|  |  |  |
| --- | --- | --- |
| Image result for hcc hamilton clermont | **Policy Title:** **Acceptable Use of Information Technology** | **Policy Owner:** Executive Director |
| **Policy Category:** Information TechnologyInformation Security  | **Policy Number:**  | **Responsible Office(s):** Information Technology |
| **Policy Applicable For:**Staff, Contractors, Guests, Customers, Business Partners |  | **Effective Date:** |

Table of Contents

[1.0 Purpose 1](#_Toc37683790)

[2.0 User Responsibilities 1](#_Toc37683791)

[3.0 Unacceptable Use of HCC Resources 2](#_Toc37683792)

[4.0 Data Confidentiality 3](#_Toc37683793)

[5.0 Expectation of Privacy 3](#_Toc37683794)

# 1.0 Purpose

The computing resources at the Hamilton Clermont Cooperative (HCC) support the educational, instructional, operational, and administrative activities and the use of these resources is a privilege that is extended to members of the HCC community.

This document formalizes the policy for employees and contractors ("users") on acceptable use of information technology resources; ("ITRs"), including any HCC owned, licensed, or managed hardware and software, and use of the HCC network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

# 2.0 User Responsibilities

It is the responsibility of any person using HCC information technology resources to read, understand, and follow this policy. In addition, users are expected to exercise reasonable judgement in interpreting this policy and in making decisions about the use of ITRs. Any person with questions regarding the application or meaning of this policy should seek clarification from appropriate management. Failure to observe this policy may subject individuals to disciplinary action, including termination of employment. Individuals are also subject to federal, state and local laws governing many interactions that occur on the Internet. These policies and laws are subject to change as state and federal laws develop and change.

Additionally, to ensure continued confidentiality, integrity, and availability of HCC information technology resources:

1. Only HCC email and social media accounts are used to conduct HCC official business.
2. Only HCC approved collaboration, application and storage cloud services are to be used for HCC or customer data.
3. Users must comply with the Ohio Data Retention Laws and HCC data retention schedules.
4. Users must ensure that the transmission or handling of personally identifiable information (PII) or other sensitive data is encrypted or has adequate protection.
5. All devices connected to the HCC Network must have updated malware/anti-virus protection.
6. Users must ensure all files downloaded from an external source to the HCC Network or any device connected to the HCC Network, or any other electronic medium, are scanned for malicious software such as viruses, Trojan horses, worms or other malicious code.
7. Access to the Internet or HCC network from HCC-owned, home based, devices must adhere to all acceptable use policies. Employees must not allow family members or other non-employees to access nonpublic accessible information systems.
8. Users must report any weaknesses in security or suspicious activity that may result in a security incident to the Information Security Officer and their direct supervisor for follow-up investigation. Weaknesses in computer security include unexpected software or system behavior, which may indicate an unauthorized disclosure of information or exposure to security threats.
9. Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of information.
10. Users must report any incidents of possible misuse or violation of the Acceptable Use Policy.

# 3.0 Unacceptable Use of HCC Resources

Unless such use is reasonably related to a user's job, or explicitly approved by HCC leadership:

1. Users may not connect personal devices to the HCC Network without express written permission from Director of IT and Information Security Officer. This requirement does not apply to users who connect to the HCC-supplied “guest” Wi-Fi network.
2. Personally owned “smart” devices may not be connected to the HCC Network. “Smart” devices, commonly referred to as the “Internet of Things,” include smart thermostats, smart appliances, or wearable technologies.
3. Users must not attempt to access any data, documents, email correspondence, and programs contained on systems for which they do not have authorization.
4. Systems administrators and authorized users must not divulge remote connection information or other access points to information technology resources to anyone without proper authorization.
5. Users must not share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or other similar information or devices used for identification and authorization purposes.
6. Users must not make unauthorized copies of copyrighted or HCC-owned software.
7. Users may not download, install or distribute software to HCC-owned devices unless it has been approved by the Director of IT and Information Security Officer.
8. Users must not download HCC or customer data to personally owned devices.
9. Users must not engage in activity that may degrade the performance of information resources, deprive an authorized user access to resources, obtain extra resources beyond those allocated, or circumvent information security measures.
10. Users must not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of information technology resources unless approved in writing by the Director of IT and Information Security Officer.
11. Users must not purposely engage in activity that is illegal according to local, state or federal law, or activity that may harass, threaten or abuse others, or intentionally access, create, store or transmit material which may be deemed to be offensive, indecent or obscene.
12. Other specific prohibitions include, but are not limited to, the following:
	1. Unsolicited commercial advertising by public employees. For the purpose of
	2. in furtherance of any illegal act, including violation of any criminal or civil laws or regulations, whether state or federal
	3. for any political purpose
	4. or any commercial purpose
	5. to infringe any intellectual property rights
	6. to gain, or attempt to gain, unauthorized access to any computer or network
	7. for any use that causes interference with or disruption of network users and resources, including propagation of computer viruses or other harmful programs
	8. to intercept communications intended for other persons
	9. to misrepresent either the HCC or a person's role at the HCC
	10. to distribute chain letters
	11. to access online gambling sites or
	12. to libel or otherwise defame any person
	13. any activity that disrupts, degrades, harms or threatens to harm any HCC or customer personnel, equipment, services, data, or network resources.

# 4.0 Data Confidentiality

In the course of performing their jobs, HCC employees and contractors often have access to confidential or proprietary information, such as personal data about identifiable individuals or commercial information about business organizations. Under no circumstances is it permissible for employees or contractors to acquire access to confidential data unless such access is required by their jobs. Under no circumstances may employees or contractors disseminate any confidential information that they have rightful access to, unless such dissemination is required by their jobs and in compliance with HCC policies and procedures.

# 5.0 Expectation of Privacy

HCC-provide information technology resources remain the property of the Hamilton Clermont Cooperative (HCC) and are to be used in conformance with this policy. HCC retains, and when reasonable and in pursuit of legitimate needs for investigation, supervision, control, and the efficient and proper operation of the workplace, will exercise the right to inspect any user's computer, any data contained in it, and any data sent or received by that computer. Users should be aware that network administrators, in order to ensure proper network operations, routinely monitor network traffic. Use of HCC ITRs constitutes express consent for HCC to monitor and/or inspect any data that users create or receive, any messages they send or receive, and any web sites that they access.