WILLESLEY PARK
GOLF CLUB

Members Data Protection Policy

Introduction

Willesley Park Golf Club (WPGC) needs to gather and use certain information about our members. The General Data Protection Regulations (GDPR) protects individuals against the misuse of personal data and may cover both manual and electronic records.

All records whether they be held electronically or physically fall within scope of the Regulations.

The Regulations require that any personal data held should:

1. be fairly and lawfully processed
2. be processed for limited purposes and not in any manner incompatible with those purposes
3. be adequate, relevant and not excessive
4. be accurate
5. not be kept for longer than is necessary
6. be processed in accordance with individuals' rights
7. be secure; and
8. not be transferred to countries without adequate protection

The Regulations also give individuals certain rights. For membership purposes, the most important right is the right to access personal data held about the member. This policy describes how this personal data must be collected, handled and stored to meet data protection standards and comply with the law.

Policy Scope

This policy applies to any personal information, in any form, applying to any individual. This may include members, suppliers, business contacts, and other people the Club has a relationship with or may need to contact. The Club has a separate Data Protection Policy for Employees.

Policy Objectives

This policy ensures WPGC

1. Complies with data protection law and follows good practise
2. Protects the rights of, members and business associates and relationships
3. Is open about how WPGC stores and processes individual's data
4. Protects itself from the risk of a data breach.
5. Offers choice (all individuals should be free to choose how WPGC uses data relating to them)
6. Protects against reputational damage (WPGC could suffer if hackers successfully gained access to our data.)

Policy Implementation

WPGC will hold personal data about members. WPGC will provide a privacy notice which tells our members what information we hold, what we do with it, who we share it with, and the lawful basis for the processing of the data.
The information collected will be kept for the following purposes

1. Membership applications and eligibility
2. Administration of and the notification and collection of membership fees
3. Calculation of Life membership
4. All modes of information giving and information receiving communications required to support the business
5. Accident reports

WPGC considers that the following personal data falls within the categories above

1. Personnel details including name, address, telephone contact and age
2. Emergency contact details
3. Bank and Building Society details
4. Medical declarations.

WPGC will review the information held on an annual basis to ensure there is a sound business reason for requiring the information to be retained.

The information collected will be held for the duration of membership. On termination of membership the information collected will be reviewed and where there is no business reason for keeping the information the information will be securely destroyed. Information will be held for retention periods as outlined below

Record	Retention period (S signifies statutory)
Name and date of joining	20 years
Health and safety records	Permanently (S)
Applications and interview notes for unsuccessful membership	1 year

In exceptional circumstances this information may be held for longer periods and WPGC will explain the legal basis for retaining the data on request.
A member has the right to request that their personal data is deleted, such requests will be dealt with by the WPGC Chair of Board who will review the request and take appropriate steps. If the request is denied WPGC will respond with the Company's reasons including the legal basis for retaining the data.

Special Category Data

Special category data includes information relating to the following matters:

1. racial or ethnic origin
2. political opinions
3. religious or similar beliefs
4. trade union membership
5. physical or mental health or condition
6. his or her sex life; or
7. the commission or alleged commission of any offence

To hold special category data, the WPGC must additionally satisfy a special category data condition. The most appropriate condition for employment purposes is that the processing is

necessary to enable WPGC to meet its legal obligations (for example, to ensure health and safety or to avoid unlawful discrimination).

Responsibilities
Everyone who works for or with WPGC has some responsibility for ensuring data is collected, stored and handled appropriately.

However, these people have key areas of responsibility:

- The Board of Directors is ultimately responsible for ensuring that WPGC meets its legal implications. The Chair of the Board will be the Data Controller for WPGC

- The Data Protection Officer, (The Director responsible for Compliance) is responsible for

1. Keeping the Board updated about data protection responsibilities risks and issues
2. Reviewing all data protection procedures and related policies
3. Dealing with requests from individuals to see the data WPGC holds about them (also called subject access requests)
4. Checking and approving any contracts or agreements with third parties that may handle WPGC sensitive data.

- The Club Secretary is responsible for

1. Ensuring all systems, services and equipment used for storing data meet acceptable security standards
2. Performing checks and scans to ensure security software is functioning properly

- The Director Responsible for Marketing and Communication is responsible for

1. Approving any data protection statements attached to communications such as emails and letters
2. Addressing any data protection queries from external bodies i.e. media outlets
3. Where necessary working with other Directors and employees to ensure marketing, initiatives abide by data protection principles.

- The Managers of Greens and House and Bar are responsible for

1. Arranging data protection training and advice for the people covered by this policy
2. Handling data protection questions from staff and anyone else covered by this policy

General Employee Guidelines

- The only people able to access data covered by this policy should be those who need it for their work
- Data should not be shared informally. When access to confidential information is required, employees should request it from their line manager.
- WPGC will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following these guidelines
- Strong passwords should be used and never shared
- Personal data should not be disclosed to unauthorised people either within WPGC or externally

- Data should be regularly reviewed and updated if it is found to be out of date, if no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection.

General Member Guidelines
Members must only access data available through the Club members only website to: -

- Arrange matches
- Arrange social golf

Data Storage

- When data is stored on paper it should be kept in a secure place where unauthorised people cannot see it.
- When not required paper and files should be kept in a locked drawer or filing cabinet
- Data print outs should be shredded and disposed of securely when no longer required.
- When data is stored electronically it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts.
- Data should be protected by strong passwords that are changed regularly and never shared
- If data is stored on a removable media these should be kept locked away securely when not in use
- Data should only be stored on designated drives and servers
- Data should be backed up frequently.
- Data should never be saved directly to laptops or other mobile devices like tablets and smart phones
- All servers and computers continuing data should be protected by approved security software and a firewall

Data Usage

Personal data is of no value to WPGC unless the club can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.

- When working with personal data employees should ensure the screens of their computers are always locked when left unattended
- Personal data should not be shared informally. In particular it should not be sent by e mail as this form of communication is not secure.
- Personal data should never be transferred outside of the European Economic area
- Employees should not save copies of personal data to their own computers
-

Use of Personal Data
To ensure compliance with the Regulations and in the interests of privacy, member confidence and good member relations, the disclosure and use of information held by the WPGC is governed by the following conditions:

1. personal data must only be used for one or more of the purposes specified in this Policy

2. WPGC documents may only be used in accordance with the statement within each document stating its intended use; and
3. provided that the identification of individual members is not disclosed, aggregate or statistical information may be used to respond to any legitimate internal or external request for data (for example, surveys, membership level figure); and
4. personal data must not be disclosed, either within or outside the company, to any unauthorised recipient

Data Accuracy

The law requires WPGC to take reasonable steps to ensure data is kept accurate and up to date.

- Data will be kept in as few places as necessary
- Data will be kept in a way that is easy to amend or delete
- Employees should take every opportunity to ensure data is updated
- WPGC will make every effort to make it easy for data subjects to update the information WPGC holds about them for instance via the website.
- Data should be updated as inaccuracies are discovered. For instance, if a person can no longer be reached on their stored telephone number it should be removed from the data base
- Data will be removed within a reasonable time frame if no longer required.
- It is the responsibility of the Director for Marketing to ensure marketing databases are checked every six months

Subject Access Requests

All individuals who are the subject of personal data held by WPGC are entitled to

- Ask what information the company holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how WPGC is meeting its data protection obligations,

If an individual contacts WPGC requesting the information this is called a subject access request. These can be made by e mail at Info@willesleypark.com or in writing addressed to the Data Controller (Chair of the Board) who will respond to the enquiry

Enquiries about personal data

WPGC is permitted to charge an administration fee of up to £10 for responding to this type of request. Individual employees should not deal with this type of enquiry, unless they have been given specific authorisation to do so. The request should normally be passed to the person within the business who has responsibility for Data Control. Personal data should not be given out to the friends or relatives of an individual without that individual's specific consent.

Data Breaches

Where the company becomes aware of a personal data breach it will, without undue delay and where feasible, not later than 72 hours of becoming aware of it, notify the personal data breach to the ICO/Data Protection Commission, unless the controller is able to demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of individuals. Where the above aim cannot be achieved within 72 hours, an explanation of the reasons for delay will accompany the notification to the ICO/Data Protection Commission and information may be provided in phases without undue further delay. In addition, data subjects will be notified

without undue delay if the personal data breach is likely to result in a high risk to their rights and freedoms to allow them to take the necessary precautions. This notification will describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. This will be done as soon as reasonably feasible, and in close co-operation with the ICO/Data Protection Commission.

Data Protection Impact Assessments' (DPIAs)

These are mandatory in certain circumstances. A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

1. where a new technology is being deployed;
2. where a profiling operation is likely to significantly affect individuals; or
3. where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks. (Appendix 1 ICO guidance and best Practise on DPIA)

Any Director or WPGC employee implementing a new technology or adopting an organisational change (risk and project management) must consider the Data protection implications and assess using a DPIA.(appendix 2). They will be responsible for ensuring completion and any resulting actions.

Using CCTV Systems

WPGC must ensure that Data Protection laws are followed in the use of CCTV cameras. Before installation an installation checklist must be completed (this is found in appendix 3, The Rules Governing the use of CCTV). The WPGC Data Controller has responsibility for applying the governing rules

Data Privacy Notices

WPGC will share their Data privacy notice by

- Displaying the notice in the club house
- By giving a copy to new members
- By uploading onto the club website
- By making it available to business partnerships and employees

Policy Review

Policy Development/Owner	**WPGC Board**
Version Control	
Version 1	**01/04/18**
Approved by/date	J Seal Chairperson WPGC Board
Review	01/04/2020

Signed:……

Date:……