SECTION 6.6: TELECOMMUNICATIONS POLICY
(Computer, E-Mail & Voice-Mail Systems)

A. INTRODUCTION

The purpose of this policy is to establish guidelines to ensure the proper use of Hamilton County telecommunications systems (including e-mail, computer and voice-mail systems) by all users, including, but not limited to all employees, independent contractors, vendors and other persons or entities accessing or using county telecommunication resources and services.

The following policy, provisions, and conditions apply to all users of telecommunication resources and services, under the Board of County Commissioners, wherever the users are located. Violations of this policy may result in disciplinary action up to and including termination, and/or legal action.

B. GENERAL GUIDELINES

1. Telecommunication resources include, but are not limited to host computers, file servers, workstations, standalone computers, laptops, software, terminals, printers, telephones, faxes, and internal or external communications networks (Internet, intranet, commercial online services, social media tools, bulletin board systems, Ohio Department of Job and Family Services systems, county departmental systems, county wide area network [WAN], and e-mail systems) that are accessed directly or indirectly from county telecommunication facilities.

2. Each department shall have a designated System Administrator. The department head shall be System Administrator unless this function is specifically delegated to another employee in the department.

3. County telecommunication resources and services are property of the county and are intended for official county business purposes.

4. The BCC shall designate content managers who are authorized to post content to the BCC's social media pages and who are responsible for monitoring content broadcast via the BCC's social media channels. (Reference: Hamilton County Board of Commissioners Social Media Program Guidelines and Policies, adopted 05/25/2011, Vol. 322, Image 6745.)

5. The county has the right, but not the duty, to monitor any and all aspects of the telecommunications systems, including user e-mail, voice-mail (refer to Section C.), networks, intranet and Internet usage, to ensure compliance with this policy. This includes the right to perform manual or automated audits.

6. The telecommunications resources and services accessible to users are to assist them in the performance of their jobs. Users do not have a right to privacy in anything they create, send or receive on these systems.

7. All users have the responsibility to use all telecommunication resources and services in an efficient, effective, ethical, and lawful manner.

8. In no case shall software, unauthorized by the System Administrator, be installed or used on county equipment at any time.

9. No games are to be installed or played on county computer equipment at any time. Any games that come with the computer are to be deleted.

10. Users are not permitted to use the county network to play, “stream,” or download radio, audio (e.g., MP3), video or any multimedia files unrelated to county business.

11. A user’s ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless specifically authorized to do so by the operators of those systems and/or the department head.

12. The county’s Internet facilities and computing resources must not be knowingly used 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 of the county’s resources for illegal activity is grounds for discipline up to, and including, dismissal. The county will cooperate with any legitimate law enforcement activity.

13. E-mails and other documents and/or files that may be electronically transmitted are subject to the county’s Records Retention and Disposition Schedule.

14. To ensure policy compliance, this policy should be included in appropriate vendor contracts and professional services contracts. An annual review of this policy will be conducted with each employee during the year-end performance appraisal process.

15. Employees may use recording devices in the workplace environment only with the permission of all present.

C. E-MAIL / ELECTRONIC MAIL

1. Applicability

While this section principally applies to e-mail, the underlying principles and guidelines also apply to the voice-mail system.

2. Privacy

Users do not have a right to privacy in their work-related conduct or to the use of county-owned equipment or supplies. This includes all components of the e-mail system.

3. Management's Right to Access Information

a. The e-mail system has been installed to facilitate business communications among and between participating licensed users. While a user may have an individual mailbox and password on the system, the system, in its entirety, belongs to the county. Therefore, the contents of all e-mail messages are considered county property.

b. The county reserves the right to review contents of any user's e-mail communications at any time, for any reason, without prior notification. Users should also be aware that most e-mail messages are public records and, thus, are subject to disclosure to the general public.

Users should know that if the user deletes an e-mail message, this action does not ensure that the message has been deleted throughout the system.

c. All system passwords must be made available to the System Administrator upon demand. Users must not use passwords that are unknown to the System Administrator or install encryption programs without first receiving the approval of and then turning over encryption keys to the System Administrator.

4. Personal Use of E-Mail

The e-mail system is intended for official county business. While occasional personal use of e-mail is permitted, it must be responsible and clearly subordinate to business use. All messages are subject to management review and may be reviewed and disclosed by management, at its option, with or without cause and without regard to content. Users

should not create and/or transmit any message they would not want read by a third party.

5. Content of E-Mail Messages

a. E-mail messages should be written in a courteous, professional and business-like manner.

b. The county's e-mail system must not be used in any way that violates county policies, including e-mails that may be insulting, disruptive, harmful or offensive to other persons. Prohibited e-mail shall not be received, sent or forwarded. Prohibited e-mail includes, but is not limited to:

1.) Indecent messages, sexual innuendo, chain letters, harassing or threatening statements and material that may be hostile or offensive on the basis of age, gender, race, color, religion, national origin, or disability;

Receipt of unsolicited prohibited materials (e.g., sexually explicit, racist, etc.) does not violate this policy if the user immediately reports the receipt to his/her supervisor, does not further circulate the material and, under supervision of the System Administrator or supervisor, deletes it.

2.) Fund raising (unless consistent with the Board of County Commissioners' solicitation policy Section 6.8 and approved by the department head), commercial interests, partisan political opinions, campaigns or endorsements;

3.) Any message that encourages violation of county personnel policies (e.g., Section 6.1 Fair Employment Rights and Responsibilities), procedures, rules and/or regulations or any message that expresses knowledge or allegations of such violation.

6. Password Security and Integrity

a. Users may not intentionally intercept, eavesdrop, record, read, alter, or receive another user's e-mail messages without management's authorization. Other than the System Administrator, a user shall not use the password of another user without authorization of the System Administrator or department head.

b. Any suspected violations of this policy shall be reported to the System Administrator and department head.

7. Electronic Mailing Lists

a. Users must not subscribe to nonwork-related electronic mailing lists.

b. If users wish to subscribe to work-related mailing lists, they must notify their System Administrator of the subscription, as well as provide their password and instructions on how to remove their name from the mailing list.

D. INTERNET ACCESS

1. Purpose

The Internet provides a powerful medium for sharing a wide range of information. Through group communication, sharing of ideas and information can be accomplished with many jurisdictions to enhance public service and the business of government. The county provides Internet, intranet and network access at county expense to further county business.

2. Access

a. Users are expected to communicate in a professional manner that will reflect positively on themselves, their department/office and the county.

b. Access to the Internet is provided for official county use. Occasional and incidental personal use is permitted, subject to the limitations of this policy and subject to the operational needs of the department, as determined by the department head.

c. Restraint shall be exercised regarding the amount of time spent accessing the Internet.

d. Only authorized content managers shall post content to BCC social media sites on behalf of the BCC.

e. Users must not load/download any software that is not licensed by the county. Exceptions to this policy require the approval of the System Administrator.

f. Any software or files downloaded via the Internet into the county's network become the property of the county. Any such files or

software must be used only in ways that are consistent with their licenses or copyrights.

g. No users should knowingly use county Internet facilities to download or distribute pirated/stolen software or data.

h. No users should knowingly use the county's Internet facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the network and the privacy or security of another user.

i. Access is strictly prohibited involving transmissions set forth in the above Section C.5.b.1., 2., and 3. (examples of prohibited e-mail listed on page 4 of this policy).

E. PRIVACY

1. Users are reminded that any record generated in the workplace may be a public record. Electronic records are no exception. There is no reasonable expectation of privacy with regard to the use of the wide area network, the intranet or the Internet. User files and activity may be monitored by management at any time.

2. In the event of a public records request, any request received from the public with regard to accessing computer records shall be directed to the System Administrator.

F. SECURITY

1. Users are expected to be vigilant in maintaining system security. Users must not break into or exceed authorized limits when accessing any computer network. Furthermore, the entry or distribution of any self-replicating code, any file which may cause damage to any computer system, or any computer virus is strictly prohibited. No user should log on to any system with any identification or password other than that assigned to the user. Users should also follow all account authorization processes, log-on procedures and password protection features. Any user who suspects or detects a breach of security must immediately notify the System Administrator.

2. The county's Network Administrator shall employ virus protection software. Department heads and System Administrators may make additional virus protection software available to users. Users shall take reasonable precautions to not damage or overload their system. This includes the use of virus protection software when downloading any file or

copying from a diskette, compact disc or other media. When transferring a large file that will take an extended period of time, the System Administrator should be contacted. Users are also encouraged to cancel a mailing list subscription if they will be out of the office for an extended period of time.

3. The county has installed a variety of security systems to ensure the safety and security of the county's networks. Any user who attempts to disable, defeat or circumvent any county security facility, or assists anyone else in doing the same, will be subject to disciplinary action up to, and including, dismissal.

4. Computers that use modems to create independent data connections sidestep the county's 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. 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.) Therefore, if any such connections as described herein are necessary, the department head shall first give approval and then the Telecommunications Division of the Communications Center should be contacted for instructions on connecting safely.

5. Department heads and System Administrators shall take reasonable measures to ensure that e-mail messages are properly handled, including archiving and disposal. Archived messages should be organized and filed with descriptive titles for easy retrieval and messages should be deleted in the shortest time consistent with laws, policies and business needs. These actions must be consistent with the county's Records Retention and Disposition Schedule.

6. The connection of any wireless network device to any computer system that accesses the county's network, no matter where the computer is located (e.g., home, work, remote office, etc.), must be first approved by the department head and then the Telecommunications Division of the Communications Center.