

WARREN COUNTY COMPUTER USAGE POLICY

Introduction

Username: last name first initial

Password: pass (To change password hit ctrl+alt+delete)

E-mail address: last name first initial@warrencountyny.gov

The computer, software, Internet connection and e-mail system supplied by Warren County for use by Warren County officials and/or employees is owned and/or licensed for use by Warren County.

While our direct connection to the internet offers a cornucopia of potential benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. As presented in greater detail, that may mean preventing machines with sensitive data or applications from connecting to the internet entirely, or it may mean that certain users must be prevented from using certain Internet features like file transfers. The overriding principle is that security is to be everyone's first concern. An Internet user can be held accountable for any breaches of security or confidentiality.

Certain terms in this policy should be understood expansively to include related concepts. Document covers just about any kind of file that can be read on a computer screen as if it were a printed page, including HTML files read on an Internet browser, any file meant to be accessed by a word processing or desk-top publishing program or its viewer, or the files prepared for the Adobe Acrobat reader and other electronic publishing tools. Graphics includes photographs, pictures, animations, movies, or drawings. Display includes monitors, flat-panel active or passive matrix displays, monochrome LCDs, projectors, televisions and virtual-reality tools.

All employees granted Internet access with County facilities will be provided with a copy of this policy. All internet users must sign the statement at the end of this policy.

INTERNET POLICY PROVISIONS

A) Management and Administration

1. The County has software and systems in place that can monitor and record all Internet usage. We want you to be aware that our security systems have the potential to record (for each and every user) each World Wide Web site visit, each chat, newsgroup or email message, and each file transfer into and out of our internal networks, and we reserve the right to do so at any time. No employee should have any expectation of privacy as to his or her Internet usage. Periodic review of Internet activity will analyze usage patterns to assure that County Internet resources are devoted to maintaining the highest levels of productivity.

2. We reserve the right to inspect any and all files downloaded from the Internet and stored in private areas of our network in order to assure compliance with policy.

3. The display of any kind of sexually explicit image or document on any County system is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.

4. The County has available independently supplied software to identify inappropriate or sexually explicit Internet sites. We may block access from within our networks to all such sites. If you find yourself connected accidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.

5. This County's Internet facilities and computing resources must not be used knowingly to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any material way. Use of any County resources for illegal activity is grounds for disciplinary action, and we will cooperate with any legitimate law enforcement activity.

6. Any software or files downloaded via the Internet into the County network become the property of the County. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

7. No employee may use County facilities knowingly to download or distribute pirated software or data.
8. No employee may use the County's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.
9. No employee may use the County's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
10. Each employee using the Internet facilities of the County shall identify himself or herself honestly, accurately and completely (including one's County affiliation and function where requested) when participating in chats or newsgroups, or when setting up accounts on outside computer systems.
11. The County retains the copyright to any material posted to any forum, newsgroup, chat or World Wide Web page by any employee in the course of his or her duties.
12. Employees are reminded that chats and newsgroups are public forums where it is inappropriate to reveal confidential County information. Employees releasing protected information via a newsgroup or chat - whether or not the release was inadvertent - will be subject to disciplinary action as outlined in existing policies and procedures.
13. Use of County Internet access facilities to commit infractions such as misuse of County resources, sexual harassment and misappropriation or theft of related properties are also prohibited by general County policy.
14. E-mail is a strategic business tool to facilitate communication between employees and other business organizations. Warren County's e-mail systems are County owned or licensed property and are intended to be used for official County business. All messages sent or received via e-mail are County property. It is against County policy to use e-mail for any unlawful endeavor.

Additional Provisions:

1. The County will provide Internet access to those employees who demonstrate a legitimate business need.
2. Since a wide variety of materials may be deemed offensive by colleagues, suppliers or the general public, it is a violation of County policy to store, view, print or redistribute any document or graphic file that is not directly related to the user's job or the County's business activities.
3. The County will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries and archives on individuals' Internet activities.
4. Employees with Internet access must take particular care to understand the copyright, trademark, libel, slander and public speech control laws of all agencies in which this County maintains a business presence, so that our use of the Internet does not inadvertently violate any laws which might be enforceable against us.
5. Employees with Internet access may download software with direct business use, after Department Head approval and review by the Director of Information Technology, and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license.
6. Employees with Internet access may not use County Internet facilities to download entertainment software or games.
7. Employees with Internet access may not use County Internet facilities to download images or videos unless there is an explicit business related use for the material.
8. Employees with Internet access may not upload any software licensed to the County or data owned or licensed by the County without explicit authorization from the Department Head responsible for the software or data.
9. Any form of computerized gambling is prohibited.
10. Employees requiring access to otherwise prohibited websites may gain access after Department Head approval and review by the Director of Information Technology.
11. Any on-line presence and its content must first be approved by the Department Head, Director of Information Technology, County Administrator and Committee with oversight of the Department. Subsequent changes/updates to content will require the same approval.

B) Technical

1. User ID's and passwords help maintain individual accountability for Internet resource usage. Any employee who obtains a password or ID for an Internet resource must keep that password confidential. County policy prohibits the sharing of user ID's or passwords obtained for access to Internet sites.

2. Employees should schedule communications-intensive operations such as large file transfers, video downloads, mass e-mailings and the like for off-peak times and only after approval from Director of Information Technology.

C) Security

1. The County has installed a variety of firewalls, proxies, Internet address screening programs and other security systems to assure the safety and security of the County's networks. Any employee who attempts to disable, defeat or circumvent any County security facility will be subject to immediate disciplinary action.

2. Files containing sensitive County data cannot be transferred without Department Head approval and, if approved, information must be encrypted prior to distribution via the Internet.

3. Computers that use their own modems to create independent data connections sidestep our network security mechanisms. An individual computer's private connection to any outside computer can be used by an attacker to compromise any County network to which that computer is attached. That is why any computer used for independent dial-up or leased-line connections to any outside computer or network must be physically isolated from the County's internal networks. (Major on-line services such as CompuServe and America Online, and content providers such as Lexis-Nexis, can be accessed via firewall-protected Internet connections, making insecure direct dial-up connections generally unnecessary).

4. Only those Internet services and functions with documented business purposes for this County will be enabled at the Internet firewall.

Password Policy

All passwords used by employees to accessing County network, data or information systems must meet or exceed the standards defined by the NYS Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) in the publication PO3-002 V2.1 Information Security Policy;

As such the following specific criteria must be met:

1. Passwords are not to be written down or stored in an unencrypted form
2. Temporary passwords must be changed upon first use
3. Passwords must be a minimum of 8 characters in length
4. Passwords must be changed at least every 90 days
5. A password cannot be reused for a minimum of one year
6. Passwords must also meet the following requirements
 - They do not contain all or part of the user's account name or common word
 - Passwords must contain characters from each of the following 3 categories:
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Base 10 digits (0 through 9)

Please read and sign the following statement and return to IT.

“I have received a written copy of **Warren County’s Computer Usage Policy**. I fully understand the terms of this policy and agree to abide by them. I realize that the County’s security software may record for management use the Internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive has the potential to be recorded and stored in an archive file for management use. I know that any violation of this policy could lead to disciplinary action or even criminal prosecution. I understand that any use of County owned, leased or licensed computer equipment and/or software for Internet access constitutes consent to monitoring, recording and inspection of downloaded files and e-mail, as set forth in this policy.”

Signed

Date

Print Name

Department