Pentyrch Bowling Club

Data Protection Policy and Procedures

Introduction

Pentyrch Bowling Club (PBC) needs to collect and use certain types of information about its members and others for administrative purposes. PBC is committed to protecting individuals' rights and privacy and ensuring that any personal information it holds is collected and processed appropriately, that is, fairly, transparently and legally. This policy describes PBC's procedures for achieving that objective.

The Data Protection Act 1998 (DPA) governs the use of information about people (personal data). Personal data can be held on computer or in a manual file. They include names, addresses, phone numbers, emails, minutes of meetings, and photographs. For DPA purposes, PBC is the data controller collectively responsible for processing and using the information it holds. Officers and members of PBC who have access to personal information are expected to read and comply with this policy, which will be updated as necessary in accordance with changes in legislation.

While committed to full compliance with the principles of the DPA, PBC, as a small, not for profit organisation, is exempt from the requirement to register its activities with the Information Commissioner's Office.

A list of definitions of technical terms used in this policy derived from the DPA and supplementary legislation is attached as Appendix A. The Act contains 8 principles for processing personal data. These are listed in Appendix B. The Act also sets out the rights of data subjects, that is people about whom information is held. These are listed in Appendix C.

Collecting data

PBC collects and processes data about members and others with whom it comes into contact. These are normally limited to personal contact information, but may include photographs or, exceptionally, health information which is necessary (and lawful under Article 9(2) of GPDR) to assess or meet members' health or social care needs. PBC will ensure data subjects know what personal data are being collected and why, and that data collected are only used for the purpose stated, are accurate and up to date, and are kept no longer than necessary for the stated purpose.

Correcting data

Individual data subjects have a right to have data corrected if they are inaccurate, to prevent use which is causing them damage or distress, or to stop marketing information being sent to them.

Responsibilities of Data Controller

As a small, not for profit organisation, PBC is the Data Controller legally responsible for complying with the DPA, which means that it determines what purposes personal information it holds will be used for. Its management committee will consider legal requirements and ensure that these are properly implemented, and that criteria and controls are applied appropriately. Specifically, it will ensure that PBC:

- Fully observes conditions regarding the fair collection and use of information,
- Meets its legal obligations and keeps a record of the purposes for which information is used,
- Collects and processes appropriate information only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,
- Ensures the quality ie accuracy of information used and keep it up to date,
- Ensures that the rights of people about whom information is held (as listed in Appendix B) can be fully exercised under the DPA.
- Takes appropriate technical and organisational security measures to safeguard personal information,
- Treats people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
- Maintains clear procedures for responding to requests for information.

Responsibilities of the Data Protection Officer

The Club Secretary serves as the Data Protection Officer responsible for implementing PBC's policy. Assisted by the Membership Secretary, they have overall responsibility for:

- Obtaining consent from data subjects (see below) and explaining their rights,
- Ensuring everyone processing personal information understands that they are responsible for following good data protection practice,
- Ensuring that anyone wanting to make enquiries about handling personal information knows what to do,

- Dealing promptly and courteously with any enquiries about handling personal information and describing clearly how PBC handles personal information.

Consent

When collecting data, PBC will ensure that the data subject:

- Clearly understands why the information is needed and what it will be used for,
- Grants explicit consent, either written or verbal, for data to be processed,
- Is informed of their rights to withdraw consent for data to be stored and processed, to have access to the data about them, and to correct any inaccuracies in it.

Data Storage

Information and records relating to members and others will be stored securely and will only be accessible to authorised individuals for administrative purposes. Information will only be stored for as long as it is needed or is required by statute and will thereafter be deleted. PBC will ensure all personal and organisational data are non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

Data Subject Access Requests

Data subjects have a statutory right of access to data held about them and can expect to be enabled to access data *within one month of that request* (other than in exceptional circumstances), and *free of charge* (other than when the request is excessive or repetitive in which circumstances a modest fee can be charged).

Disclosure

PBC is committed to the lawful and correct treatment of personal information and would not expect to share data with third parties other than when required by law. There are circumstances where the law allows (or even requires) an organisation to disclose data (including sensitive data) without the data subject's consent. These include:

1. Carrying out a legal duty or as authorised by the Secretary of State
2. Protecting vital interests of a Data Subject or other person
3. Where the Data Subject has already made the information public
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights.

Deletion (erasure) of personal data.

Personal data should only be kept for as long as they are needed and securely disposed of once when no longer required. PBC will ensure that this information is confidentially destroyed at the end of the relevant retention period.

Further information

If members of PBC have specific questions about information security and data protection, they are advised to contact the Club Secretary in the first instance. For general information about data protection and the legislation governing it, they should consult The Information Commissioner's website (www.ico.gov.uk).

Appendix A.

Definitions

The Data Protection Act 1998 (DPA) contains the following definitions of technical terms employed in the preceding policy:

Consent – A freely given, specific and informed agreement by a Data Subject (see definition below) to the processing of personal information about them.

Data Controller – The person or legal entity (in this case PBC) which decides what personal information the organisation will hold and how it will be held or used.

Data Protection Act 1998 (DPA) – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person who, on behalf of PBC, is responsible for ensuring that PBC follows its data protection policy and complies with the Data Protection Act 1998 and General Data Protection Regulation 2016.

Data Subject – An individual whose personal information is being held or processed by PBC.

General Data Protection Regulation (EU) 2016 (GPDR)- The regulation which came into force in May 2018 by which the protections offered to data subjects under the DPA and the Human Rights Act 1988 are enhanced and made enforceable.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Personal Information/data – Information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses (whether held on paper or by electronic means). It does not apply to information about organisations, companies and agencies but to named persons only.

Processing **–** Collecting, amending, handling, storing or disclosing personal information.

Appendix B.

Data Protection Act Principles

The DPA contains 8 principles for processing personal data with which PBC are committed to comply. These are that personal data:

1. Shall be processed fairly and lawfully and shall not be processed unless specific conditions are met,

2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,

3. Shall be adequate, relevant and not excessive in relation to those purpose(s)

4. Shall be accurate and, where necessary, kept up to date,

5. Shall not be kept for longer than is necessary

6. Shall be processed in accordance with the rights of data subjects under the Act,

7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,

8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

Appendix C.

The rights of Data Subjects under the DPA

The rights of Data Subjects under the DPA which PBC commits to respect include:

- The right to be informed that processing is being undertaken.
- The right to withdraw consent to data being held or processed.
- The right of access to one's personal information.
- The right to prevent processing in certain circumstances.
- The right to correct, rectify, block or erase information which is regarded as false or inaccurate.
- The right to be protected against unauthorized access to data and to seek compensation for damages caused by breaches of Data Protection legislation.