Claremont Railway LTC Data Protection Policy

Introduction

Under normal operations, the Club needs to gather and use certain information about members, officers and relevant 3rd parties. This policy describes how this personal data must be collected, handled and stored to meet the club's data protection standards and to comply with GDPR.

This data protection policy ensures that the Club:

- Complies with the data protection law and follows good practice
- Protects the rights of members, officers and 3rd parties
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

General Data Protection Regulation (GDPR)

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual EU Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge and that it is processed with their consent. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safety and not disclosed unlawfully.

GDPR is underpinned by the following important principles that say personal data must:

- Be processed fairly and lawfully
- Be obtained with consent and only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up-to-date
- Not held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not transferred outside the European Economic Area (EEA) unless that country or territory also ensures an adequate level of protection

Scope

This policy applies to:

- The Club
- All officer, members and volunteers of the Club
- All contractors, suppliers and other third parties working on behalf of the Club

It applies to all data that the club holds relating to identifiable individuals.

The purpose of this policy is to remain compliant with law and reduce any risk of breaches of confidentiality or any other data requirements under GDPR.

Responsibilities of Officers

Each officer/volunteer of the Club has some responsibility for ensuring data is collected, stored and handled appropriately.

Everyone who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The Committee is ultimately responsible for ensuring that the Club meets its legal obligations, as well as:

- Approving of any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries form journalists or media outlets like newspapers.
- Monitoring data protection responsibilities, risks and issues.
- Reviewing the data protection policy annually for fitness.
- Ensuring that all officers with day-to-day responsibilities involving personal data and processing operations, and those with permanent/regular access to personal data, are appropriately trained and can demonstrate compliance with the GDPR.
- Handling data protection questions from members / third parties.
- Ensuring that personal data collected is adequate, relevant and non-excessive and is to be used for the specified purposes only.
- Dealing with subject access requests from individuals
- Checking and approving any contracts or agreements with third parties that may handle the club's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks to ensure security hardware / software is functioning properly.
- Evaluating any third-party services the club is considering using to store or process data in detail before proceeding.

Guidelines

- The only officers able to access data are those who require it for their portfolio of work.
- Data is not shared informally
- Officers keep all data secure by taking sensible precautions in line with this policy.

- Strong passwords must be used on any sharing of personal information, with passwords to be passed via a separate medium.
- No unauthorised disclosures of personal data.
- Data should be maintained and regularly reviewed to ensure it is up to date.
- When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out: When not required, the paper or files should be kept in a locked drawer or filing cabinet. Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer. Data printouts 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.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Electronic data should be kept on appropriate servers only and data should be backed up frequently.
- If saving data to a personal device, it must be encrypted and deleted after use where possible.
- Data will be retained only as long as the club requires it for the administration of memberships. It will be retained for 6 years after a member leaves the club, after which time it will be deleted.
- Data will only be used after consent for the specific use has been provided by the relevant individual.
- When working with personal data, officers should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally except with the consent of the data subject.
- Sensitive data must be encrypted before being transferred electronically.

Data Accuracy

The law requires the Club to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all officers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets. Staff should take every opportunity to ensure data is updated, for instance, by confirming a member's details when they call. The Club will make it easy for data subjects to update the information it holds about them. Data should be updated as inaccuracies are discovered, for instance, if a member can no longer be reached on their stored telephone number, it should be removed from the database. It

is the officer's responsibility to ensure email databases are checked against the consent and marketing preferences of data subjects.

Subject Access Requests

- All individuals who are the subject of personal data held by the Club are entitled to:
- Ask what information the club holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the club is meeting its data protection obligations with respect to them as an individual. If an individual contacts the club requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the Club email. Individuals will be charged €6 per subject access request. The club manager will aim to provide the relevant data within 14 days. The club manager will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, the Club will disclose requested data. However, the Committee will ensure the request is legitimate, seeking assistance from legal advisors where necessary.

Providing information

The Club aims to ensure that individuals are aware that their data is being processed and that they understand how the data is being used and how to exercise their rights. If anything in this policy is unclear, members can seek additional guidance from the Committee or on the Tennis Ireland website: https://www.tennisireland.ie/data-protection/gdpr/