Thanet Roadrunners AC
IT Security Policy
Effective from 01/02/2019

Introduction
This document sets out the measures to be taken by all members of Thanet Roadrunners AC (the "Club") and by the Club as a whole in order to protect the Club's computer systems, devices, infrastructure, computing environment and any and all other relevant equipment (collectively, "IT Systems") from damage and threats whether internal, external, deliberate or accidental.

Key Principles
- IT Systems are to be protected against unauthorised access.

- IT Systems are to be used only in compliance with relevant Club Policies.

- All data stored on IT Systems are to be managed securely in compliance with all relevant parts of the GDPR and all other laws governing data protection whether now or in the future in force.

- Club members and any and all third parties authorised to use the IT Systems including, but not limited to, contractors and sub-contractors (collectively, "Users"), must ensure that they are familiar with this Policy and must adhere to and comply with it at all times.

- Management Committee (collectively, "committee") must ensure that all users under their control and direction must adhere to and comply with this Policy at all times as required under in previous paragraph.

- IT Systems must have up-to-date securities installed, maintained, serviced, repaired and upgraded ensuring appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- The responsibility for the security and integrity of all IT Systems and the data stored lies with the committee including, but not limited to, the security, integrity and confidentiality of that data.

- All breaches of security pertaining to the IT Systems or any data stored thereon shall be reported and subsequently investigated by the Committee.

- All Users must report any and all security concerns relating to the IT Systems or to the data stored thereon immediately to the Committee.

1. **Software Security Measures**
a. The committee's responsibilities are:
b. Ensure that all IT systems are assessed and deemed suitable for compliance with the Club's security requirements;
c. Ensure that IT security standards within the Club are effectively implemented and regularly reviewed in line with this Policy;
d. Ensure that all users are kept aware of the requirements of this policy and of all related legislation, regulations and other relevant rules whether now or in the future in force including, the GDPR.

2. **Users' Responsibilities**

a) Comply with all relevant parts of this policy at all times when using the IT systems.
b) Keep up to date with Club IT system policies as listed at the end of the document.
c) Inform the committee of any security concerns relating to the IT systems.
d) Inform the committee of any other problems which may impact on documents/downloads/cloud storage and email systems**.**
e) Users are granted levels of access to IT systems that are appropriate for each user, taking into account their role, responsibilities and any special security requirements; ensuring all club documents/downloads are stored in the cloud enabling regular backups to taken at regular intervals.
f) Any and all deliberate or negligent breaches of this policy by users will be handled as appropriate by the committee.

3. **Anti-Virus Security Measures**

a. IT systems (including all computers and servers) will be protected with suitable anti-virus, firewall and internet security software. All such anti-virus, firewall and internet security software will be kept up-to-date with the latest software updates and definitions.
b. Anti-virus software will be subject to a full system scan at least weekly.
c. Storage media (e.g. USB memory sticks or disks of any kind) used by Users for transferring files must be virus-scanned before any files may be transferred.
d. Users shall be permitted to transfer files using the club provided cloud storage systems. All files downloaded from any cloud storage system must be scanned for viruses during the download process.
e. Any files being sent to third parties outside the Club, whether by email, on physical media or by other means (*(file transfer protocol)* FTP or shared cloud storage) must be scanned for viruses before being sent or as part of the sending process, as appropriate. All email attachments are scanned automatically upon sending.
f. Users must ensure all detected virus are reported immediately to the committee (even where the anti-virus software automatically fixes the problem). The committee shall promptly take any and all necessary action to remedy the problem.

4. **Hardware Security Measures**

a. The committee asks that, IT systems, when not in use, are securely locked by using Windows Key+L keyboard sequence to lock the computer as a minimum security action or otherwise logout/shut down ensuring confidentiality to data.
b. Mobile devices, such as laptops, provided by the club, where left unattended, every reasonable effort should be made to store out of sight.
c. The Committee shall maintain a complete asset register of all IT Systems. All IT Systems shall be labelled and the corresponding data shall be kept on the asset register.

5. **Access Security**

a. IT systems must be protected with a secure password or such other form of secure log-in system.
b. Password access to data and IT systems will be based on authority levels and job functions, e.g. granting access on a need-to-know and least privilege basis, use of user IDs and passwords. The system will be periodically reviewed and changed as and when roles change or terminates.

6. **Data Protection**

a. Personal data (as defined in the General Data Protection Regulation ("GDPR")) collected, held and processed by the club will be collected, held and processed strictly in accordance with the GDPR and the club's Data Protection Policy.
b. The committee shall ensure there are data security controls which include at a minimum, but may not be limited to, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilisation of commercially available and industry standard encryption technologies for personal data that is:

c. Transmitted over public networks (i.e. the Internet) or when transmitted wirelessly; or at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives, back-up tapes).

d. All emails containing personal data must be encrypted/password protected.

e. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.

f. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

g. No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the club where the party in question has agreed to comply fully with the letter and spirit of this Policy and of GDPR (which may include demonstrating to the club that all suitable technical and organisational measures have been taken).

h. The committee shall ensure that it has in place appropriate technical practices in place to protect against unauthorised or unlawful processing of personal data and against accidental loss.

i. Ensure that availability of and access to personal data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures are adopted.

j. All electronic copies of personal data should be stored securely using passwords and data encryption ensuring confidentiality.

k. Only users that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the club.

l. Users handling personal data for and on behalf of the club shall be subject to, and must comply with, the provisions of the club's Data Protection Policy.

7. **Internet and Email Use**

a. All Users shall be subject to, and must comply with, the provisions of the Club's Communications, Email and Internet Policy when using the IT Systems.

b. Where provisions in this policy require any additional steps to be taken to ensure IT security when using the internet or email over and above the requirements imposed by the Communications, Email and Internet Policy, users must take such steps as required.

8. **Reporting IT Security Breaches**

a. All concerns, questions, suspected breaches or known breaches shall be referred immediately to the committee. Upon receiving a question or notification of a breach, the committee shall, within 72 hours assess the issue including, but not limited to, the level of risk associated therewith, and shall take any and all such steps as the committee deems necessary to respond to the issue.

b. Under no circumstances should a user attempt to resolve an IT security breach on their own without first consulting the committee. Users may only attempt to resolve IT security breaches under the instruction of, and with the express permission of, the committee.

c. All IT security breaches, whether remedied by the committee or by a User under the committee's direction, shall be fully documented.

Implementation of Policy

This Policy shall be deemed effective as of 1st March 2019. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Thanet Roadrunner AC Policies to be used as part of this document:

- Data Protection Policy
- Privacy Statement
- Privacy Policy

- Data Retention Policy
- Statement of Intent (Clubs commitment of personal data & accountability
- IT Policy
- Report Breach Policy

This Policy has been approved and authorised by:

Name:	**Julie Williams**
Position:	**Club Secretary**
Date:	**26.9.2023**
Due for Review by:	**Annually, in April.**