Privacy Policy

**Introduction**

This document is a statement of the Company’s Privacy policy and is provided with the intention to comply with your right to be informed under the General Data Protection Regulation. This policy applies to anyone that we interact with, including employees, customers and potential customers.

**Who are we?**

We trade as Addpace Classics Limited for reasons of simplicity when this Policy refers to the ‘company’, ‘we’ and ‘us’, this means: - Addpace Classics Ltd / The Bristol

**Legal Obligations**

There are several reasons why we may collect and process your personal data as defined under data protection law.

These include Consent, Contractual obligations, Legal compliance and Legitimate interest.

**Consent**

On occasions we can collect and process your data with your consent.

*For example, you may ask us to keep you informed of any special offers etc.*

**Contractual Obligations**

In certain circumstances, we need your personal data to comply with our contractual obligations.

*For example, when you place an order with us we will collect your address details and pass them to our courier to deliver your purchase. We will also forward the invoice to you, electronically.*

**Legal Compliance**

If the law requires us to, we may need to collect and process your data

For example, we can pass on details of people involved in fraud or other criminal activity a

*For example, we can pass on details of people involved in fraud or other criminal activity affecting the Companies(s) to Law Enforcement bodies.*

**Legitimate Interest**

In specific situations, we require your data to pursue our legitimate interests in a way which might reasonably be expected as part of running our business and which does not materially impact on your rights, freedom or interests.

*For example, we may use your purchase history to send you or make available personalised offers.
We will also combine the purchasing history of many customers to identify trends and ensure we can keep up with demand or develop new products or services.*

This policy applies to the holding and processing of personal data in any form, whether manually or electronically and includes all human resource activity and functions of the Company.

It applies to the personal data of current and past employees, apprentices, full time, temporary and casual workers, job applicants, interns, volunteers and contractors (*individuals*).

The Bristol, is committed to ensuring that personal data, including special categories of personal data and data about criminal offences is processed in accordance with the GDPR and any related UK legislation, and that all individuals abide by the requirements of this and any other related policies. The Company understands that it is accountable for the data processing of personal data and that any third party that processes personal data on behalf of the Company undertakes such measures as required to fulfil the Company’s obligations and commitments to protecting personal data.

The Company has appointed a Data Protection Officer who is responsible for data protection compliance within the Company. This person has responsibility for the processing and controlling of personal data held by the Company, auditing and reviewing of the data protection processes, systems and procedures and ensuring that all data is protected.
The Data Protection Officer can be contacted by calling 01454 620000 or via Email to henry@bristolgolfclub.co.uk.

**Definitions**

***Personal Data:*** is any information that relates to an individual who can be directly or indirectly identified from that information. This could be the individual’s name, any identification number, code or information that could lead to identifying them or their location.

***Data Processing:*** is any use that is made of the personal data, whether it is collecting, storing, amending, recording, disclosing by any means or destroying the personal data. Holding data, of itself, is data processing.

***Special Categories of Personal Data:*** means data about an individual’s health, race, ethnic origin, sex life, sexual orientation, religion, philosophical beliefs, political opinions, trade union membership, genetic and biometric data.

***Criminal Offence Data:***is data about an individual’s criminal convictions, offences, any allegations or proceedings.

**How we will use your personal information for business activities: -**

* to administer and manage our relationship with you, including to set up and maintain your account facility;
* to process orders from you for goods and services;
* to deal with any enquiries we receive from you;
* for the purposes of any corrective action (including a product recall) which may be required in respect of any of the products we supply to you;
* to comply with applicable laws, regulations and rules;
* to provide you with details of our product ranges, services and promotions;
* to notify you of changes to what we do;
* to carry out checks with credit reference agencies from time to time (for example, upon completion of a trade account application form or a request to amend a credit limit); and
* for the purposes of recovery of a debt in case of non-payment.

We are the controller, and we are also the processor of this information. This data has been gathered with your consent from your previous giving of this information, your receipt of Marketing communications from us and/or your purchase or interest in our products and services.

You can email our Data Protection Officer at henry@bristolgolfclub.co.uk or call 01454 620000.

Your data will be used to continue to provide you with details and information relating to the products and services offered by The Bristol. This is done on the basis of your continued consent. Should you withdraw your consent, your data will then be retained and added to our ‘Unsubscribed User’ lists so that we are aware to no longer provide you with details and information relating to our products and services.

Your data will be kept until such time that you request you no longer wish for us to provide you with details and information relating to our products and services and for a further period thereafter of 6 years. This period has been set for the protection of our organisation in the event of any complaint or claim for breach of contract or professional negligence claim. If such a claim has been filed, the data will be retained for a period of 6 years following resolution of that claim and for 6 years following the resolution of any further claims. This period has been determined for the protection of the organisation in the event any professional negligence or breach of contract claims in the event we use representation to defend any claims.

**Data Protection Principles**

All personal data obtained and held by the Company will be processed by the following Data Protection Principles. The Company will:

* process personal data fairly, lawfully and in a transparent manner,
* obtain personal data only for specific, explicit and legitimate purposes,
* process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing,
* keep accurate personal data and take reasonable steps to correct inaccurate personal data or delete it without delay
* only keep personal data for the duration of time that it is necessary for processing and for no longer than is necessary for the stated purpose,

* ensure that personal data is held securely and is protected from unauthorised or unlawful processing, accidental loss, destruction or damage,
* ensure that any personal data that is transferred to any country outside the European Economic Area (*EEA*) will be on the basis of the required GDPR procedures for international transferring of personal data.

**Individual Data Protection Rights**

The Company recognises that individuals have data protection rights and commits that personal data will be processed according to these rights. Individuals have the right:

* to be informed about their data protection rights
* to be informed about the reasons for processing data, the legal basis for which the data is processed, how the Company uses and protects the data, the source of the information if it has not been provided by the individual and the periods of time that the information will be held,
* to make a subject access request,
* to have any inaccuracies in the information corrected (rectified) promptly,
* to have information deleted or erased,
* to stop the processing of data if the individual’s interests override the Company’s legitimate grounds for processing the data (where this is/was the reason for processing the data)
* to stop the processing of data for a period of time where the data is inaccurate or where there is a dispute about whether an individual’s interests override the Company’s legitimate grounds for processing the data.
* to stop the processing or require the erasing of data where the processing is unlawful
* to complain to the Information Commissioner if the individual thinks that the Company has not complied with the individual’s data protection rights
* to be informed to whom the individual’s data may be disclosed, if such recipients are located inside or outside the EEA and the safeguards that apply to such transfers,
* to know whether the Company uses any automated decision-making or profiling of personal data and the logical basis of such decision-making.

**Company Actions to Implement Data Protection**

The Company has appointed one or more individuals to be responsible for implementing the Company’s duties and responsibilities for data protection as detailed above.

The Company will keep records of, and account for, the personal data it has collected and holds, where the data has been obtained, with whom it is, or will be, shared and the processing of personal data that it undertakes.

The Company will inform all appropriate individuals of their data protection rights under the GDPR and this policy as required and by providing a **Privacy Notice** if appropriate.

The Company will train individuals on the importance of protection of personal data and how to implement the Company’s duties and responsibilities in their job and to maintain confidentiality of personal data.

The Company will review its personal data handling, carry out risk assessment and introduce processes and procedures to minimise the risk of data breaches or incorrect handling of personal data. To this end, the Company will put in place relevant internal policies, procedures, process and controls to protect personal data from loss, accidental destruction, misuse or disclosure. This will include policies and procedures to make sure that personal data is not accessed by anyone except those individuals who have the required permission and authority to do so in the proper performance of their duties for the Company.

In the event that the Company decides to use a third party or organisation to process personal data on its behalf, it will implement appropriate standards, policies and procedures to do so, which will include written agreements with the third party which will include commitments of confidentiality and security and the requirement to implement appropriate technical and other measures to ensure the security of the data.

The Company understands and will implement its responsibilities to obtain the consent of individuals for obtaining, holding, using and sharing their personal data. Further, the Company understands that such consent must be freely given, informed, specific and unambiguous. It also recognises that individuals have the right to withdraw such consent at any time.

The Company has put in place and will maintain the required processes and procedures for detecting, investigating and reporting suspected or actual personal data breaches and that it must report serious breaches that could or will cause significant harm to affected individuals to the Information Commissioner. The Company understands the consequences of such data breaches.

**Subject Access Requests**

Individuals have the right to make a subject access request which is a request to access the data the Company holds on that individual. If an individual makes a subject access request, the Company will provide the following information:

* A copy of the personal data that the Company holds and is processing,
* The categories of personal data that are processed and why it is processed,
* The source of the personal data if it has not been provided by the individual
* The period of time that the personal data is or will be stored,
* The individual’s right to correct any inaccuracy (rectification) or delete any of the data (erasure) or to restrict or object to the processing,
* The right to complain to the Information Commissioner if the individual thinks the Company has failed to comply with their data protection rights,
* Whether or not the Company uses automated decision-making in the processing of the data and if so, the logic underlying such automated decision-making.

To make a subject access request, the individual should contact the Data Protection Officer by calling 01454 620000 or emailing henry@bristolgolfclub.co.uk providing full details of the request. In some circumstances, the Company may request proof of identification before processing a request. If this is the case, the individual will be informed of the details of the documents required.

The Company will respond to a request without delay. Subject to any legally permitted exceptions the Company will respond within one month of a request, but this may be extended to three months in total if there are a number of requests or they are complex. If this is the case, the Company will write to the individual within one month of receiving the request to inform them that the response will be within a maximum of a three-month period.

The Company will not charge for responding to a subject access request unless the request is manifestly unfounded or excessive or there is a request for further, duplicate copies to be sent to persons other than the individual making the request. Further, where a request is manifestly unfounded or excessive, the Company is not required to respond to it, or may respond to it but charge a fee related to the administrative cost of responding to the request. Where this is the case, the Company will inform the individual making the request of the approach it intends to take regarding the request.

Where an individual believes that the data held and processed by the Company is inaccurate, they must inform the Company as soon as possible. The Company will rectify the information without delay.

**Data Breach**

If the Company discovers that a data breach has taken place and the breach is such that it is likely to risk the rights and freedoms of individuals, such breach will be reported to the Information Commissioner within 72 hours of the Company becoming aware of the breach. It is possible that it might be necessary to report any such breach in several stages or instalments. A record of all breaches will be maintained.

If a data breach is likely to result in a high risk to the rights and freedoms of individuals, the Company will inform the individuals who are affected.

**International Data Transfer**

Personal data is also transferred to countries outside the EEA for the processing of payroll to individuals based within the relevant country. As we also trade with customers outside of the EEA we will hold and process data, adopting the same protection principals as detailed above.

**Disclosing Data**

From time-to-time, it may or will be necessary for the Company to disclose personal data to other persons or organisations. Any such disclosure will only be made where this must be made for the required purpose. Any such disclosure could be for a variety of reasons which may include:

* Statutory Pay requirements
* HR management and administration
* Employee benefits administration where this service is provided by a third party
* Establishing where reasonable adjustments are required for a disabled employee
* Pension and insurance plan administration
* Employee health data to fulfil Company obligations regarding health and safety

**Training**

The Company will provide individuals with training about data protection, confidentiality and any actions they should take in the event of a data breach. This information will be given to individuals during Company induction and Company training sessions.

All individuals who are required to use the Company’s computer systems, to implement this policy, respond to subject access requests or have access to confidential and personal data will be trained to protect personal data to ensure that they understand their duties and responsibilities. They will be trained in their personal responsibilities and the consequences for them and the Company for any data breaches or personal failures to uphold the Company’s policies and procedures.

**Employees’ responsibilities for Data Protection**

Every employee has a personal responsibility to help to keep personal data safe and secure and to comply with the requirements of the GDPR. All employees must uphold the requirements placed on the Company for data protection. It is the responsibility of every employee to protect any personal data with which they come into contact, they hold, or for which they are responsible on behalf or the Company. In particular you must comply with and implement the provisions of the Company’s Privacy Notices and Data Protection Policy together with any other policies and procedures that the Company may put in place to protect any data and personal data in particular.

Where an individual has access to personal data, they must:

* Keep data secure by using the password protection and the secure file storage provided by the Company at all times,
* Never to abuse passwords by disclosing passwords to others, especially to those who are not authorised to have access to such passwords or the information which can be accessed using the password,
* Only access such information that they are authorised to access and only for the purpose for which such authorised access was granted,
* Never to disclose personal data to others who are not authorised to have access to such data,
* Ensure that all written information or files (whether electronic or paper based) containing confidential information are kept securely and cannot be seen or accessed by individuals who do not have the authority to read or access them,
* Ensure that all personal data that is entered into the Company records is accurate,
* Never to keep personal data on transportable data storage devices, such as laptops, USB sticks, portable back-up disks or in “cloud” based storage without the express authority of the Company. Where such authority is granted, any such data must be stored in a secure manner, as prescribed by the Company but in any event must be encrypted. The physical security of the portable devices must also be protected to ensure that they cannot be stolen.
* Never to remove personal data or any portable device holding personal data from the Company’s premises without the express authority of the Company and if so authorised to ensure that any data is stored securely as prescribed by the Company and is encrypted.

Any employee who is found to have failed to apply the Company’s Data Protection Policy or in any way prejudiced, lost, revealed or disclosed any personal data to any unauthorised person or organisation will be in breach of Company policy and will be subject to disciplinary action, which may, dependent on the nature of the offence, be regarded as gross misconduct and subject to dismissal without notice. Any such disclosure may also be treated as a criminal offence.