Charles Design

Privacy Policy

Last Modified – April 2018

Introduction:

Charles Design are dedicated to ensuring that all information stored about clients and individuals are kept as secure as possible at all times and stored in accordance to the General Data Protection Regulations 2018.

The Company policy is to respect the privacy of clients and individuals and to maintain compliance with the General Data Protection Regulations (GDPR). Personal data related to client and individuals will be protected.

The company have obligations imposed on it by the General Data Protection Regulation (GDPR) to ensure that all information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully. We must ensure that our policies are written in a clear, plain way that everyone will understand.

This policy outlines the information we collect and how we use it.

Data Protection Officer:

Our Data Protection Officer is Richard Maskery. For further information, subject access requests or complaints please contact richard@charlesdesign.co.uk.

GDPR Principles:

In order to comply with its obligations, Charles Design, undertakes to adhere to the eight principles:

1) Process personal data fairly and lawfully.

We will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

2) Process the data for the specific and lawful purpose for which the data is collected and shall not further process the data in a manner incompatible with this purpose.

We will ensure that the reason for which the data is originally collected is the only reason for which it is process, unless the individual is informed of any additional processing before it takes place.

3) Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.

We will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If individuals give any irrelevant data, it will be destroyed immediately.

4) Keep personal data accurate and, where necessary, up to date.

We will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify us if, for example, a change in circumstances means that the data needs to be updated. It is the responsibility of the company to ensure that any notification regarding the change is noted and acted on.

5) Only keep personal data for as long as is necessary.

We undertake not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means we will undertake a regular review of the information held and implement a weeding process.

We will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

6) Process personal data in accordance with the rights of the data subject under the legislation.

Individuals have various rights under the legislation including a right to:

- be told the nature of the information we hold and any parties to whom this may be disclosed.
- prevent processing likely to cause damage or distress.
- prevent processing for purposes of direct marketing.
- be informed about the mechanics of any automated decision taking process that will significantly affect them.
- not have significant decisions that will affect them taken solely by automated process.
- take action to rectify, block, erase or destroy inaccurate data.
- sue for compensation if they suffer damage by any contravention of the legislation.
- request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened. We will only process personal data in accordance with individuals' rights.

7) Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

The Data Protection Officer is responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

We will ensure that all personal data is accessible only to those who have a valid reason for using it.

We will have in place appropriate security measures:

- keeping all personal data in a lockable cabinet with key-controlled access.
- password protecting personal data held electronically.
- ensuring that PC screens are not left unattended without a password protected screen-saver being used.

In addition, we will put in place appropriate measures for the deletion of personal data - manual records will be shredded or disposed of as 'confidential waste'. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed.

8) Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

We will not transfer data to such territories without the explicit consent of the individual.

This also applies to publishing information on the Internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA - so we will always seek the consent of individuals before placing any personal data (including photographs) on its website or social media sites.

The information you provide us:

When you engage our services, we input your company details into our customer relationship management database (CRM). These details include: name of company, address, contact details. These details are retained by the company for legitimate interests. Only authorised employees, workers and sub-contractors of the company have access to our CRM system.

Your details will be stored on our accounting system, Xero for invoicing and accounting purposes. The data is limited to name of company, address of company and contact name. The directors of the company and the company accountant have access to this data. This system is password protected.

Our company accountant has a separate data policy which you may request from our Data Protection Officer.

Website enquiries:

If you fill in our contact form via our website, your information will be emailed to our team. Your details will only be used to contact you for that particular enquiry and will not be added to any marketing list without your consent.

Social Media:

We do not ask you to provide us with any personal data in order for you to view our social media platforms.

If you provide us with your customer contact details for marketing purposes:

If you engage our services in order for us to carry out marketing campaigns on your behalf, we ask that you only provide us with email addresses on an excel spreadsheet (unless you require the marketing campaign to be personalised).

It is your responsibility to ensure that you have explicit consent to send out marketing literature to that individual prior to sending the information to Charles Design. Please ensure that you only send data to us where consent has been gained. It is also your responsibility to inform your client that you have passed their information on to a third party.

We do not retain the excel spreadsheet, we securely erase the data once a campaign has been successfully sent.

We do not pass this data onto any third parties.

We use a third party system, which sends out client marketing emails to the contacts provided by the client. This system records how successful a campaign has been and we aim to keep this information for a period of 6 months in order to provide you with this data.

Email password information:

We do not store password information for emails. If you ask us to re-set passwords we will do so and erase the record of the new password. It is your responsibility to change your email passwords on a regular basis and to retain them.

E-Commerce:

We do not store payment details such as credit/debit cards. We use a trusted third party.

We can access your customer's data via an administration system which is password protected.

Information Security:

Only authorised employees of the company will have access to personal data. All electronic data is password protected and is only accessible in our office environment.

We have authentication systems in place, WIFI logins and all employees, workers and sub-contractors have their own logins and passwords. All passwords are changed regularly.

We ask all employees, workers and sub-contractors to sign a confidentially clause.

We back up data securely.

We review our security regularly and take all necessary cyber precautions.

Storage:

We delete customer data immediately from our web hosting server following a cancellation of services. This will include the e-commerce data.

Third party:

We do not pass your data onto any third party, other than detailed above.

Transparency and Choice:

You may at any time contact us and ask what information we hold on you. You may ask us to update this information if it is incorrect, which we will strive to do as quickly as possible.

You have the right to be forgotten and may at any time request that we delete your data. Please be aware that this request may be refused due to legal requirements.

Changes:

Our policy may change as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

Compliance:

We regularly review this policy to ensure that it complies with current legislation.