal of employee records that are no longer required.

Criminal Liability

Knowingly or recklessly disclosing the personal data of others without the express consent of the Company can constitute a criminal offence.

Date of Implementation

This policy is effective from 4th January 2016 and shall not apply to any actions that occurred prior to this date.

Questions

If you have any questions regarding this policy document and how it applies to you, including how to request access to your personal data please consult the Management.

Alteration of this Policy

This policy will be subject to review, revision, change, updating, alteration and replacement in order to introduce new policies from time to time to reflect the changing needs of the business and to comply with legislation. Any alterations will be communicated to you by the Management

July 2022

Managing Director