DATA PROTECTION POLICY

1 Introduction

1.1 We hold personal data about our customers, apprentices, employees, sub-contractors, suppliers and other individuals for a variety of business purposes.

1.2 We take seriously our obligations under the General Data Protection Regulation (GDPR) and all other relevant regulation and legislation in relation to the personal data we hold.

1.3 This policy sets out how we seek to protect personal data and ensure staff understand the rules governing their use of personal data to which they have access to during their work. In particular, this policy requires staff to ensure that the DPCO should be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

2 Definitions

2.1 It is important that you understand the following terms:

2.1.1 Business purposes—the purposes for which personal data may be used by us, e.g. creating and administering customer accounts, personnel, administrative, financial, regulatory, payroll and business development purposes. These include the following:

(a) **creating, and managing our contracts and accounts with our customers**

(b) **contacting customers** for reasons related to the services/work they have requested or to provide information they have requested

(c) contacting customers to notify them of any changes to our services that may affect them

(d) **contacting/following up potential customer enquiries** relating to the potential services/work they have requested

(e) invoicing for and collecting payments due for services provided to customers

(f) collecting overdue payments

(g) compliance with our legal, regulatory and corporate governance obligations and good practice

(h) gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests

(i) ensuring business policies are adhered to (such as policies covering email and internet use)

(j) operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting

(k) investigating complaints and resolving disputes

(l) checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments

(m) monitoring staff conduct, disciplinary matters

(n) improving services

(o) **following up leads and** marketing our business

2.1.2 Personal data—information relating to identifiable individuals, such as customers, alternative contacts, suppliers, marketing contacts, job applicants, current and former employees, agency, contract and other staff including sub-contractors. Personal data we gather may include: individuals' contact details, financial and payment details including NI number, UTR number, legal business entity, i.e. sole trader, partnership, limited co. company number (where applicable), details of education, qualifications and skills, marital status, nationality, job title, and CV.

2.1.3 Sensitive personal data—personal data about an individual's racial or ethnic origin, sexual orientation, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, CCTV images and any other biometric data —any use of sensitive personal data should be strictly controlled in accordance with this policy.

3 Scope

3.1 This policy applies to all members of staff. You must be familiar with this policy and comply with its terms.

3.2 We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

4 Who is responsible for this policy?

4.1 The Proprietor of the business has overall responsibility for this policy and for ensuring this policy is adhered to by all staff.

5 Legal responsibilities

5.1 The GDPR imposes requirements that:

5.1.1 we only hold data if we have a lawful basis for doing so, for example, where we have a contract with a customer, to administer the customer's account and provide the services the customer requires, to comply with our legal obligations, if we have a genuine and legitimate business interest in processing that information or we have the consent of the person to whom the data relates. This also relates to any sub-contractors that conduct work on behalf of Swell Campers & Bespoke Metal Work

5.1.2 we keep that data confidential and secure

5.1.3 we use it only for authorised purpose(s)

5.1.4 any data we hold is:

(a) adequate

(b) relevant

(c) not excessive

(d) accurate, and

(e) up-to-date

5.1.5 we do not keep data for longer than is necessary

6 Our procedures

6.1 Fair and lawful processing – Privacy Notices

6.1.1 We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the processing is:

(a) necessary to perform legal obligations or exercise legal rights, or

(b) otherwise in our legitimate interests and does not unduly prejudice the individual's privacy

In most cases this provision will apply to routine business data processing activities for our business purposes.

6.1.2 Our Privacy Notice is a notice to customers on data protection. The notice:

(a) sets out the purposes for which we hold personal data on customers (i.e. for the provision of legal services and related purposes including legal and regulatory compliance)

(b) highlights that we may be required to give information to third parties such as law enforcement agencies or need to share it with suppliers of materials, goods, trades, local councils' planning and/or building control departments, service providers such as insurers, credit reference agencies, debt collection agents and payroll providers, and

(c) provides that individuals have a right of access to the personal data that we hold about them.

6.1.3 Our Privacy Notice needs to be given to the customer at the first point of contact. Our website will direct customers to our Privacy Notice when they make an enquiry on-line. If a customer/potential customer, makes an enquiry direct with any member of staff, be it face to face or via email, then you must give them a copy of our Privacy Notice at that time. If

enquiries are made by telephone, you will need to inform them that we take the privacy of their data seriously and advise them that they can view our Privacy Notice on-line or we can send it to them by post or email.

6.2 Sensitive personal data

6.2.1 In almost all cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

6.3 Accuracy and relevance

6.3.1 We will ensure that any personal data we process is accurate, adequate, relevant and not excessive given the purpose for which it was obtained. We will not process personal data obtained for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

6.3.2 Individuals may ask that we correct inaccurate personal data relating to them and we need to respond to them within one month. If any person makes a request to correct inaccurate information, you must inform the DPCO immediately giving details of the request. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and pass this on to the DPCO when you report that the request has been made.

6.4 Right to stop direct marketing

6.4.1 As a company, we may on occasions post leaflets through doors. Should we receive a request from an individual that we do not to use their personal data for direct marketing purposes, the Proprietor of the business **must be made aware** about any such request.

6.4.2 Do not send direct marketing material to someone electronically (e.g. via email) unless the person has given their consent to this. You will need to follow industry guidance on following up on people who have made enquiries or asked for an estimate from us.

6.4.3 Please contact the Proprietor for advice on direct marketing before starting any new direct marketing activity.

6.5 Right of access to personal data – subject access requests

6.5.1 Please note that under the Data Protection regulations, individuals are entitled (subject to certain exceptions) to request access to information held about them.

6.5.2 If you receive a subject access request, you should refer that request immediately to the Proprietor. We may ask you to help us comply with those requests.

6.5.3 Please contact DPCO if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

6.6 Right to be forgotten or to restrict use of personal data

6.6.1 Please note that under the Data Protection regulations, individuals are entitled (subject to certain exceptions) to request that we restrict how we use the personal information we hold about them or that we delete it altogether.

6.6.2 If you receive a request of this kind, you should refer that request immediately to the DPCO. We may ask you to help us comply with those requests.

6.7 Your personal data

6.7.1 You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required, e.g. if your personal circumstances change then please inform the DPCO so that they can update your records.

6.8 Data security

6.8.1 You must keep personal data secure against loss or misuse. This means you should comply with our security guidelines and policies set out in the *Information Security Schedule below*.

6.8.2 Where other organisations process personal data as a service on our behalf (e.g. accountants, insurance), the Proprietor will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

6.9 Data retention

6.9.1 We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our Data retention guidelines.

6.10 Transferring data internationally

6.10.1 There are restrictions on international transfers of personal data. You must not transfer personal data internationally at all without first consulting the Proprietor

7 Reporting breaches

7.1 All members of staff have an obligation to report actual or potential data protection compliance and data security failures. This allows us to:

7.1.1 investigate the failure and take remedial steps if necessary

7.1.2 maintain a register of compliance failures

7.1.3 notify the regulatory authorities if we are required to do where any compliance failures are material either in their own right or as part of a pattern of failures.

7.2 If you suspect or become aware of any data security breach or that we have failed to do something which may be a breach of our data compliance obligations, you should report these facts or your suspicions immediately to the DPCO.

8 Training

8.1 All staff are provided with training of this policy and have access to the current policy. New employees will receive training as part of the induction process. Further training will be provided whenever there is a substantial change in the law or our policy and procedure.

8.2 Training will cover:

8.2.1 the law relating to data protection

8.2.2 our data protection and related policies and procedures

8.3 Completion of training is compulsory.

8.4 The Proprietor will continually monitor training needs but if you feel that you need further training on any aspect of the relevant law or our data protection policy or procedures, please contact the Proprietor .

9 Monitoring

9.1 Everyone must observe this policy. The Proprietor will take steps to ensure it is being adhered to.

9.2 The Proprietor will review this policy from time to time, to ensure it remains fit for purpose and compliant with the applicable legislation.

10 Consequences of failing to comply

10.1 We take compliance with this policy very seriously.

10.2 Failure to comply puts both you and the business at risk.

10.3 The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal.

10.4 If you have any questions or concerns about anything in this policy, do not hesitate to contact the Proprietor.

INFORMATION SECURITY SCHEDULE

1 Introduction

1.1 We are committed to high standards of document and information management and security and treat confidentiality and data security seriously.

1.2 One of the purposes of this policy is to:

1.2.1 protect against potential breaches of confidentiality and failures of integrity or availability of information

1.2.2 ensure our information assets and IT facilities are protected against damage, loss or misuse

1.2.3 ensure all staff are aware of and comply with UK law and our own procedures applying to the processing of data

1.2.4 increase awareness and understanding in the business of the requirements for information security and the responsibility of staff to protect information they handle

1.3 All PC's used to support the business must have anti-virus software activated. There are regular security and software updates. All members of staff must restart their PC's at least weekly to finish installing updates.

2 Our procedures

2.1 Information management

2.1.1 Records and information are owned by the business and not by any individual or team.

2.1.2 Keeping accurate and up-to-date records is an integral part of all business activities.

2.1.3 Complete and accurate records must be securely stored in the appropriate locations and be easily identifiable and accessible to those who need to see them. This means:

(a) files must be kept in accordance with our normal file management protocols and must be kept organised and up-to-date

(b) substantive matter related emails and notes of telephone or other conversations must be placed on file and must not be stored solely in personal mailboxes

(c) files must not be removed from the office except as permitted under this policy

2.1.4 Information includes information stored anywhere on our IT system, as well as paper records and CCTV images.

2.1.5 Information will be held only as long as required and disposed of in accordance with our Information retention and destruction guidelines.

2.1.6 All staff must ensure that any information and data gathered is accurate and, where appropriate, kept up-to-date.

2.2 Human resources information

2.2.1 Given the internal confidentiality and sensitivity of personnel files, access to such information is limited to the Proprietor of the Business and HR/Finance, except as provided in individual roles, no other staff are authorised to access that information.

2.2.2 Any staff member in a management or supervisory role must keep personnel information confidential.

2.2.3 Subject to the provisions of the GDPR and associated codes of conduct, staff may ask to see their personnel files at any time by request to the Proprietor.

2.3 Access to offices and files

2.3.1 At the end of each day, or when desks are unoccupied, all files, backup systems and devices containing confidential information must be securely locked away or access disabled in case of temporary absence.

2.3.2 Customers and visitors should never be left alone in areas where they could have access to confidential information.

2.4 Computers and IT

2.4.1 Computers must be password protected and those passwords must be secure. Passwords should not be written down or given to others.

2.4.2 Computers and other devices should be locked when not in use to minimise the risk of accidental data loss or disclosure.

2.4.3 The use of memory sticks and other removable media is prohibited with the exception of the Proprietor of the Business. No confidential information is to be copied onto floppy disk, removable hard drive, CD or DVD or memory stick/thumb drive without the express permission of the Proprietor.

2.5 Backup of data

2.5.1 All electronic data must be securely backed up at the end of each working day.

2.6 Communication and transfer

2.6.1 Business related information must not be removed from our offices without permission from the Proprietor.

2.6.2 Personal electronic devises should not be attached to or used to log into company networks or email systems.

2.6.3 Postal, fax and email addresses and numbers should be checked carefully before information is sent to them. Particular care should be taken with email addresses where auto-complete features may have inserted incorrect addresses.

2.6.4 All sensitive or particularly confidential information should be encrypted before being sent by email, or be sent by recorded delivery.

2.6.5 Sensitive or particularly confidential information should not be sent by fax.

2.7 Personal email and cloud storage accounts

2.7.1 Do not use a personal email account or cloud storage account for work purposes. Do not plug in or attach your personal devices to the business's IT system – charge from a wall plug socket.

3 IT system management and development

3.1 Our IT systems are managed by the Proprietor of the Business with support from suitably qualified consultants as and when necessary.

3.2 The Finance Controller is responsible for the management of user accounts and will implement procedures to ensure:

3.2.1 appropriate permissions are set for different types of user accounts, e.g. administration, standard or guest

3.2.2 all members of staff have the correct type of user account

3.2.3 users run with a minimal set of permissions whenever possible

3.2.4 user accounts are suspended or deleted promptly where required, e.g. if a member of staff leaves the firm

3.3 New IT systems, or upgrades to existing systems, must be authorised by *the* Proprietor and the authorisation process must take account of security requirements.

4 Reporting breaches

4.1 If you suspect or become aware of any data security breach or that we have failed to do something which may be a breach of our data compliance obligations, you should report these facts or your suspicions immediately to the Proprietor.