Policy Purpose

The purpose of this policy is to ensure that all employees understand the Club requirements in relation to the disclosure of personal data and confidential information.

Internal Data policy

During your employment, The Club will entrust you with access to information and knowledge **"data"** that is valuable to its business and not available in the public domain **"confidential information".**

SECTION A: TYPES OF DATA

The Club recognises that **data** is gathered and exists in the following forms, but may not be limited to:

- **Members details**, including names, addresses, occupation, phone numbers, email addresses, club activities and other information which may relate to personal conduct.
- **Employee and Director details,** including names, addresses, tax file numbers, phone numbers, email addresses, bank details and other information which may relate to health.
- **Supplier & Contractor details,** including names, addresses, position, phone numbers, email addresses and contract agreements.
- **Client details,** including names, phone numbers, email addresses and employment positions.

The identified Data above has the potential to cause harm to the owner if used incorrectly or for unintended purposes.

SECTION B: DATA STORAGE AND ACCESS

All data stores onsite by The Club is monitored by Watchguard firewalls. The management of the onsite data storage system is performed by specialised information technology suppliers who are engaged to ensure our system is as up to date as possible.

Additional filters are also applied to the Group email and internet access to reduce the risk of malicious external threats.

Internal System and Data Access: it is a requirement of the club that access to the data is limited. This by no way means that a restriction to duties is enforced, all access to information will be available through the Gaming and Systems Manager in conjunction with approval by the CEO or Compliance Manager.

External Systems and Data Access: For the purpose of system management, service, upgrades or enhancements, external suppliers will need access to The Club internal IT systems and data from time to time.

This access is available by requestion access through the IT ticketing system.

Approved suppliers will be granted access for performing their role in maintaining our system, for the time required to do so.

Cloud Storage: Cloud computing and storage of data has become part of everyday business activities.

The cloud systems used or adopted will be at the discretion of the management as systems are changed and enhanced.

Employees are not permitted to personally activate cloud storage or move information to the cloud unless approved. Approval for the use of cloud service in under the guidelines of data sharing in section (C) of this document.

SECTION C: DATA SHARING

For the purpose of performing specific duties you may be required to send or share data with external providers.

Employees must be granted permission by the Management before sharing and Data.

Before the group agrees to sharing data, the external business may be required to sign a Non-Disclosure (NDA). Examples of Data sharing is listed below but are not limited to:

- Membership mailouts
- Payroll activities
- Storage of employee files
- Legislative commitment

Breach of these guidelines may result in disciplinary action, including dismissal. It may also expose you to personal liability.

If an employee has any questions or requires further explanation on acceptable practices, legislative or operational requirements, they may do so by contacting the Management at any time.

This policy will be reviewed annually or as required to ensure The Club meets national data security requirements.