

VOLUNTEER INDUCTION PROGRAMME

COMPUTER USE POLICY

2026/2027

POLICIES & PROCEEDURES - COMPUTER USE POLICY

The Association has invested heavily in Information Technology and its use is covered by the Computer Usage Policy.

While the Association has relevant and current protection procedures in place, it is also important that users make use of the IT system responsibly.

All users are required to understand the risks of introducing unauthorised software or other electronic information.

It is not permitted to download and/or install programs or applications directly onto the network without prior consent from the external IT Administrator. This ensures that all programs and applications are free from viruses, does not infringe copy right and is fit for purpose.

Email messages and misuse of the internet also carry risks. Email and internet must only be used for Association business and any deliberate or negligent misuse of them may be treated as an act worthy of dismissal.

Users are expected to take responsible precautions to safeguard equipment and to maintain integrity of the data retained on the system.

Files and documents must not be deleted by volunteers.
Please see the Email Policy and Computer Usage Policy.

POLICIES & PROCEEDURES - COMPUTER USE POLICY

Overview

Though there are several reasons to provide a user network access, by far the most common is granting access to employees and volunteers for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the Associations network. This policy explains how Association information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use common sense when using Association resources. Questions on what constitutes acceptable use should be directed to the Chairperson or IT Support.

Purpose

Since inappropriate use of agency systems exposes The Claddagh Association Inc (the Association) to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of Association information technology resources for the protection of all parties involved.

Scope

The scope of this policy includes all use of association IT resources including but not limited to, computer systems, email, the network, and the agency internet connection.

POLICIES & PROCEEDURES - COMPUTER USE POLICY

Email Use

Personal usage of Association email systems is permitted as long as:

- a) Such usage does not negatively impact the computer network and,
- b) Such usage does not negatively impact the users job performance.

The following is never permitted:

- a) Spamming, harassment, communicating threats, solicitations, chain letters or pyramid schemes. This list is not exhaustive but is included to provide a frame of reference for types of activities that are prohibited;
- b) The user is prohibited from forging email header information or attempting to impersonate another person;
- c) It is Association policy not to open email attachments from unknown senders or when such attachments are unexpected;
- d) Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

Please note that detailed information about the use of email may be covered in the Associations' Email Policy.

Confidentiality

Refer to the Associations Privacy Policy and Confidentiality Policy for details on the treatment of confidential information.

Network Access

The user should take reasonable efforts to avoid accessing network data, files and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access.

POLICIES & PROCEDURES - COMPUTER USE POLICY

Unacceptable Use

The following actions shall constitute unacceptable use of the Association network. This list is not exhaustive but is included to provide a frame of reference for the types of activities that are deemed unacceptable. The user may not use the Association network and/or systems to:

- Engage in activity that is illegal under local, state, federal or international law.
- Engage in any activities that may cause embarrassment, loss of reputation or other harm to the Association.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Engage in activities that cause an invasion of privacy.
- Engage in activities that cause disruption to the workplace environment or create a hostile workplace.
- Make fraudulent offers for products or services.
- Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging or other IT information gathering techniques when not part of the employees' job function.
- Install or distribute unlicensed or 'pirated' software.
- Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

POLICIES & PROCEEDURES - COMPUTER USE POLICY

Blogging and Social Media

Blogging and social networking by employees are subject to the terms of this policy, whether performed from the agency network or from personal systems.

Blogging and social networking are allowed from Association computer networks provided that:

- it is done in a professional manner;
- confidential data is not disclosed;
- it does not impact the users job performance;
- no information detrimental to the Association is published.

The user assumes all risks associated with blogging and/or social networking. Please take time to read and understand the Social Media Guidelines before engaging in any social media communications.

POLICIES & PROCEEDURES - COMPUTER USE POLICY

Instant Messaging

Instant messaging is allowed for agency communication only. The user should recognise that instant messaging may be an insecure medium and should take any necessary steps to follow the guidelines on disclosure of confidential data.

Overuse

Actions detrimental to the computer network or other Association resources, or that negatively impact job performance are not permitted.

Web Browsing

The internet is a network of interconnected computers of which the Association has very little control. The user should recognise this when using the internet and understand that it is a public domain and he or she can encounter information, even inadvertently, that he or she may find offensive, sexually explicit or inappropriate. The user must use the internet at his or her own risk. The Association is specifically not responsible for any information that the user views, reads or downloads from the internet, however, the Association has internet filters in place to block known 'bad' sites and log all users' activity.

Personal Internet Use

The Association recognises that the internet can be a tool that is useful for both personal and professional purposes. Personal usage of Association computer systems to access the internet is permitted if such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect of the Association or on the users' job performance.

POLICIES & PROCEDURES - COMPUTER USE POLICY

Copyright Infringement

The Associations computer systems and networks must not be used to download, or otherwise handle illegal and/or unauthorised copyrighted content. Any of the following activities constitute violations of the unacceptable use policy if done without permission of the copyright owner:

- copying and sharing images, music, or other copyrighted material using P2P file sharing or unlicensed CD's and DVD's;
- posting or plagiarising copyrighted material; and
- downloading copyrighted files which the employee has not already legally procured.

This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than listed above.

Streaming Media

Streaming media can use a great deal of network resources and thus must be used carefully and for job functions only.

Monitoring and Privacy

Users should expect no privacy when using the Association network or resources. Such use may include but is not limited to the transmission and storage of files, data and messages. The Association reserves the right to monitor all use of the computer network. To ensure compliance with the Associations policies this may include the interception and review of any emails or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removeable media along with all internet-based activity.

Personal Computer Usage

Personal usage of association computer systems is permitted as long as such usage follows pertinent guidelines in this document and does not have a detrimental effect on the Association or on the users' job performance.

POLICIES & PROCEEDURES - COMPUTER USE POLICY

Remote Desktop Access

Remote desktop access is available to those who require it as determined by the Committee. This access can be arranged through the Coordinator with the Associations external IT support. Use of remote access software or access services other than that provided by the Association is prohibited.

Circumvention of Security

Using Association-owned or Association-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

Use for Illegal Activities

No Association-owned or Association-provided computer systems may be knowingly used for activities that are considered illegal under the local, state, federal or international law. Such actions may include, but are not limited, the following:

- unauthorised Port Scanning;
- unauthorised Network Hacking;
- unauthorised Packet Sniffing;
- unauthorised Packet Spoofing;
- unauthorised Denial of Service;
- unauthorised Wireless Hacking;
- any act that may be considered an attempt to gain unauthorised access to or escalate privileges on a computer or other electronic system;
- acts of Terrorism;
- identity Theft;
- spying;
- downloading, storing or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes;
- downloading, storing or distributing copyrighted material.

The Association will take all necessary steps to report and prosecute any violations of this policy.

POLICIES & PROCEDURES - COMPUTER USE POLICY

Non-Association Owned Equipment

Non-Association-provided equipment is expressly prohibited on the Association's network.

Personal Storage Media

The Association does not restrict the use of personal storage media on Association network provided that the guidelines for data confidentiality are followed. The user must take reasonable precautions to ensure viruses, trojans worms, malware, spyware and other undesirable security risks are not introduced into the Association network. Such storage devices referred to in this clause includes but is not limited to:

- USB or flash drives;
- external hard drives;- personal music/media players;
- CD/DVD writers.

Software Installation

Installation of non-Association supplied programs is prohibited. Numerous security threats can masquerade as innocuous software – malware, spyware and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on systems performance. IT support must be contacted to approve and install any software.

Software found on computers that is not approved may be removed or blocked periodically.

POLICIES & PROCEDURES - COMPUTER USE POLICY

Reporting of Security Incident

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify the Chairperson and IT Support. Examples of incidents that require notification include:

- suspected compromise of login credentials (username, password, etc);
- suspected virus/malware/Trojan infection;
- loss or theft of any device that contains Association information;
- any attempt by any person to obtain a user's password over the phone or by email;
- any other suspicious event that may impact the Associations information security.

Users must treat a suspected security incident as confidential information and report the incident only to IT and the Chairperson. Users must not withhold information relating to a security incident or interfere with an investigation. If the threat relates to a user's PC, please make sure you are disconnected from the network and powered off as soon as possible.

Enforcement

Violations may result in disciplinary action which may include suspension, restriction of access or more severe penalties up to and including termination of employment of service.

Where illegal activities or theft of association property (physical or intellectual) are suspected, the Association may report such activities to the applicable authorities.

POLICIES & PROCEEDURES - COMPUTER USE POLICY

Definitions

Blogging: The process of writing or updating 'blog, which is an online, user-created journal (short for 'weblog').

Instant Messaging: A text-based computer application that allows two or more internet-connected users to 'chat' in real time.

Remote Desktop: Remote control software that allows users to connect to, interact with and control a computer over the internet just as if they were sitting in front of that computer.

Streaming Media: Information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing the clip before the entire down load has completed.