IT Acceptable Use Policy

1. Purpose

The purpose of this IT Acceptable Use Policy is to outline the acceptable use of all IT resources, including computer hardware and software, network systems, internet access, email systems, and other electronic communication systems, by staff, committee members and any persons delegated by the committee to use IT facilities at the club to perform work on behalf of the club.

2. Scope

Staff, committee members and any persons delegated by the committee (hereafter referred to as "users") to use IT facilities at the club to perform work on behalf of the club are bound by the provisions of its policies in addition to this Acceptable Use Policy.

2 Policy

2.1 Acceptable Use

2.1.1 Users are encouraged to utilize the IT facilities to support the golf club's business and sporting objectives. However, personal use of these facilities is a privilege, not a right, and is subject to the following conditions:

- It must not disrupt staff members' work.
- It must comply with club policies.

2.1.2 All users of the club's IT resources must comply with all applicable laws, regulations, and policies, including but not limited to the club's Data Privacy Policy, Information and Confidentiality Policy, Social Media Policy and Communications Policy.

2.1.3 All users of the club's IT resources are responsible for maintaining the security of these resources by using strong passwords, regularly updating software where applicable, and reporting any suspicious activity to the Management committee.

Examples of weak and strong passwords are below. Do not use easily guess terms such as names or words found in a dictionary. Always use special characters. The longer and more complex your password, the better.

Weak Password	Better Password	Strong Password
kitty	1Kitty	1Ki77y
susan	Susan53	.Susan53
allblacks	a11Blacks	a11Black$

2.1.4 The club respects the privacy of its users and expects all users to respect the privacy of others. Any unauthorised access, use, or disclosure of personal information is strictly prohibited.

2.1.5 Access to systems, web applications and/or club email addresses must be revoked in a timely manner e.g. when a staff member leaves the club or a committee member leaves the committee. In the interests of confidentiality, passwords on generic email accounts (e.g. office@nenaghgolfclub.com etc) must be changed whenever an employee leaves or a committee role is transitioned to a new incumbent.

2.1.6 PC's owned by the club should be appropriately backed up and protected with anti-virus software.

2.2 Unacceptable Use

2.2.1 The club IT Systems may not be used directly or indirectly by a User for the download, creation, manipulation, transmission or storage of:

- any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- unlawful material or material that is defamatory, threatening, discriminatory, extremist;
- any material which promotes terrorism or violent extremism;
- material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the club or a third party;
- material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;
- material with the intent to defraud or which is likely to deceive a third party;
- material which advocates or promotes any unlawful act;
- material that brings the club into disrepute.

2.2.2 The club's IT resources must not be deliberately used by a user for activities having, or likely to have, any of the following characteristics:

- Accessing or attempting to access unauthorised information or resources.
- Sharing passwords or other credentials with other users
- Corrupting, altering or destroying another user's data without their consent;
- Disrupting the work of other users;
- Engaging in any activity that may disrupt or interfere with the normal operation of the club's IT resources.
- Denying access to the club IT Systems and its services to other users.
- Introduce data-interception, password-detecting or similar software or devices to the club's IT resources;
- Deliberate unauthorised access to the club IT systems;
- Attempting to undermine the security of the club's IT systems.
- Intentionally or recklessly introducing any form of spyware, computer virus or other potentially malicious software;
- Installing or using unauthorised software or hardware.

2.2.3 The club's email system and messaging systems are intended for club-related activities only.

2.2.4 Users of the club's email system should not:

- harass, threaten, or intimidate others.

- solicit or promote personal or personal commercial activities.
- send confidential or sensitive information without prior approval from management.

2.2.5 The club recognises the value of social media as a communication and engagement tool. Social media should be used in a responsible and ethical manner and in compliance with the club's Social Media Policy.

3. Phishing

Be aware and vigilant against phishing attempts. Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

The information may then be used to access important accounts and can result in identity theft and financial loss.

Common features of phishing messages

- Too Good To Be True - Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people's attention immediately. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize.
- Sense of Urgency - A favourite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Some of them will even tell you that you have only a few minutes to respond. When you come across these kinds of emails, it's best to just ignore them. When in doubt, visit the source directly rather than clicking a link in an email.
- Hyperlinks - A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different or it could be a popular website with a misspelling, for instance www.bankofarnerica.com - the 'm' is actually an 'r' and an 'n', so look carefully.
- Attachments - If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it! They often contain payloads like ransomware or other viruses.
- Unusual Sender - Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of character or just suspicious in general don't click on it.

4. Enforcement

The club reserves the right to monitor all activities on its IT resources for ensuring security and performance, including but not limited to access to and usage of the club networks, emails, Internet and telecommunications means, remote connections, and social media use. Serious breaches may result in disciplinary action, up to and including termination of employment or membership.