# County of Clinton
# Information Technology Policy

# Acceptable Use of Information Technology Resources Policy

**Adopted:** **June 9, 2021**

## 1.0 Purpose and Benefits

Appropriate organizational use of information and information technology (IT) resources, and effective security of those resources, require the participation and support of the County of Clinton's workforce (users). Inappropriate use exposes the County of Clinton (County) and its component agencies and departments (departments) to potential risks including virus attacks, compromise of network systems and services, and legal issues.

## 2.0 Authority

This policy has been created by the Clinton County Department of Information Technology, under the direction of the Director of Information Technology, and approved under the authority of the Clinton County Legislature.

## 3.0 Scope

This policy applies to users of any County systems, information, or physical infrastructure, regardless of its form or format, created or used to support the County. It is the user's responsibility to read and understand this policy and to conduct their activities in accordance with its terms. In addition, users must read and understand the County's Information Security Policy and its associated policies and standards.

## 4.0 Information Statement

Except for any privilege or confidentiality recognized by law, individuals have no legitimate expectation of privacy during any use of the County's IT resources or in any data on those resources. Any use may be monitored, intercepted, recorded, read, copied, accessed or captured in any manner including in real time, and used or disclosed in any manner by authorized personnel without additional prior notice to individuals. Periodic monitoring will be conducted of systems used, including but not limited to: all computer files; and all forms of electronic communication (including email, text messaging, instant

messaging, telephones, computer systems and other electronic records). In addition to the notice provided in this policy, users may also be notified with a warning banner text at system entry points where users initially sign on about being monitored and may be reminded unauthorized use of the County's IT resources is not permissible.

The County may impose restrictions, at the discretion of County, department, or IT management, on the use of a particular IT resource. For example, the County may block access to certain websites or services not serving legitimate business purposes or may restrict user ability to attach devices to the County's IT resources (e.g., personal USB drives, smartphones).

Users accessing the County's applications and IT resources through personal devices must only do so with prior approval or authorization from both department management and the Director of IT.

## 4.1 Acceptable Use

All uses of information and IT resources must comply with all County policies, standards, procedures, and guidelines, as well as any applicable license agreements and laws including Federal, State, local and intellectual property laws.

Consistent with the foregoing, the acceptable use of information and IT resources encompasses the following duties:

- Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information;
- Protecting County information and resources from unauthorized use or disclosure;
- Protecting personal, private, sensitive, or confidential information from unauthorized use or disclosure;
- Observing authorized levels of access and utilizing only approved IT technology devices, software, and services; and
- Immediately reporting suspected information security incidents or weaknesses to the appropriate manager and the Information Security Officer (ISO)/designated security representatives.

## 4.2 Unacceptable Use

The following list is not intended to be exhaustive, but is an attempt to provide a framework for activities that constitute unacceptable use. Users, however, may be exempted from one or more of these restrictions during their authorized job responsibilities after approval from both department management and the Director of IT, in consultation with County IT staff (e.g., storage of objectionable material in the context of a disciplinary matter).

Unacceptable use includes, but is not limited to, the following:

- Unauthorized use or disclosure of personal, private, sensitive, and/or confidential information;
- Unauthorized use or disclosure of County information and resources;

- Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;
- Attempting to represent the County in matters unrelated to official authorized job duties or responsibilities;
- Connecting unapproved devices to the County's network or any IT resource;
- Connecting County IT resources to unauthorized networks;
- Connecting to any wireless network while physically connected to the County's wired network;
- Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with County policies;
- Connecting to commercial email systems (e.g., Gmail, Hotmail, Yahoo) without prior approval from department management and the Director if IT (organizations must recognize the inherent risk in using commercial email services as email is often used to distribute malware);
- Using County IT resources to circulate unauthorized solicitations or advertisements for non-County purposes including religious, political, or not-for-profit entities;
- Providing unauthorized third parties, including family and friends, access to the County's IT information, resources or facilities;
- Using County information or IT resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions);
- Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using County IT resources; and
- Tampering, disengaging, or otherwise circumventing County or third-party IT security controls.

## 4.3 Occasional and Incidental Personal Use

With permission from the individual's department head, occasional, incidental, and necessary personal use of IT resources is permitted, provided such use: is otherwise consistent with this policy; is limited in amount and duration; and does not impede the ability of the individual or other users to fulfill the County's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization. Exercising good judgment regarding occasional and incidental personal use is important. The County may revoke or limit this privilege at any time.

## 4.4 Individual Accountability

Individual accountability is required when accessing all IT resources and County information. Everyone is responsible for protecting against unauthorized activities performed under their user ID. This includes locking your computer screen when you walk away from your system, and protecting your credentials (e.g., passwords, tokens or similar technology) from unauthorized disclosure. Credentials must be

treated as confidential information, and must not be disclosed or shared. All passwords must comply with the County's Password and Authentication Standard.

### 4.5 Restrictions on Off-Site Transmission and Storage of Information

Users must not transmit restricted County, non-public, personal, private, sensitive, or confidential information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct the County's business unless explicitly authorized by both their designated department head and the Director of IT. Users must not store restricted County, non-public, personal, private, sensitive, or confidential information on a non-County issued device, or with a third-party file storage service that has not been approved for such storage by County IT.

Devices that contain County information must be attended at all times or physically secured and must not be checked in transportation carrier luggage systems.

### 4.6 User Responsibility for IT Equipment

Users are routinely assigned or given access to IT equipment in connection with their official duties. This equipment belongs to the County and must be immediately returned upon request or at the time an employee is separated from the County service. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to the County. Should IT equipment be lost, stolen or destroyed, users are required to provide a written report of the circumstances surrounding the incident to their department head and the Director of IT. Users may be subject to disciplinary action which may include repayment of the replacement value of the equipment. The County has the discretion to not issue or re-issue IT devices and equipment to users who repeatedly lose or damage IT equipment.

## 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all County policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, departments shall request an exception through the Chief Information Security Officer's exception process.

## 6.0 Definitions of Key Terms

| Term | Definition |
|---|---|
| **Information Technology Resources** | Equipment or services used to input, store, process, transmit, and output information, including, but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, Internet, email, and social media sites. |

# 7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

**Director of Information Technology**
**Clinton County Department of Information Technology**
**137 Margaret Street, Suite 202**
**Plattsburgh, NY 12901**

# 8.0 Revision History

This policy shall be subject to periodic review to ensure relevancy.

| Date | Description of Change | Reviewer |
|---|---|---|
| **06/09/2021** | **Initial policy adoption** | **David Randall, Director of Information Technology** |

# 9.0 Related Documents