

Acceptable Use Policy

1.0 Overview

The Whiteside Regional Office of Education is committed to protecting its employees, partners, and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of the Whiteside Regional Office of Education. These systems are to be used for business purposes in serving the interests of the company, and of our clients, and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Whiteside Regional Office of Education employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

The Whiteside Regional Office of Education supports the use of the office computers, network, and Internet in order to facilitate program enhancement and office efficiency through interpersonal communications, access to information, research, and collaboration.

The electronic information available to staff does not imply endorsement of the content by the Regional Office of Education, nor does the Regional Office of Education guarantee the accuracy of information received on the Internet. The Regional Office of Education shall not be responsible for any information that may be lost, damaged, or unavailable when using the network or for any information that is retrieved via the Internet.

The Whiteside Regional Office of Education shall not be responsible for any unauthorized charges or fees resulting from access to the Internet by the Whiteside Regional Office of Education staff.

The Whiteside Regional Office of Education establishes that use of the Internet is a privilege, not a right.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at the Whiteside Regional Office of Education. These rules are in place to protect the employee and the Whiteside Regional Office of Education. Inappropriate use exposes the Whiteside Regional Office of Education to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at the Whiteside Regional Office of Education, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Whiteside Regional Office of Education.

4.0 Policy

4.1 General Use and Ownership

1. While the Whiteside Regional Office of Education's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the Whiteside Regional Office of Education. Because of the need to protect the Whiteside Regional Office of Education's network, management cannot guarantee the confidentiality of information stored on any network device belonging to the Whiteside Regional Office of Education.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. For security and network maintenance purposes, authorized individuals within the Whiteside Regional Office of Education may monitor equipment, systems, and network traffic at any time per its audit policy.
4. The Whiteside Regional Office of Education reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface, for information contained on Internet/Intranet/Extranet-related systems, should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every six months.
3. All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
5. Postings by employees from a Whiteside Regional Office of Education email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Whiteside Regional Office of Education unless posting is in the course of business duties.
6. All hosts used by the employee that are connected to the Whiteside Regional Office of Education Internet/Intranet/Extranet, whether owned by the employee or the Whiteside Regional Office of Education, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
7. Employees must use extreme caution when opening e-mail attachments received from unknown senders which may contain viruses, e-mail bombs, or Trojan horse code.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the Whiteside Regional Office of Education authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the Whiteside Regional Office of Education-owned resources.

The regional superintendent shall have the authority to determine what inappropriate use is, and his/her decision is final.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Whiteside Regional Office of Education.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Whiteside Regional Office of Education does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using the Whiteside Regional Office of Education computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction as well as inappropriate language or profanity.
7. Making fraudulent offers of products, items, or services originating from any Whiteside Regional Office of Education account.
8. Making use of the network for commercial or for-profit purposes.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network, or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, the Whiteside Regional Office of Education employees to parties outside the Whiteside Regional Office of Education.
16. Using the Whiteside Regional Office of Education computing asset for political lobbying.
17. Impersonation of another user, anonymity, and pseudonyms.
18. Obtain or modify files, passwords, and data belonging to other users.
19. Destruction, modification, or abuse of network hardware or software.
20. Loading or use of unauthorized games, programs, files, or other electronic media.
21. Access obscene or pornographic material.
22. Quoting personal communications in a public forum without the original author's prior consent.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material, to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone, or paging whether through language, frequency, or size of messages.
3. Using the mail system to transmit material likely to be offensive or objectionable to recipients.
4. Unauthorized use, or forging, of email header information.
5. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
7. Use of unsolicited email originating from within the Whiteside Regional Office of Education's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the Whiteside Regional Office of Education.
8. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

1. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
2. The network user shall be responsible for damages to equipment, systems, and software resulting from deliberate or willful acts.
3. Illegal use of the network, intentional deletion or damage to files of data belonging to others, copyrighting violations, or theft of services will be reported to the appropriate legal authorities for possible prosecution.
4. General rules for behavior and communications apply when using the Internet in addition to the stipulations of this policy. Inappropriate, unauthorized, and illegal use will result in loss of access or employment termination.
5. Vandalism will result in cancellation of access privileges or possible employment termination. This includes, but is not limited to, the uploading or creation of computer viruses.

6.0 Definitions

Term	Definition
<i>Spam:</i>	Unauthorized and/or unsolicited electronic mass mailings.
<i>Vandalism:</i>	Any malicious attempt to harm or destroy data of another user, Internet, or other networks.

7.0 Revision History

4/21/2004
5/14/2004