



E-Mail and Electronic Use Policy

- 1.0 Purpose.** The proliferation of electronic mail (e-mail) systems in the corporate workplace has brought with it numerous changes to internal and external communications. The duty of RCWE and NWPAWIB is to educate our employees and partners on the proper use of such systems in order to protect the success of the corporation and the relationships with its employees, vendors, customers and prospects.
- 2.0 Policy.** RCWE and NWPAWIB have established numerous office sites within our geographical boundaries and have acquired equipment and software packages to aid us in our internal and external communications through the use of e-mail. Employees of our company are encouraged to use e-mail for company-related activities and to facilitate the efficient exchange of useful information within the framework of the appropriate federal, state, and local laws and statutes. Access to e-mail is a privilege and certain responsibilities accompany that privilege. Users of e-mail are expected to be ethical and responsible in their use. To ensure maximum benefits from e-mail, a clear defined balance between the need for open communication and the protection of the company's assets is critical. The company e-mail system should be used for business purposes only. If there is a desire to send personal e-mail from the office, it is recommended to use your own e-mail software, e-mail account and ISP, or use one of the free e-mail services available on the Web. Although this policy is directed to the use of e-mail, it works in conjunction with the company's Responsible Computer and Network Usage Policy.
- 3.0 Privacy.** Company officers and System Administrators have the privilege to monitor e-mail messages for specific reasons, such as evaluating the effectiveness and operation of the e-mail system, troubleshooting to find lost and undelivered messages, investigation of suspected criminal acts, breach of security or other corporate policies, and recovery from system failures. Because of these reasons, and the company's right to reasonable intrusions, the physical security and total privacy of e-mail cannot be guaranteed. Employees should assume that all transmissions via e-mail are publicly available information which can be intercepted by individuals other than the intended recipient(s). Employees can expect the System Administrator to conduct bi-monthly monitoring of e-mail effectiveness and system operation with random selection of messages. Please understand that reading e-mail for any reasons other than those stated above, is a violation of company policy.
- 4.0 Size of Messages and Attachments.** Please use discretion when sending files or attachments and be sensitive to your number of recipients. A typical rule-of-thumb would be to limit them to 500KB. Larger files and attachments should be approved by the Systems Administrator before sending.
- 5.0 Message Retrieval, Retention & Deletion.** Message retrieval must be performed on a timely basis and should be done at least once a week.



5.1 Retention of messages fills up large amounts of storage space on the network server and personal hard disks, and can slow down the performance of both the network and individual personal computers. Employees should audit their stored e-mail messages monthly to identify messages that are no longer needed. No long-term archiving of e-mail will be performed by the company; therefore each user will be responsible for their own archiving of e-mail on their personal computers. Short-term backup will be performed by the company to aid in recovery from unexpected system problems or crashes.

5.2 Employees are to promptly delete any e-mail messages they send or receive that no longer require action or are necessary to an ongoing project or task. RCWE and NWPAWIB reserve the right to delete any e-mail from the network server that has been read and is more than 2 years old.

6.0 Acceptable E-mail Usage.

- For means of effective communication among employees and with related entities.
- For the transfer of sales quotes, project information, etc. with the company's customer base.
- For information exchange between the company and its hardware and software suppliers.
- For other administrative communications or activities in direct support of research or special instruction.

7.0 Unacceptable E-mail Usage.

- Sending harassing, abusive, offensive or discriminatory materials to or about others.
- Sending company confidential or sensitive information inside or outside of the organization without proper authorization. This would include user passwords, HR information, etc. This type of information should be transmitted via telephone or standard mail.
- Propagating computer worms, viruses or transmissions of any type which could cause disruption or disable the recipient's facilities or equipment.
- Extensive use for private, personal or for-profit business.
- Transmission of copyrighted or licensed material without the authorization of the owner.
- For purposes to incite criminal activities that break federal, state or local laws.
- For attempting to circumvent security or break into computer resources both internally and externally.
- To make distribution of unsolicited advertising, bulk e-mail or spam.
- Misrepresenting your identity.
- Intercepting, disrupting or altering e-mail packets.



8.0 Basic Do's & Don'ts.

Do's

- Respond quickly to e-mail as you would a telephone message.
- Enter a descriptive Subject line for each message.
- Always use the spell checker.
- Be concise and develop your message clearly for ease of understanding.
- Be aware of who your recipients are.

Don'ts

- Overuse carbon copies.
- Send attachments unless recipient wants them, expects them or needs them.
- Forward messages indiscriminately.
- Create or forward "chain-letter" e-mail.
- Type in all capitals, it's the same as SHOUTING!

9.0 Sanctions. RCWE and NWPAWIB have the right to apply any of the following sanctions or combination of sanctions to deal with the misuse of the e-mail system and related procedures:

- Counseling with the offender(s).
- Removing e-mail privileges from offender(s).
- Probation, with warning of suspension or discharge for continuing or recurring offenses.
- Evidence of illegal activities will be reported to the appropriate law enforcement authorities.

10.0 Policy Modification. RCWE and NWPAWIB reserve the right to modify this policy at any time. Employees and partners will receive prompt notification of all changes.



Responsible Computer & Network Usage Policy

1.0 Purpose. RCWE and NWPAWIB strive to promote the open exchange of ideas and information; however, an open system, synergetic computing network can be vulnerable to misuse or abuse. As more and more businesses become attached to the world-wide computing and information networks, it is more important than ever that this organization educate its staff about proper ethical behavior, responsible computing practices and copyright and licensing issues.

2.0 Definitions.

User - Someone who does not have system administrator responsibilities but makes use of the computer system or network.

System Administrator - Staff employed by the company whose responsibilities include system, site or network administration. System Administrators perform functions including, but not limited to, installing hardware and software, managing computers and networks, and keeping all computers operational.

User Account - Any combination of a user number, username or password that allows an individual access to any computer or network.

Data Owner - A manager, system administrator or individual that can authorize access to information, data or software and is responsible for its integrity and accuracy. The data owner could be the author of the information, etc. or the person that negotiated license agreements for the company's use of the information, data or software.

Information Resource - Information and data and the hardware and software that makes the information and data available to the user.

Desktop Computers - PC's, laptops, workstations or any class of small single-user systems. If owned or leased by the company or if owned by an individual and connected to a company-owned, leased or operated network. The use of these computers is covered by this policy and guidelines.

Server - A computer that contains information shared by other computers on a network.

Peripherals - Special purpose devices attached to a computer or network such as printers, plotters, scanners, etc.

Network - A group of computers and peripherals that share information electronically and are typically connected to each other by cable, communications or satellite link.

Normal Resource Limits - The amount of disk storage space, memory, printing, etc. allocated to your user account by that computer's system administrator.



Software - Programs, data and other information stored on magnetic media (tapes, disks, diskettes, cassettes, etc.), usually referred to as computer programs.

3.0 Policy. All personnel of the company and/or partners who use the company's computing and information resources must act responsibly and maintain a high standard of ethics. Access to the company computing facilities (including company-owned or leased computing hardware, software or data) is a privilege given to the company and partners staff. All users of these facilities must respect the rights of other users, respect the integrity of physical facilities and controls, and respect all pertinent copyright laws, license and contractual agreements.

Access to company information resources may be granted by the owners of that information based on the owner's judgment of the following factors:

- . Relevant laws and contractual obligations
- . Requestor's need to know
- . The information's sensitivity
- . The risk of damage to or loss by the company

The company reserves the right to limit, restrict or extend computing privileges and access to its information resources. Data owners may allow individuals other than company staff, access to information for which they are responsible, so long as such access does not violate any license or contractual agreement, company policy, or any federal/state/county/local law or ordinance. Company computing facilities and user accounts are to be used for the company-related activities for which they are assigned and in accordance with all applicable laws. Company computing resources are not to be used for commercial purposes except as provided by other company policies. Users and system administrators must all guard against abuses that disrupt or threaten the integrity of all systems, including those at the company and those on networks to which the company's systems are connected. Access to information resources without proper authorization from the data owner; theft, malicious destruction, or unauthorized use of the company computing facilities; acts involving company computing facilities that impede or interfere with the business process; and intentional corruption or misuse of information resources are direct violations of the company's standards for conduct.

This policy should be followed by all staff in all company offices and locations. Periodic revisions to this policy may occur as circumstances, such as changes in technology, warrant.

4.0 User Responsibilities.

Users of the company's information resources or facilities have the following responsibilities:

- Use the company's computing facilities and information resources, including hardware, software, networks and user accounts, responsibly and appropriately, respecting the rights of other users and all contractual and license agreements.



- Do not install any software or hardware on your machine unless it has been given to you by the IT staff.
- All software that will reside on any company computer, or any individual's computer that is attached to the company network, will be approved by a systems administrator before installation. This includes desktop computers, network and business servers.
- All hardware to be used in conjunction with the company's network will be approved and installed by the system administrator.
- Use only those computers and user accounts for which you have authorization.
- Use all company-owned equipment for the purpose(s) for which they have been issued.
- Be responsible for all user accounts on your local machine and for protecting each account's password. (If someone learns your password, you should ask to have it changed.)
- Report unauthorized use of your user accounts to your supervisor or system administrator.
- Report any computing misuse or suspicion of misuse to your system administrator or supervisor.
- Cooperate with system administrator requests for information about your computing activities. Under certain circumstances, a system administrator is authorized to access your computer files.

5.0 System Administrator Responsibilities.

A system administrator's use of the company's information resources is governed by the same guidelines as any other user. However, a system administrator has additional responsibilities to the users of the network or computer systems that they administer. These are as follows:

- Manages company computer systems, networks and servers to provide the appropriate hardware and software for users to perform their day – to – day business.
- Responsibility for the security of company systems, networks and servers.
- Responsibility for the backup of data, programs and other information that reside on company servers.
- Must take reasonable and appropriate steps to continually verify that all hardware and software license agreements are faithfully executed on all systems, networks and servers for which they have responsibility.



POLICY – 304

Rev. Level: E

February 13, 2009

- Must take reasonable precautions to guard against corruption of data or software and damage to hardware or facilities.
- Must treat information about and information stored by system's users as confidential.

6.0 Misuse of Computing and Information Resources.

Misuse of computing and information resources by any user includes, but is not restricted to, the following:

- Attempting to install modify or remove computer hardware, software or peripherals without the proper authorization of a system administrator.
- Accessing desktop computers, servers, networks, software, computer data or information without proper authorization whether it be company-owned or company-connected.
- Circumventing or attempting to circumvent normal resource limits, logon procedures or security regulations.
- Using computing facilities, user accounts or computer data for purposes other than those for which they were intended or authorized.
- Sending any fraudulent electronic transmission, including but not limited to requests for confidential information, submission or authorization of purchase requisitions or journal vouchers.
- Violating any software license agreement or copyright, including copying or redistributing copyrighted software, data or reports without proper recorded authorization.
- Using the company's information resources to harass or threaten other users.
- Misuse of the internet for exchange of unethical or obscene data, information or documents.
- Interfering with other users' access to the company's computing facilities.
- Disclosing or removing proprietary information, software, printed reports or magnetic media without the explicit permission of the owner.
- Accessing other users' data, information or programs without the owner's or the owner's explicit written permission to the Chief Executive Officer or the MIS/IT Division.



POLICY – 304

Rev. Level: E

February 13, 2009

- Encroaching on others' use of the company's information resources, such as:
 - . Excessive game playing
 - . Excessive message sending
 - . Printing excessive copies of reports, documents, files, etc.
 - . Transmitting or receiving large files at inappropriate times
 - . Modifying system facilities, operating systems or normal resource limits
 - . Attempting to crash or tie up a company's computer, server or network
 - . Damaging or vandalizing company computing facilities, equipment or software

7.0 Process and Sanctions for Cases of Computing Misuse.

RCWE and NWPAWIB treat access and use violations of computing facilities and information resources very seriously. If a system administrator or supervisor has evidence that accidental or intentional misuse of information resources has occurred, and if that evidence points to the computing activities or the computer files of an individual, they have the obligation to pursue any or all of the following steps to protect the user community and the integrity of the company's information resources.

- Take immediate and appropriate action to protect the computer systems, user programs and files from damage.
- Notify the alleged abuser's supervisor of a pending investigation. The supervisor will promptly schedule an initial conference to discuss the problem and allow the individual to respond to the allegations. No written record needs to be filed at this level for instances resolved to the satisfaction of all parties without restriction of privileges.
- Suspend or restrict the alleged abuser's computing privileges during the investigation. A written record of this action and the reasons for it will be submitted by the supervisor to the personnel office. The alleged abuser may appeal a suspension or restriction and petition for reinstatement of their computing privileges. This should be submitted in writing to their immediate supervisor.
- Once a petition is submitted, further action is at the discretion of the appropriate company officers. If necessary, system administrators as well as company staff with special computing expertise may be called upon to advise the company officers on the implications of the evidence and the seriousness of the offense.
- If warranted, access to the alleged abuser's accounts, programs and data files may be required to finalize the investigation. Confidentiality of this material is important during this process.



POLICY – 304
 Rev. Level: E
 February 13, 2009

Misuse of computing privileges is subject to disciplinary action and sanctions which include:

- . Counseling with the offender(s)
- . Loss of computing privileges
- . Probation, with a warning of suspension or discharge
- . Suspension, with or without pay (based on the severity of the offense)
- . Discharge for cause
- . Civil or criminal prosecution

It should be understood that nothing in these guidelines precludes enforcement under the laws and regulations of the Commonwealth of Pennsylvania.

8.0 History.

Name	Date	Rev. Level	Description of change	Effective Date
		A	New policy	
Mark Canfield	2/25/2005	B	Changes in timeframe	
Mark Canfield	3/7/2005	C	Changes per Michele	
Mark Canfield	9/05/2006	D	Additional Changes	
Deb O’Neil	2/13/2009	E	Update logo, format, EO Officer	7/01/2009

Auxiliary aids and services are available upon request to individuals with disabilities.

Equal Opportunity Employer Program
 Paul Newlin – Equal Opportunity Officer
 Phone: (814) 333-1286
 TTY/TDD (814) 337-7205