

SECTION: ADMINISTRATION

SUBJECT: COMPUTER EQUIPMENT AND
INFORMATION PROCEDURES

Original Resolution No.: 06-01-27

Revised Resolution No.: 08-11-11

Computer Equipment and Information Procedures

The County of Warner recognizes the need to regulate the use of computer equipment and their associated information systems in order to govern their usage. In addition, this policy will assist in planning long term capital purchases, effectively and efficiently training staff to utilize these systems, as well as insuring that the Municipality's information systems are properly safeguarded.

Guidelines

1. Definitions

- a. User(s) - means all County Employees and Elected Officials
- b. Computer Information Systems - means all County stationary and portable computer hardware including attachments (printers, scanners, projectors, etc), personal computers (PC's), computer servers, software and programs.
- c. Management - means County Administrator, Public Works Superintendent, Ag Fieldman, Accountant and Bylaw Officer.
- d. County or Municipality - means "County of Warner No. 5"
- e. System Administrator - Individuals responsible for the ongoing administration and maintenance of county owned computer hardware and computer information systems.

2. Internet Access

- a. The use of the Internet is a privilege, not a right. Any unacceptable use, including the violation of the terms of this document and any additional rules the County may put in place from time to time regarding the use of the County's Computer Information Systems, may result in cancellation of access to the Internet. The County may deny, revoke, suspend, or close any user account at any time based upon a determination of unacceptable use by an account holder or user. The determination as to whether an unacceptable use has occurred will be decision solely within the discretion of the CAO, but may be appealed to the County Council.
- b. Streaming Media, such as Internet Radio, are not to be accessed, unless required to complete employment related activities or training. This is to preserve access to bandwidth for all users accessing the internet.
- c. The transmission or access to any material through the Internet, that is in violation of any International or Canadian law, whether Federal, Provincial, Municipal, or other status, is prohibited. In addition, the transmission of any material through the Internet, that is in violation of the laws of any other country or in violation of the rules or laws of any International Agency or Organization, is prohibited. The violation of Canadian law will be deemed to occur when there is a transmission or access through the Internet, to any material in breach of copyright, that is considered threatening or obscene, illegal material or material protected by trade secret. Commercial use of the County Computer Information Systems for product advertisement or political lobbying is prohibited. The uses mentioned in this paragraph are not an exclusive list, but are examples of unacceptable use that will result in the penalties outlined in this document.

- d. The County's Computer Information Systems may be used for personal communication, provided the use is consistent with the conditions and rules outlined in this document. Any personal use shall not conflict with an employee's work responsibilities. If use is required, it should be limited to coffee breaks and lunch time.
- e. The County reserves the right to review any material on user accounts and to monitor file server space in order to determine whether specific uses of the computer information system are inappropriate.

3. **Virus Detection and Removal**

- a. All personal computers and servers will be loaded with computer virus detection and removal software.
- b. All removable media (floppy disks, removable drives, CD-ROMs, zip disks, etc.) brought in from external sources must be scanned for viruses prior to the disks contents being copied onto the County's computer systems.

4. **Computer Equipment Security**

- a. All computer equipment will be documented for insurance purposes.
- b. All employees will ensure their office PC's will be shut down prior to leaving work. Computer servers will be left operating.
- c. Staff is responsible for the security of computer equipment when it leaves the workplace. If computer equipment leaves the workplace, prior approval is required from Management.

5. **New Users and Changes to Existing Users**

- a. New users will be given access to the computer information system only after a request has been received and approved by Management. This request will include computer applications, security access level, as well as the location of the PC that will be used.
- b. All users requiring computer access will be required to review these procedures at the time they are hired. Each user will be required to follow the rules, regulations and protocols outlined within this policy.
- c. Changes to a user's access will follow the same steps as adding a new user.
- d. Individual users are not permitted to install ANY software on their computers. All software must be approved by the System Administrator and the respective Department Head.

6. **Training and Staff Development**

- a. Training may be made available to users through outside training opportunities in the form of day and/or evening courses as outlined in the County's Employee Enhancement and Training Policy 120.16.

7. **Backups**

- a. Computer Information Systems will be programmed to perform nightly data backups of critical data as well as a weekly data backup of files on the server (F: Drive).
- b. Users are strongly encouraged to keep a copy of documents stored on their PCs and on the F: Drive in case of theft or equipment failure. Users are not required to keep data backups off site.
- c. Users retain the primary responsibility for ensuring their data is stored in accordance with the automated data backup systems. If users are uncertain regarding the process, they will review backup procedures with the System Administrator.

8. Equipment Maintenance, Redundancy, Power Protection

- a. All servers will be protected by an Uninterruptible Power Supply (UPS).
- b. Systems maintenance shall be provided to meet the County's needs in accordance with approved department budgets.

9. Computer Equipment

- a. Computer equipment shall be provided to meet the County's requirements as authorized by Management, in accordance with approved budgets. Software, hardware and related computer equipment purchase requests by users must be approved by Management prior to their purchase.
- b. Any upgrades to computer equipment will be conducted by the System Administrator as required.
- c. New computer equipment may be assigned to users with high performance needs, with the older computers being rolled down to other users, at the discretion of Management.
- d. Surplus computer equipment may be sold off through employee and/or elected official purchase plans. Items remaining unsold will remain in parts inventories, be sold to the general public, or disposed of in an environmentally appropriate manner.
- e. Surplus computer equipment to be sold must not contain any information or software that is the property of the County.
- f. Any and all programs and data that are on any county owned computer information system are subject to provisions of the Freedom of Information and Privacy legislation. As such, personal applications and data are not to be used on county owned computer equipment and information systems.
- g. Councillor laptop computers will be replaced on an as needed basis when they begin to fail or no longer meet the needs of the Councillor's duties.

10. Contractors and Technicians

- a. The use of outside resources (contractors and/or technicians) for repairs or maintenance shall only be done with prior approval of Management and the System Administrator.

11. Clarification of Procedures

- a. Any inquiries with respect to clarifying and confirming the intents and purposes for the above noted procedures should be directed to the System Administrator or Management.

12. WARRANTIES

- a. The Municipality makes no warranties of any kind, whether express or implied, for access to the Internet it is providing. The Municipality will not be responsible for any damages a user suffers. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by the Municipality's (either knowingly or unknowingly) or by the user's errors or omissions. Use of any information obtained through the Internet is at the user's own risk. The Municipality specifically denies any responsibility for the accuracy or quality of information obtained through the Internet service. All users need to consider the source of any information they obtain and how valid that information may be.

13. Network Security

- a. Security on any computer network is a high priority, especially when the network involves many users. A user must never allow other people to use their password. Users shall protect their passwords to facilitate network security, individual access privileges, and the ability to gain access to the network. If a user feels they can identify

a security problem on the network, they shall immediately notify the System Administrator and further, not demonstrate the problem to any other user. Except for those personnel who are originally assigned Network maintenance responsibilities, individuals who attempt to log on to the County's computer network, as a System Administrator, may result in cancellation of user privileges or other disciplinary action, unless they have received prior permission from the CAO.

14. **Vandalism and Harassment**

- a. Vandalism and harassment shall result in cancellation of a user's privileges or other disciplinary action including termination of employment. Vandalism is defined as any malicious attempt to harm, modify, or destroy data of another user, or of other networks that are connected to the Internet. This includes, but is not limited to, the uploading or creating of computer viruses. Harassment is defined as being persistent annoyance to another user(s), or as interfering with another user's work.

15. **E-mail Records Management Policy**

- a. Retention - Staff are encouraged to delete incoming E-mail messages DAILY, immediately after reading, replying, or taking other action confirming them. If an E-mail needs to be continually retained in a digital format, then a hard copy of it should be generated and placed in the proper paper file for further retention, in accordance with the County's Records Retention Bylaw.
- b. Backup - Because E-mail folders are located on the local system hard drives, they are not included in the scheduled automated back ups. If a user wishes to have their E-mail folders backed up, then special arrangements and procedures will need to be put in place.
- c. Content - It is the policy of the County that all E-mail shall be conducted in a professional and businesslike manner. The inclusion of remarks of a derogatory nature is strictly prohibited. Employees are advised, from a legal point of view, all E-mail messages are discoverable to the same extent as any other Municipal information. Employees are advised that the Municipality retains the right to access all E-mail files, just as it retains the right of access to any other Municipal property.

16. **E-mail Etiquette**

- a. All users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited, to:
 - i. Being Polite - Do not get abusive in your communication with others.
 - ii. Use appropriate language - Do not swear, use vulgarities, or any other inappropriate language.
 - iii. Do not engage in activities prohibited under municipal, provincial, federal, or international law.
 - iv. Do not reveal the personal information, such as address, phone numbers, etc, of any other County employee or colleagues.
 - v. Electronic mail (E-mail) is not private. People who operate the Computer Information System have access to all E-mail. Messages relating to, or in support of illegal activities, will be reported to the appropriate authorities and may result in the loss of user privileges, legal action and loss of employment with the County.
 - vi. Do not use the network in any way that will disrupt the use of the network by others users.

- vii. All communications and information accessible through the Internet should be assumed to be the private property of those who place it on the Internet.

17. **Unacceptable Material**

- a. Users may unintentionally encounter or access material which is unacceptable. It is the user's responsibility not to initiate access to such material that has been inadvertently gained. The Municipality shall not be liable for any decision by any service provider, or by the Municipality itself, to restrict access to, or to regulate access to material on the Internet. It is also understood by users that the Municipality does not control material on the Internet and therefore the Municipality is unable to control the content of data that a user may discover or encounter through the use of the Internet.

18. **Penalties for Improper Use**

- a. Any user violating these policy rules, applicable Provincial, Federal, Municipal, or International laws, other related misconduct and misuse of the County computer information systems is subject to loss of Internet privileges and any other disciplinary actions the Municipality determines to be appropriate, including termination from employment.