Carrickmines Croquet and Lawn Tennis Club

Data Protection Policy

Key Details

- Policy prepared by: CCLTC GDPR sub-committee
- Approved by main committee on: 14/5/18
- Policy became operational on: 25/5/18
- Next Review Date: 13/5/19

Introduction

In the normal operations of the club Carrickmines Croquet and Lawn Tennis Club (CCLTC) needs to gather and use certain information about members, staff and other people the club has a relationship with or may need to contact.

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 the law.

Why this policy exists

This data protection policy ensures that CCLTC:

- Complies with the data protection law and follows good practice
- Protects the rights of members, staff and partners
- 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 safely 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

People, risks and responsibilities

Policy Scope

This policy applies to:

- CCLTC
- All staff and volunteers of CCLTC
- All contractors, suppliers and other people working on behalf of CCLTC

It applies to all data that the club holds relating to identifiable individuals, even if that information technically falls outside of the GDPR 2016.

Data protection risks

This policy helps to protect CCLTC from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the club uses data relating to them.
- Reputational damage. For instance, the club could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with CCLTC 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.

These people have key areas of responsibility:

- The Main Committee is ultimately responsible for ensuring that CCLTC 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.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

- The Club Manager is responsible for:
    - Keeping the main committee updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Ensuring that all Employees/Staff 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 staff and anyone else covered by this policy.
    - Ensuring that personal data collected is adequate, relevant and non-excessive and is to be used for the specified purposes only.
    - Dealing with requests from individuals to see the data CCLTC holds about them (also called 'subject access requests').
    - 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 and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the club is considering using to store or process data. For instance, cloud computing services.

General Staff 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 can request it from the club manager.
- CCLTC **will provide GDPR 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 the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the club 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 the club manager if they are unsure about any aspect of data protection.

Data Storage

These rules describe how, where and for how long data should be safely stored. Questions about storing data safely can be directed to the club manager.

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 for some reason:

- 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:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing service**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the club's standard backup procedures.
- Unless absolutely necessary, data should **never be saved directly** to laptops or other mobile devices like tablets or smartphones, in which case it should be encrypted.
- All servers and computers containing data should be protected by **approved security software and a firewall**.
- 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 Use

Personal data is of no use to CCLTC 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:

- Data will only be used **after consent for the specific use has been provided** by the relevant individual.
- 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 never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The club manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees **should not save copies of personal data to their own computers**. Always access and update the central copy of any data.

Data Accuracy

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

The more important it is that the personal data is accurate, the greater the effort CCLTC should put into ensuring its accuracy.

It is the responsibility of all employees 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.
- CCLTC will make it **easy for data subjects to update the information** CCLTC holds about them. For instance, via the club website.
- 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 club manager's responsibility to ensure **databases are checked against industry suppression files** every six months. For instance, email addresses in suppression lists are NOT to be included while emailing; those people who have chosen not to receive emails for that purpose should NOT be included on such emails.

Subject Access Requests

All individuals who are the subject of personal data held by CCLTC 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**.

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 manager. The club manager can supply a standard request form, although individuals do not have to use this.

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, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, CCLTC will disclose requested data. However, the club manager will ensure the request is legitimate, seeking assistance from the Main Committee and from the club's legal advisors where necessary.

Providing information

CCLTC aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the club has a privacy statement, setting out how data relating to individuals is used by the club.