RESOLUTION NO. 3-0799

TO THE HONORABLE IOWA COUNTY BOARD OF SUPERVISORS:

WHEREAS, the Committee on Information Systems, recognizes the County's significant investment in electronic communications devices such as e-mail, voice mail, computers, facsimiles, etc. to assist the Iowa County employees in performing their job duties;

WHEREAS, Committee on Information Systems, has reviewed the need for an establishment of an Iowa County policy that provides guidelines for the acceptable use of electronics communications in the workplace for the Iowa County employees;

WHEREAS, the Committee on Salary and Personnel also recognizes both the County's investment and the need for an acceptable usage policy and has reviewed and supports the recommendation of the Information Systems Committee for an Iowa County policy that provides the employees guidelines for the acceptable use of electronic communications in the workplace;

WHEREAS, the Electronic Communications Acceptable Usage Policy has been legally reviewed by the Wisconsin County Mutual Insurance Corporation through its loss control program of Personnel Policies and Procedures program;

NOW THEREFORE BE IT RESOLVED, that the Committee on Information Systems and the Committee on Salary and Personnel recommends that the following Electronic Communications Acceptable Usage Policy be included as an appendices to the Iowa County Personnel Policies. Also, that the policy be included in and adhered to in any and all departmental policies and or employee handbook(s) within Iowa County;

BE IT FURTHER RESOLVED, that the Committee on Information Systems and the Committee on Salary and Personnel on Salary and Personnel does hereby recommend that the Electronic Communications Acceptable Usage Policy be adopted by the County Board of Supervisors and that such policy apply to all Iowa County employees from this date forward;

Dated this 20th day of July 1999.

Respectfully submitted:

Neil Jefferson
Chairperson - Salary & Personnel

Robert Murphy
Chairperson – Information Systems

David Gollon, Jr.

David Blume

Jerome Laufenberg

LaVerne Clifton

Diane McGuire

Leo Hull

Thomas Paull

Neil Jefferson

Adopted this 20th day of July 1999.

Richard Scullion
Iowa County Chairman

ATTEST:

Gregory Klusendorf
Iowa County Clerk

CERTIFICATION OF ADOPTION

This is to certify that the above resolution was duly adopted by the County board of Iowa County on the 20th day of July 1999.

Gregory Klusendorf
Iowa County Clerk
Iowa County, Wisconsin

Electronic Communications - Acceptable Usage Policy July 1999

Iowa County Government provides access to a variety of electronic communications (e.g., e-mail, voice mail, computers, facsimiles, etc.) which include resources of the Internet to help you do your job faster and smarter, and be a well-informed Iowa County citizen. The facilities to provide that access represent a considerable commitment of county resources for telecommunications, networking, software, storage, etc., and all these things are regarded as county property. This Internet usage policy is designed to help you understand the County's expectations for the use of those resources in the particular conditions of the Internet, and to help you use those resources wisely.

While we've set forth explicit requirements for Internet usage below, we'd like to start by describing our Internet usage philosophy. First and foremost, the Internet for this county is a business tool, provided to you at significant cost. That means we expect you to use your Internet access exclusively for business-related purposes, i.e., to communicate with the public, suppliers, to research relevant topics and obtain useful government information. We insist that you conduct yourself honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as you would in any other county business dealings. To be absolutely clear on this point, all existing county policies apply to your conduct on the Internet, especially, but not exclusively, those that deal with intellectual property protection, privacy, misuse of county resources/county property, harassment which includes sexual harassment, information and data security, and confidentiality.

Unnecessary or unauthorized Internet usage causes network and server congestion. It slows other users, takes away from work time, consumes supplies, and ties up printers and other shared resources. Unlawful Internet usage may also garner negative publicity for the county and expose it to significant legal liabilities.

The chats, newsgroups and email elements of the Internet give each individual Internet user an immense and unprecedented reach to propagate Iowa County messages and tell our story. Because of that we must take special care to maintain the clarity, consistency and integrity of the county's image and posture. Anything that any one employee writes in the course of acting for the county on the Internet can be taken as representing the county's posture. That is why we expect you to forgo a measure of your individual freedom when you participate in chats or newsgroups on county business as outlined below.

While our direct connect 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 below, 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 the 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 includes but is not limited to the following as if it were a printed page, including the so-called HTML files read in an Internet browser, any files 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, animation's, movies, or drawings. **Display** includes monitors, flat-panel active or passive matrix displays, monochrome LCDs, projectors, televisions and virtual-reality tools.

Any employees granted Internet access with county facilities will be provided with a written copy of this policy.

Detailed Electronic Communications Policy Provisions

A) Management and Administration

1. No employee should have any expectation of privacy as to his or her Internet usage or any other county provided electronic communications, e.g., e-mail, voice mail, computers, facsimiles, etc.

2. We reserve the right to inspect any and all files stored in private areas of the 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. If you fmd yourself connected accidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately.

5. The county's Internet facilities and computing resources must not be 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 county resource for illegal activity is grounds for discipline up to and including immediate dismissal, and the county 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. An employee must obtain permission prior to downloading any software or files, which are licensed to copyrighted. Any such files or software may be used only in ways that are consistent with their licenses or copyrights and the county policies.

7. No employee may use county facilities to download or distribute pirated software or data.

8. No employee may use the county's Internet facilities to knowingly disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

9. No employee may use the county's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

10. Each employee using the Internet facilities of the county shall identify himself or herself honestly, accurately and completely (e.g., including one's county affiliation, position/title and function where requested) when participating in chats or newsgroups, or when setting up accounts on outside computer systems.

11. Only those employees or officials who are duly authorized to speak to the media, to analysts or in public gatherings on behalf of the county may speak/write in the name of the county to any newsgroup or chat room. Other employees may participate in newsgroups or chats in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves. Where an individual participant is identified as an employee or agent of this county, the employee must refrain from any unauthorized political, union or religious advocacy and must refrain from the unauthorized endorsement or appearance of endorsement of any commercial product or service.

12. 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.

13. Employees are reminded that chats and newsgroups are public forums where it is inappropriate to reveal any material covered by existing county confidentiality policies and procedures.

14. Use of county Internet access facilities to commit infractions such as misuse of county assets or resources, harassment which includes harassment, unauthorized public speaking and misappropriation

or theft of intellectual property are also prohibited by general county policy, and will be sanctioned under the relevant provisions of the personnel handbook.

15. Since a wide variety of materials may be deemed offensive by colleagues, suppliers and 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.

16. The county will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives and backups on individuals' Internet activities, which could include resurrecting "deleted" files and messages.

17. All employees with Internet access must take particular care to understand the copyright, trademark, libel, slander and public speech control laws so that their use of the Internet does not inadvertently violate any laws which might be enforceable against the county.

18. The content of any, or all, electronic communications are not confidential may be monitored to support operational, maintenance, auditing, security, and investigative activities.

B) Technical

1. User IDs 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. Policy prohibits the sharing of user IDs or passwords obtained for access to Internet sites. Management reserves the right to the passwords for all data stored on its computers. All passwords utilized on any county computer must be provided to the Information Systems Director or the Information Systems' designee. In addition, there will be no file(s), programs or data that cannot be accessed by appropriate management personnel.

2. Employees should schedule communications-intensive operations such as large file transfers, video downloads, mass emailing and the like for off-peak times.

3. Any file that is downloaded must be scanned for viruses before it is run or accessed.

4. Video and audio streaming and downloading technologies represent significant data traffic which can cause local network congestion. Video and audio downloading should be avoided.

C) Security

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.

:END