HRPS05

Data Protection Policy

Policy information	
Organisation	The Data Controller is the Managing Director, supported by the management team.
Scope of policy	All personnel records and client confidential data held in hard copy and electronic formats, as maintained by the Data Controller and delegated members of the management team.
Policy operational date	04th August 2021
Policy prepared by	Managing Director and the SHEQ Advisor
Date approved by the Managing Director	04th August 2022

Data Protection Policy

Introduction	
Purpose of policy	• Complying with the law • Following good practice • Protecting clients, staff and other individuals • Protecting the organisation
Personal data	This includes hard and electronic copies of personnel records, including but not limited to: • Application forms and other records that include staff addresses, contact details, photographs, bank details, and National Insurance numbers etc. • Competency records that include staff names, photographs, and National Insurance numbers etc.
Client data	This includes hard and electronic copies of client documents and records, including but not limited to: • Contract specification, purchase orders and other documents that include addresses and contact details, etc. • Client supplied drawings that includes the layout of buildings and other structures etc.
Supplier data	This includes hard and electronic copies of supplier documents and records, including but not limited to: • Supplier evaluation and other records that include addresses, contact details, bank details etc. • Invoices / receipts that include addresses, contact details, bank details etc.
Policy statement	the Company is committed to: • Comply with both the law and good practice • Respect individuals' rights • Be open and honest with individuals whose data is held • Provide training and support for staff who handle personal data, so that they can act confidently and consistently • Protect data held against customers and suppliers,
Key risks	Main risks to the Company: • Information about individuals, customers and suppliers getting into the wrong hands, through poor security or inappropriate disclosure of information • Individuals being harmed through data being inaccurate or insufficient

Responsibilities	
Trustees	The Managing Director has overall responsibility for ensuring that the business complies with its legal obligations, under the Data Protection Act 1998 / General Data Protection Regulation (GDPR) (EU) 2016
Data Protection Officer **Data Controller**	The Managing Director is identified as the Data Protection Officer. He's responsibilities include: • Briefing the management, training and support team on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising other staff on tricky Data Protection issues • Ensuring that Data Protection induction and training takes place, • Handling subject access requests • Approving unusual or controversial disclosures of personal data
Management Team, including Administration Support Staff	Staff that handle personal data shall comply with this Policy and all supporting management system procedures to ensure that good Data Protection practice is maintained. This includes induction and training records etc. Also, staff must ensure that the Data Protection Officer is informed of any changes in their uses of personal data that might affect the Company's Notification.
Enforcement	The penalties levied on the Company and individuals within the Company for infringing the Data Protection may include an unlimited fine and compensation paid to the damaged party. Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts.

Confidentiality	
Scope	As part of this Policy, confidentiality shall be limited to personal data covered by the Data Protection Act 1998, the General Data Protection Regulation (GDPR) (EU) 2016. GPDR will apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU. Additionally, confidentiality shall also cover commercial and security data relating to our customers and supply chain.
Understanding of confidentiality	the Company shall ensure that personal data is not disclosed or access made available to such data to persons that have no authority to see such data. There will always be cases where the Company feels it is right to break confidentiality, although this should be decided on a case-by-case basis whether this is appropriate. Access to personnel records shall be limited to Managing Director and administration staff (including specialist suppliers for audit purposes). Access to personnel and financial records shall be limited to the Managing Director and administration staff, i.e. on a “need to know” basis; no one should have access to information unless it is relevant to their work. Access to customer or supplier documents and records shall be limited to the Managing Director and Project Managers, i.e. on a “need to know” basis; no one should have access to information unless it is relevant to their work.
Communication with Data Subjects	Staff shall be informed about confidentiality of their personnel and financial record, so that there is minimal risk of them being surprised at any later stage to find out that who has information about them.
Communication with staff	All staff that process and maintain personal data on individuals, and data on customers and suppliers shall receive appropriate training and information to enable

	them to undertake their duties in-accordance with Company policies and procedures, and specifically whether information should be disclosed, or access allowed.

Security	
Scope	Security shall be applied to all personnel and training records. Security shall also be applied to all commercial and security documents and records relating to our customers and suppliers.
Setting security levels	Security levels include: • The communication of data over the phone, • The transmission of data via fax or email, • Desktop security, where hard copy and electronic data may be left on the desk or displayed on the screen by authorised staff, and where unauthorised staff or outside parties may view or remove such data, • The transport of paper records by vehicle, • The storage of electronic data / records, • The transfer of records upon request to a new employer.
Security measures	Security measures shall include but not limited to: • Training and instruction to staff to prevent data being disclosed over the phone, without establishing the caller's authorisation to have the data, • Call back process, to ensure he requesters identity is verified before disclosing data, • Faxed data is only sent once the recipient has confirmed they are by the receiving fax, • Fax headers to clearly state the data being sent is confidential, • Screen savers and password protection set up to ensure inactive screens do not display data, • Promote and monitor a clear desk policy, to ensure personal data is not left unattended, • Paper records to be stored out of sites when transporting these by vehicle, and the vehicle doors to be locked and the immobilizer / alarm activated when leaving the vehicle for any length of time, • Ideally paper records should not be stored overnight in a vehicle, • Server networks and databases shall be protected by appropriate security software / firewalls, • The uploading of software onto server networks must be authorised by the Managing Director,

	• All requests for the transfer of records a new employer must be made in writing and confirmed with the individual prior to the transfer taking place.
Business continuity	The Company shall maintain all personnel, records in secure filing cabinets, and the offices shall be alarmed against intruders and fires. The Company Database and other electronic registers, containing personnel data shall be retained on the Company server, which is backed-up weekly, with the back-ups held in a fireproof safe off-site. The Company Database, containing customer and supplier data shall be retained on the Company server, which is backed-up weekly, with the back-ups held in a fireproof safe off-site.
Specific risks	Staff may be tricked into giving away personal, customer and supplier data by phone or e-mail. Staff shall receive guidance for dealing with these threats.

Data recording and storage	
Accuracy	Where information is taken over the telephone, it shall be checked back with the person by repeating the information, and where appropriate confirmed in writing. If information is supplied by a third party, the accuracy of the information shall be checked for errors or omissions and to ensure it is legible.
Storage	All hard copy personal data shall be stored in secure cabinets at the Worthing Office. Data held electronically, shall be restricted to authorised personnel only, and protected by password.
Retention periods	Personnel and training data shall be held for the duration of an individual's employment then retained as an archive record for at least 40 years. Customer and supplier data shall be held for the duration of a contract / supplier approval is maintained, then retained as an archive record for at least 6 years, or as specified by contract requirements.
Archiving	Hard copy archive records shall be held in numbered storage boxes that detail the records enclosed, with a register for each archive box. The boxes shall be held securely and protected from damage or deterioration. The content of the archive storage boxes shall be checked at least annually. Records passed their retention period shall be destroyed through shredding or incineration. Electronic records shall be held on Company server, and permanently deleted.

Subject access	
Responsibility	All requests for access to personal data must be processed by the Managing Director who is responsible for ensuring that subject access requests are handled within the legal time limit of 40 days. All requests for access to customer and supplier data must be processed by the Managing Director who is responsible for ensuring that subject access requests are only made to legitimate authorities, including the Police, HMRC, HSE and EA etc.
Procedure for making request	Subject access must be in writing to the Managing Director. He shall review the request and confirm receipt in writing to the requester. As requests are infrequent and can be complex, the Director may seek legal advice before agreeing to release the data. Subject access relating to customers and suppliers must be in writing to the Managing Director. He shall review the request and confirm receipt in writing to the requester. As requests are infrequent and can be complex, the Director may seek legal advice before agreeing to release the data.
Provision for verifying identity	Before handing over any data, the Requester shall be required to provide proof of identity using photographic identification. This may include a Passport, Driving Licence, Warrant or other Cards etc.
Charging	The the Company reserves the right to charge a £10 administration fee, which shall be clearly detailed in the confirmation letter, which shall have an invoice attached for payment.
Procedure for granting access	The provision of the data shall normally be as a hard copy (in permanent form) format. Supervised access in person may be arranged for certain types of data.
Removal of Harmful Information	Prior to the release of personal data to the requester, the Company shall ensure this data has been reviewed by an authorised person so that harmful information and references to other people are removed. In the case of personnel and financial records, the data shall be reviewed by the Managing Director.

Transparency	
Commitment	the Company is committed to ensuring that in principle staff, customers and suppliers are aware that their data is being processed and • For what purpose it is being processed • What types of disclosure are likely, and • How to exercise their rights in relation to the data
Procedure	This shall be achieved through the Company Induction process for staff. Other individuals shall be informed in a manner appropriate to the type of data being held, e.g.: • Quotations • Purchase Orders • Consent forms
Responsibility	The Managing Director is responsible for ensure all staff are inducted into the Company. The Managing Director and administration staff are responsible for ensuring Employees are suitably informed and sign the appropriate consents and acknowledgements.

Consent	
Underlying principles	Consent from individuals is one way of complying with the fair processing conditions covered under the Data Protection Act 1998 / General Data Protection Regulation (GDPR) (EU) 2016. Personnel records shall only be disclosed to other staff in order to arrange a method for payment and for communicating important safety information. In such cases, no consent is formally requested. Where outside parties request personal information, this shall not be disclosed without written consent from the staff. By agreeing to a Quotation or accepting a Purchase Order, it is accepted this is reasonable consent to forward data relating to customers and suppliers for the purposes of business, i.e. the delivery and handover of products and services.
Withdrawing consent	the Company acknowledges that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where the Company has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

Staff training & acceptance of responsibilities	
Documentation	Staff responsibilities regarding Data Protection are detailed within their agreed Job Descriptions.
Induction	All staff who have access to any kind of personal data and data relating to customers and suppliers are briefed against their Job Descriptions as part of their Company Induction.
Continuing training	Data Protection issues shall be communicated through training, team meetings, and supervisions etc.

Policy review	
Responsibility	The Managing Director is responsible for reviewing the Policy at least annually.
Procedure	The review shall take place at the Annual Management Review Meetings, which must be chaired by the Managing Director, attended by at least one of the management team.
Timing	Annually.

Signed……

Managing Director

24th September 2020

Next Review by: 23rd September 2021

Notes

Data Controller

The Data Controller is the legal 'person' responsible for complying with the Data Protection Act 1998 / General Data Protection Regulation (GDPR) (EU) 2016.

Fair processing conditions

Schedule 2 of the Data Protection Act lays down six conditions, at least one of which must be met, in order for any use of personal data to be fair. These are (in brief):

- With consent of the Data Subject
- If it is necessary for a contract involving the Data Subject
- To meet a legal obligation
- To protect the Data Subject's 'vital interests'
- In connection with government or other public functions
- In the Data Controller's 'legitimate interests' provided the Data Subject's interests are not infringed

Subject access

Individuals have a right to know what information is being held about them. The basic provision is that, in response to a valid request (including the fee, if required), the Data Controller must provide a permanent, intelligible copy of all the personal data about that Data Subject held at the time the application was made. The Data Controller may negotiate with the Data Subject to provide a more limited range of data (or may choose to provide more), and certain data may be withheld, especially if this is likely to cause harm or distress to a person. This also includes some third-party material, especially if any duty of confidentiality is owed to the third party, and limited amounts of other material. ("Third Party" means either that the data is about someone else, or someone else is the source.)