

ANGLING COUNCIL IRELAND CODE OF CONDUCT INTERNET & E-MAIL

The Internet and Electronic mail (e-mail) are important communication and research tools for the the Angling Council of Ireland (ACI) network users. This document details standards for the secure use of Internet and e-mail facilities for ACI purposes, including teaching, research and administration.

*Angling Council
Ireland
Internet & E-mail
Policy*

Code of Conduct



General Policy

1. Introduction

The Internet and Electronic mail (e-mail) are important communication and research tools for the Angling Council Ireland (ACI) network users. This document details standards for the secure use of Internet and e-mail facilities for ACI purposes, including teaching, research and administration.

2. Scope

This policy applies to all ACI staff, tutors, coaches, trainers, trainees and third parties granted use of ACI Internet and E-mail facilities. This includes members of affiliated organisations, their staff and trainees in

- Irish Federation of Sea Anglers
- Salmon & Sea Trout Recreational Anglers of Ireland
- National Coarse Fishing Federation of Ireland
- Northern Ireland Fly Fishing Association
- Game Angling Instructors Association

Third parties are defined as any individual, group contractor, vendor or agent not registered as an ACI staff member or member.

3. Acceptable Usage

All Internet and Email usage and this policy document must be compliant with the ACI computer acceptable usage policy.

All Email usage will also be in line with the ACI acceptable usage policy

4. Data Protection

E-mails fall under the scope of the data protection act. Under this legislation the email originator, all email recipients and any persons named in the e-mail are entitled to view the information about them and if it is incorrect they are entitled to have it corrected.

Home or personal use has a “domestic exemption” from data protection law, but ACI has no such exemption even for personal e-mails if they originate from the ACI network. In addition, e-mails can constitute publication for the purpose of the law of libel.

Additionally any information, which ACI users collect via the Internet such as personal or financial details collected via Internet forms or surveys, fall under the Data Protection Act. All users must ensure that the methods of collecting processing and storing information in this way comply with the ACI policies the data protection Act and any other relevant legislation.

5. Copyright

Copyright law stops other people from using and abusing users' original work. Users should bear in mind, therefore, that:

- Messages sent to a list should not be quoted out of context, changed or reworded or mis-attributed.
- Software or files downloaded from the Internet may be protected by copyright restrictions. E-mail messages are creative works and therefore are copyrighted.
- All e-mail messages sent by a user are copyrighted to the user (or ACI). Users do not have to register this copyright - it exists automatically.
- When users post to a public list they do not lose copyright, but the message may be archived forwarded to other lists or quoted by others.

6. Privacy

Data users must assume that all e-mail or Internet communications are not secure unless encrypted and they should not send via e-mail any information, which is confidential. Users may not, under any circumstances, monitor, and intercept or browse other users' e-mail messages unless authorised to do so. Network and computer operations personnel, or system administrators, may not monitor other users' e-mail messages other than to the extent that this may occur incidentally in the normal course of their work.

The ACI reserves the right to access and disclose the contents of a user's e-mail messages, in accordance with its legal and audit obligations, and for legitimate operational purposes. The ACI reserves the right to demand that encryption keys, where used, be made available so that it is able to fulfil its right of access to a user's e-mail messages in such circumstances.

7. Internet Policy

All users must adhere to the following when using ACI facilities to connect to the Internet:

- Access to the Internet is provided for ACI purposes and must not be abused for personal use.
- Commercial use, which is not connected to or approved by ACI, is strictly prohibited and will result in disciplinary procedures.
- Internet access in ACI is available only via the ACI infrastructure. Users should not connect to the Internet via a dial-up ISP account on ACI computers connected to the network.
- Users are expected to act ethically and responsibly in their use of the Internet and to comply with the relevant national legislation, the ACI Information Security Policy, regulations and codes of practice. Users must not post messages on newsgroups or chat areas that are likely to be considered abusive, offensive or inflammatory by others.
- Users must not use the ACI Internet connection to scan or attack other individuals/devices/organizations. The use of port scanners or other hacking tools is strictly prohibited.
- Users should be aware that the public nature of the Internet dictates that the confidentiality and integrity of information cannot normally be relied upon.

- Where a requirement exists to send or receive confidential or commercially sensitive data over the Internet, a security mechanism recommended by ACI executive or the Sport Ireland IT Security Specialist should be used.
- Passwords used for Internet services should not be the same or similar to passwords used for services accessed within ACI. This is to prevent passwords that grant access to ACI IT resources being sent out on the Internet in clear text where any Internet user can potentially see them. Similarly, any username used for the Internet services should not be the same or similar to an ACI username.
- Software copyrights and license conditions must be observed. Only licensed files or software may be downloaded from the Internet.
- The use of the ACI Internet Connection to download or distribute copyright material using peer-to-peer applications is strictly prohibited. The IS IT department reserves the right to disconnect any machines involved in illegal file distribution from the ACI network.
- All devices connected to the Internet must be equipped with the latest versions of anti-virus software, which has been both approved and supplied by ACI.
- All forms of data received over the Internet should immediately be virus checked.
- All forms of data transmitted from ACI over the Internet should be virus checked in advance.
- Data, which has been compressed or encrypted, should be decompressed or decrypted as required before virus checking.
- All security incidents involving Internet access must be reported to the ACI Chairman.

8. Email Policy

All users must adhere to the following when using ACI E-mail facilities:

- Users are expected to act ethically and responsibly in their use of e-mails and to comply with the relevant national legislation, the ACI Information Security policy, regulations and codes of practice.
- Discrimination, victimisation or harassment on the grounds of gender, marital status, family status, sexual orientation, religious belief, age, disability, race, colour, nationality, ethnic or national origin is against ACI Policy. Users must not bully, hassle or harass other individuals via e-mail. Users must not send messages that are likely to be considered abusive, offensive or inflammatory by the recipient/s.
- All users should regard all e-mails sent from ACI facilities or member federations as first, representing the ACI and, secondly, representing the individual. Users should be civil and courteous. Users should not send e-mail, which portrays the ACI in an unprofessional light. The ACI is liable for the opinions and communications of its staff and members. Any e-mail involved in a legal dispute may have to be produced as evidence in court.
- The email system should not be used to target members with commercial advertising, should abide by all ACI standards.
- The 'reply to address' should be targeted to the source of the original message. This will protect the Admin office from being inundated with replies to message which did not originate from the Admin office, and will not dilute the importance of the administrator account.

- The 'Subject Line' should always give a clear indication of the message content so that interested members will open the message, and uninterested members can simply delete message which they believe are not of relevance or interest to them.
- Once a policy has been agreed, the person (people) with responsibility to send out the message should be fully familiar with the email usage policy so that a quick decision can be made regarding the message's suitability for general circulation.
- It would be imperative that any requests to send a message to members via the email system should be dealt with immediately, and if there is any legitimate objection to the transmission of a message, that fact would be relayed to the person who wishes to send the message without delay.
- All users should do their best to ensure that email content is accurate, factual and objective especially in relation to individuals. Users should avoid subjective opinions about individuals or other organisations.
- Users should be aware that e-mails can easily be forwarded to other parties. Users should assume that anyone mentioned in e-mail could see it or hear about it or he/she may, under data protection or other law, be entitled to see it.
- All users should be aware that. It is possible for the origin of an e-mail to be easily disguised and for it to appear to come from someone else.
- Users must not use a false identity in e-mails.
- Users must not create or forward advertisements, chain letters or unsolicited e-mails e.g. SPAM
- All users should protect data displayed on their monitor, e.g. by locking their office door or by locking their workstation or using a screen saver in password-protected mode when leaving their desk. This is in order to prevent unauthorised individuals from using the workstation to send an e-mail, which will appear to originate from the user.
- All users should exercise caution when providing their e-mail address to others and be aware that their e-mail address may be recorded on the Internet.
- All users should be cautious when opening e-mails and attachments from unknown sources as they may be infected with viruses.
- All users must have up-to-date ACI approved anti-virus software installed and operational on the computer that they access their email on.
- All emails or attachments that are encrypted or compressed should be decrypted or decompressed and scanned for viruses by the recipient.
- Users should be aware that e-mails may be subject to audit by the Sport Ireland IT department to ensure that they meet the requirements of this policy. This applies to message content, attachments and addressees and to personal e-mails.
- Currently the ACI standard computing and telecommunications practices, email systems and the systems involved in the transmission and storage of e-mail messages are not normally "backed up" centrally. It is envisaged that in the future these will be backed up centrally on a routine basis for administrative purposes. The back-up process results in the copying of data, such as the content of an e-mail message, on to storage media that may be retained for periods of time and in locations unknown to the originator or recipient of an email. The frequency and retention of back-up copies vary from system to system. However, this back-up is for ACI administrative purposes only and it is the user's own responsibility to back-up any of their e-mails they wish to retain for future reference.

10. Wireless Network Policy

The Sport Ireland / ACI wireless network is intended to be a convenient supplement to the wired network for general functions, including web browsing and e-mail. Wireless “access points”, located in certain areas of the Sports HQ; allow suitably equipped and configured computers to make wireless connections to the Sport Ireland/ACI network, including the Internet.

Because wireless radio signals are shared by everyone using the same wireless access point, the bandwidth available to each connection decreases and performance deteriorates as the number of users and traffic increases. Distance from the access point, buildings or objects shielding the access point, signal interference, quality of your equipment, battery power and other factors may also impact performance. As such, the wireless network should not be expected to provide the same quality-of-service as the wired network. When reliability and performance are a must, the wired network should be used.

Applications that generate high network traffic do not work well on wireless networks and negatively impact performance for everyone connected to the same access point. In addition, wireless networks are highly sensitive to overlapping frequencies and can present a risk to the integrity and security of the ACI data network. To promote efficient and secure wireless network access the ACI management committee maintains strict standards for the deployment of wireless devices at ACI.

RESTRICTIONS

- A.** All wireless access points must be approved by and registered with the ACI admin office before they are connected to the Sport Ireland /ACI network.
- B.** Broadcast frequencies used by the wireless network may be monitored on Sport Ireland /ACI property. Devices that generate interference with the ACI wireless network may be subject to restriction or removal.
- C.** Use of the wireless network is subject to the general restrictions of the ACI and Sport Ireland Acceptable Use Policy.
- D.** Only authenticated access to the ACI’s wireless network is permitted. Typically, authentication is provided via the administration office at the time a member federation is registered for wireless services with the ACI Admin office. Device and connection logs may be used for assessing network problems or identifying unauthorised or unacceptable use of the wireless network.
- E.** All data transmitted via the member wireless connections across the Sport Ireland /ACI network is not secured
- F.** Instructions will be given to member federations and trainees on how to configure their laptops IPAD’s etc. to connect to the wireless network.

LIMITED SUPPORT

- A.** The wireless network's maximum data speed is significantly lower than the speed of the Sport Ireland /ACI wired network. High bandwidth operations, such as large file transfers, Microsoft Windows System updates, and media sharing with peer-to-peer programs do not constitute acceptable use of the wireless network. These services are blocked.
- B.** Performance varies and cannot be guaranteed.

- C. Off-ACI connections to the wireless network are not permitted.
- D. Devices connecting to the wireless network must be capable of meeting minimum security standards, as defined by the ACI Admin. Some older devices do not meet these standards, and may not be used on the wireless network.

ON-SPORT IRELAND CAMPUS WIRELESS ACCESS POINTS NOT OWNED BY ACI

The use of non ACI provided wireless access points, connected to the ACI network, pose a security risk that could give unauthorised or malicious persons access to confidential ACI data. They can also degrade the performance of the Info Systems-provided wireless services on campus.

Because of these risks, the ACI Admin is restricting the use of wireless access points connected to the ACI network. Only Sport Ireland /ACI provided access points are allowed. **IMPORTANT:** Many laptops / phones etc. can be configured as access points. Windows allows Internet Connection Sharing across a wireless interface, and Mac OS X and GNU/Linux provide similar features. Enabling these features effectively turns the laptop into an access point. In order to avoid interference with the Sport Ireland /ACI provided wireless networks these features must be disabled while the wireless device is used on the Sport Ireland /ACI campus.

DEFINITIONS

- A. Wireless Network (WLAN) means local area network technology that uses radio frequency spectrum to connect computing devices to ACI wired networks and may connect to the ACI Network Backbone and the Internet. This technology is alternately known as Wi-Fi.
- B. Access Point (AP) means electronic hardware that serves as a common connection point for devices in a wireless network. An access point acts as a network hub that is used to connect segments of a network, using transmit and receive antennas instead of ports for access by multiple users of the wireless network. Access points are shared bandwidth devices and can be connected to the wired network, allowing access to the ACI network backbone.
- C. Wireless device means a desktop, laptop, hand-held, portable, or other computing device with a component installed to provide a wireless network interface.
- D. Interference means the degradation of a wireless communication signal caused by electromagnetic radiation or an overlapping frequency generated from another source. Interference can slow down or eliminate a wireless transmission depending on the strength of the interfering signal.
- E. Client Software means the software that is installed in a desktop, laptop, hand-held, portable, or other computing device to provide an authenticated wireless network connection.

