James Glancy Design Ltd.

Company Data Protection Policy 2018

Review Summary

Next Review May 2019

Review Number	Brief Details of Review	Person Carrying out Review	Date
01	First Issue	Lydia Alexis-Webb	May 2018
02	Added CCTV Monitoring	Lydia Alexis-Webb	July 2018

Introduction

We hold personal data about our employees, clients, suppliers, subcontractors and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work

Definitions

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, service delivery, payroll and business development purposes. *Business purposes include the following:* - *Compliance with our legal, regulatory and corporate governance obligations and good practice* - *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests* - *Ensuring business policies are adhered to (such as policies covering email and internet use)* - *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting and checking* - *Investigating complaints* - *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments* - *Monitoring staff conduct, disciplinary matters* - *Marketing our business* - *Improving services*

Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. *Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.*
Sensitive personal data	*Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, allergies, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.*

Scope

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

This policy supplements our other policies relating to internet and email use. 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.

Who is responsible for this policy?

We are under no obligation and therefore are choosing to not appoint a data protection officer; however, we do have a team of employees educated and informed about GDPR and we are working together to enforce the law.

Our procedures

Fair and lawful processing

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 individual whose details we are processing has consented to this happening.

Responsibilities:

- Reviewing all data protection procedures and policies on a regular basis

- Arranging data protection training and advice for all staff members and those included in this policy

- Answering questions on data protection from staff, directors and other stakeholders

- Responding to individuals such as clients and employees who wish to know which data is being held on them by James Glancy Design Ltd

- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

Responsibilities of Office Employees

- Approving data protection statements attached to emails and other marketing copy

- Addressing data protection queries from clients, target audiences or media outlets

- Working to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy
- Aim to ensure all systems, services, software and equipment meet acceptable security standards
- Co-ordinate with our IT Company to ensure that security hardware and software is checked and scanned regularly to ensure it is functioning properly

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Our Terms of Business contains a Privacy Notice to clients on data protection.

The notice:

- Sets out the purposes for which we hold personal data on customers and employees
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
- Provides that customers, employees, subcontractors and tenants have a right of access to the personal data that we hold about them

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's *explicit, written* 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.

Accuracy and relevance

We will endeavour to 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 one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform one of the employees using the email address mentioned on page 8.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform one of the employees one of the employees using the email address mentioned on page 8 so that they can update your records.

Data security

You must keep personal data secure against loss or misuse.
Please be aware other organisations process personal data as a service on our behalf, for the purposes of payroll and auto enrol pension.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks *if permitted* must be locked away securely when they are not being used
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

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.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting one of the employees using the email address mentioned on page 8.

Subject access requests

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them.

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

Please contact the one of the employees using the email address mentioned on page 8 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.

Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify one of the employees using the email address mentioned on page 8 about any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

Please contact one of the employees using the email address mentioned on page 8 for advice on direct marketing before starting any new direct marketing activity.

Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

GDPR provisions

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

What information is being collected?	Subcontractors: Name, phone number, address, email address, bank account details, CV, certification, driving license, insurance documents, UTR, NI number Employees: Name, phone number, address, email address, bank account details, certification, driving license, National Insurance number, past employment information, passport, personal tax codes Businesses: Name, phone number, email address Suppliers: Name, phone number, email address Tenants: Name, phone number, email address, bank details CCTV Monitoring: video images of individuals entering and leaving our main office
Who is collecting it?	Office Administration Staff, Head of Production, Production Floor Manager, Electrical Staff
How is it collected?	Subcontractors: We request the information from you or you provide the information in the form of your CV or Pre-Qualification Questionnaire Employees: We request the information from you upon the start of your employment Businesses: Supplied by the individual or by their employer Tenants: We request the information from you upon

	the start of your tenancy CCTV Monitoring: through CCTV camera installed within our office and at the entrances
Why is it being collected?	Subcontractors: To contact them regarding seasonal work and while the work is taking place Employees: For payroll, pension scheme, to be contacted if working out of the office or on site, to verify ability to work, Businesses: To contact regarding past, current and future business Tenants: To contact you during your tenancy and for invoicing purposes CCTV Monitoring: for security reasons, to monitor unauthorised/unnecessary access to our building, to ensure correct procedure is followed
How will it be used?	Subcontractors: Contacting you for and about work through emails, text messages, phone calls and WhatsApp messages, accounts department to pay you, certification is sent to clients to meet health and safety requirements Employees: To contact if working on site or out of hours through phone calls, text and WhatsApp messages, email addresses for payslips and pension scheme, certification is sent to clients to meet health and safety requirements Businesses: To contact regarding past, current or future business via phone calls or emails Tenants: To compile contracts, contact via email or phone about queries, for invoicing purposes CCTV Monitoring: It will only be used/accessed if one of the above mentioned happens and people need to be identified
Who will it be shared with?	Subcontractors: Phone numbers will be shared with other team members, truck and access delivery drivers, centre security, site/client contacts. Email addresses will be shared with accounts department, and with other company employees Employees: phone numbers occasionally shared with subcontractors and other employees, Businesses: email addresses and business numbers shared with other company employees if necessary to contact you regarding works being carried out Tenants: the accounts department CCTV Monitoring: information will only be shared if necessary, with relevant managers, directors or in certain cases – law enforcement
Identity and contact details of any data controllers	jgdhelp@jamesglancydesign.com
Details of transfers to third party and safeguards	Clear instructions are given as to how data can be used
Retention period	Data is retained for as long as we perceive to be necessary Accounting and employee records need to be retained for 6 years

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

We will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International data transfers

No data may be transferred outside of the EEA without first discussing it with the data protection officer. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

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

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

Please refer to our Compliance Failure Policy for our reporting procedure.

Monitoring

Everyone must observe this policy. Appointed employees will monitor this policy regularly to make sure it is being adhered to by other members of staff.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

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. A solicitor in breach of Data Protection responsibility under the law or the Code of Conduct may be struck off.

If you have any questions or concerns about anything in this policy, do not hesitate to contact one the employees using the email address mentioned on page 8.