Data Protection Policy

Introduction

The Club is committed to being transparent about how it collects and uses the personal data of individuals, and to meeting its data protection obligations. This policy sets out the Club's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of members ("member data"), personal data processed for business purposes, as well as the personal data of job applicants, employees, workers, contractors, and former employees ("HR- related personal data").

The Club has not appointed a Data Protection Officer (DPO), as is not required to under GDPR. However the board is responsible for ensuring that the Club complies with its obligations under GDPR. The Club, acting through the Board, is, therefore, the Data Controller for the personal data referred to below. For the purposes of GDPR, the first point of contact with the Board is through the Company Secretary ("the Secretary"). Responsibility for HR related personal data lies with Natwest Mentor who can be contacted at the Club. Requests in relation to HR related data should be forwarded to reception@parsonsgreenclub.com

The **General Manager** has responsibility for member data and can be contacted at gm@parsonsgreenclub.com

Definitions

- 'Personal data' is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.
- 'Special categories of personal data' means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.
- 'Criminal records data' means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

The Club processes personal data in accordance with the following data protection principles:

- The Club processes personal data lawfully, fairly and in a transparent manner.
- The Club collects personal data only for specified, explicit and legitimate purposes.
- The Club processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The Club keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The Club keeps personal data only for the period necessary for processing.
- The Club adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The Club tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its Member and Employee Privacy Policies. It will not process personal data of individuals for other reasons.

Where the Club is relying on legitimate interests as its lawful basis for processing, a Legitimate Interests Assessment (LIA) will be carried out and documented to ensure that the rights of the individual are considered.

Where the Club processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the Club's Employee Privacy Policy.

The Club will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the employment, worker, contractor relationship, or apprenticeship or internship is held in the individual's personnel file in hard copy or electronic format, or both, and on Club systems. The periods for which the Club holds HR related personal data are contained in its Employee Privacy Policy.

Personal data gathered during membership is held by the **General Manager** in both hard copy and electronic formats. The periods for which the Club holds member data are contained in the Member Privacy Policy and data retention schedule.

The Club keeps a record of its processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data. Any requests from members should be immediately forwarded to the General Manager for processing. Employees wishing to exercise their rights in relation to GDPR should contact the Club.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the Club will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers
- for how long his/her personal data is stored (or how that period is decided)
- his/her rights to rectification or erasure of data, or to restrict or object to processing
- his/her right to complain to the Information Commissioner if he/she thinks the Club has failed to comply with his/her data protection rights
- whether or not the Club carries out automated decision-making and the logic involved in any such decision-making.

The Club will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

In some cases, the Club may need to ask for proof of identification before the request can be processed. The Club will inform the individual if it needs to verify his/her identity and the documents it requires.

The Club will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Club processes large amounts of the individual's data, it may respond within three months of the date the request is received. The Club will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, the Club is not obliged to comply with it. Alternatively, the Club can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Club has already responded. If an individual submits a request that is unfounded or

excessive, the Club will notify him/her that this is the case and whether or not it will respond to it.

For further information, please refer to the Subject Access Request procedure.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the Club to:

- rectify inaccurate data
- stop processing or erase data that is no longer necessary for the purposes of processing
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the Club relies on its legitimate interests as a reason for processing data)
- stop processing or erase data if processing is unlawful
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

Where the Club has a legal obligation or overriding legitimate interest for retaining information, it can refuse to comply with a request to erase personal data.

Data security

The Club takes the security of personal data seriously. The Club has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the Club engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Impact assessments

Some of the processing that the Club carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the Club will carry out a Data Protection Impact Assessment to determine the necessity and proportionality of processing. This will include

considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

If the Club discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The Club will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken. The Club will investigate the breach and follow the procedures in accordance with the Data Breach Policy.

International data transfers

The Club will not transfer HR related personal data to countries outside the EEA.

Individual responsibilities

Individuals are responsible for helping the Club keep their personal data up to date.

Individuals should let the Club know if data provided to the Club changes, for example if an individual moves house or changes his/her contact details.

Any requests from members to update their personal data should be forwarded to the General Manager.

Individuals should let the Club know about any requests from members of the public, for example if an individual needs the Club to provide a reference for letting a property.

Individuals should report any breaches or suspected data breaches to the Club by emailing parsonsgreenclub@gmail.com. The Club will then investigate the breach in accordance with the Data Breach Policy.

Individuals may have access to the personal data of other individuals and of our members and clients in the course of their membership, employment, contract, internship or apprenticeship. Where this is the case, the Club relies

on individuals to help meet its data protection obligations to staff, members and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes
- not to disclose data except to individuals (whether inside or outside the Club) who have appropriate authorisation
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction)
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device
- not to store personal data on local drives or on personal devices that are not authorised for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Club's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

The Club will provide some training to all individuals about their data protection responsibilities as part of the induction process.