

GREEN COUNTY COMPUTER USAGE POLICIES

The Information Technology (IT) Department is governed by the Finance Committee. The IT Department, under direction from the Finance Committee, will develop and maintain the Computer Policies and Procedures.

All county employees who have Internet access will receive a copy of the Computer Usage Policies and the Internet/E-mail Usage Policy. Each employee shall certify that they have read and agree to comply with all policies.

The county reserves the right to modify and revise these policies at any time to reflect changes in technology or strategic direction or for any other reason deemed sufficient by the IT Department. All policy changes must be approved by the Finance Committee. Employees will be given the revisions as they occur. Employees shall implement any new policies immediately upon receipt.

Green County provides a variety of information technology resources such as computers, software, printers, scanners, electronic mail and Internet access for employees. IT resources owned and utilized by the county are provided, at considerable expense, to its employees to enable them to perform their job-related duties in an effective and efficient manner. It is the policy of the county that its IT resources be safeguarded from abuse, loss, and degradation of capacity due to inappropriate or inefficient use.

Employees are responsible for appropriate use of IT resources in accordance with county policies. In addition to complying with all laws and policies, employees are expected to adhere to the highest ethical standards when conducting business.

The county reserves the right to monitor any employee's use of county IT resources at any time for any reason including, but not limited to, monitoring sites employees visit on the Internet, monitoring and reviewing materials downloaded or uploaded by employees and reviewing e-mail sent or received. The IT Department may block any Internet sites that it feels are inappropriate.

Department heads, managers and supervisors are responsible for ensuring that business or personal use of IT resources is consistent with all department policies and work rules.

Violation of these policy requirements must be addressed immediately with the employee, and may result in loss of computer, network, or Internet privileges, disciplinary action, or dismissal.

PERSONAL USE

Except as prohibited by this or another more restrictive department policy, limited and reasonable use of IT resources for occasional and incidental employee personal use is permitted, subject to management approval, provided that this personal use does not:

- Interfere with the work of other personnel or the county's ability to perform its mission;
- Degrade the performance of the systems, such as gaming, music or video streaming;
- Result in any additional cost from loss of time or diversion of resources from their intended business purpose.

The use of IT resources for limited personal use is a privilege which may be revoked at any time by Green County management if use is deemed inappropriate. Individuals generating or receiving information on any county owned computer, network information system, the Internet, or on other systems linked to the county network shall not have an expectation of privacy over such information. Employees waive any right to privacy in anything that is created, stored, sent or received on the computer or the Internet, owned by the county.

Personal files such as pictures, music, documents, etc. may not be saved on county servers, laptops or pc hardware. Live streaming of radio or other media through the Internet is prohibited.

Personal use of the Internet during non-working hours from personal equipment is not restricted unless it conflicts with this or other Green County policies.

INAPPROPRIATE USE

Inappropriate use of IT resources, including limited personal use as authorized herein, may result in revocation of privileges, job related discipline, or both. Uses that are prohibited include, but are not limited to:

- Accessing resources or altering data without explicit management authorization
- Intentionally deleting or damaging data
- Intentionally introducing a computer virus
- Engaging in illegal activities as defined by state and federal law or local ordinance
- Wagering, betting, or selling chances
- Initiating or forwarding chain letters
- Transmitting threatening, abusive, obscene, lewd, profane, or harassing material
- Viewing, reading or accessing any sexually explicit sites or materials that are in any way sexually revealing, sexually suggestive, sexually demeaning, or pornographic, unless it is job related
- Engaging in commercial activities
- Soliciting, except in relation to Green County activities
- Promoting personal, political, religious or private causes, positions or activities, or working on behalf of organizations that have no professional or business affiliation with Green County
- Attempting to evade, disable, or bypass any security provisions of systems or the network
Obtaining unauthorized access to any county owned computer
- Allowing unauthorized individuals access to county Internet resources

DOWNLOADING SOFTWARE

Downloading software presents a significant risk of virus infection and license fee liability. Unless specifically authorized by the IT Department, employees shall not download software residing on the Internet or bulletin boards. This includes, but is not limited to games, screen savers, utilities, shareware programs, public domain programs, demo software, third party software, or employee purchased programs.

Only software that has been approved by the department head and purchased or leased by the county shall be considered for installation on county computers or servers. Installation must be coordinated with the IT Department. Updates to existing software may be downloaded and installed; any questions about software updates should be directed to the IT Department.

Any unauthorized copying, downloading or importing of software by employees using any method is strictly prohibited. If downloading is necessary, work orders must be submitted and downloading must be done by IT department staff following designated procedures for file transfer, virus checking and licensing.

WALLPAPER

Wallpapers and screen savers, downloaded from the Internet, which require a program to display may degrade system performance or conflict with other installed software, and therefore, are prohibited. Wallpapers which are inappropriate, as defined in the Inappropriate Use section above, are strictly prohibited.

COPYRIGHTED MATERIAL

Material on the Internet may be copyrighted. Duplicating or distributing copyrighted material without the express written consent of the owner is against the law and is prohibited. Employees should not assume that software is available for public use free of charge simply because there is no copyright or intellectual property notice on or in the software. U.S. copyright law and that of many other countries, no longer requires a copyright notice as a prerequisite to copyright protection.

SOCIAL MEDIA

Green County believes in the importance of open exchange and learning. Interactive or social media is a new and rapidly growing medium for collaboration, discussion and networking. We support the responsible use of this technology and offer the following guidelines:

- All county sponsored social network sites must be registered with the IT Department;
- The content of all county sponsored social network site communications is to be compliant with state and federal laws and consistent with the business objectives and existing policies of Green County;
- Social media sites may not be used as a means of exchanging information with or between county board or committee members where such exchange could be considered a “meeting” and a violation of Wisconsin open records laws;
- No information related to Green County may be posted that violates Health Information Privacy (HIPAA) laws, proprietary information, copyright, or other confidential or protected information, or in any other way violates state or federal law.

SECURITY OF SENSITIVE INFORMATION

All information that due to legislative mandate or other cause is defined as sensitive or confidential in nature must be kept secure. Confidential information includes any information protected by county, state, or federal privacy acts or administrative regulations, including HIPAA laws; and anything that in the opinion of the department head would be appropriately kept confidential in order to protect the interests of the county, its employees, or its clients, so long as such action by the department head does not conflict with relevant open meetings and records statutes.

Many employees have access to confidential information through the course of their job. Confidential information may only be used to perform job functions. Access to confidential information outside of the strict business needs of job function is prohibited. Reasonable measures must be taken to safeguard confidential information from unauthorized access.

The following guidelines have been established for all employees given access to IT resources:

- Employees may only access information explicitly authorized for their positions by management or for limited personal use as authorized by this policy or a stricter department policy;
- Employees are responsible for safeguarding their login IDs and passwords and are held accountable for any activity that occurs under their login ID;
- To protect the integrity of their ID, employees should log off their workstation if they will be away from it for an extended period of time;
- Any unauthorized activity must be immediately reported to management.

ANTI-VIRUS MEASURES

All computers will have virus protection installed. At no time shall an employee disable or delete anti-virus protection. Even though anti-virus software will detect many viruses, it will not detect them all.

If it is suspected that a computer has been infected by a virus, the user should not attempt to remove the virus, but immediately contact the IT Help Desk which will arrange for diagnosis and/or removal.

Computer viruses, defective programs, and corrupted data pose a threat to county IT resources, including the potential to involve the entire network in resulting damage. Any time an employee attaches or installs any non-county owned hardware or software, the potential exists for corruption of the network. Employees may not connect personal laptop computers, or any other personal peripheral devices that contain data that is non-work related to any county owned computer or to the county network without approval from the IT Department.

PASSWORDS

Passwords are there for a reason, to prevent unauthorized access to county computers and programs. Follow the password guidelines as required by all third-party applications. Use the following guidelines for strong password management:

- Passwords should not contain the employee's name or any other personal information that could easily be guessed by someone who is familiar with the employee;
- Passwords should be a minimum of 8 characters in length;
- Passwords should be a combination of upper and lower case, letters, symbols, and numbers;
- Do not re-use passwords.

The following are password guidelines for the I-Series (AS400):

- Minimum of 8 characters, maximum of 10
- Must have at least 1 number
- Passwords expire every 90 days
- Password cannot be the same as the last 7

HARDWARE & SOFTWARE

All hardware, including computers, printers, scanners and other peripherals that will be connected to the county network must be installed through the IT Department unless otherwise authorized by the manager of the IT Department. All Green County computers and new hardware technology will be ordered only after review and approval through the budget process.

The IT Department is responsible for routine maintenance, routine upgrades and technical support for any issues that arise from the use of these systems. No outside vendors shall be allowed access to the county network, or computers installed on the network unless authorized and scheduled in coordination with the IT Department.

Upon arrival, all hardware and software installations will be scheduled and performed by the IT Department unless otherwise authorized by the manager of the IT Department.

TECHNICAL SUPPORT

Green County maintains an on-line help desk for technical support. The help desk is the central clearing house for all technical issues. The help desk should be used for I Series programming issues, maintenance requests, software support, equipment requests, network issues, e-mail addresses, meeting requests, etc. A drop down box with pertinent subjects is provided on the help desk site.

The help desk function is responsible for logging all technical support calls from initiation to closure. End users should request a log in ID and password to access the help desk from the Data Center at 328-9468, or k2its@k2its.com. Users will be required to change their password after initial log in. End users will need to provide contact information, a brief description of the problem and the urgency (low, medium, high) of the current issue. Each request will be assigned a ticket number for follow-up and the user will be notified by e-mail that the request has been received and that a ticket number has been assigned.

For technical support during off hours (M-F 4:30 pm to 8:00 am, Sat, Sun, Holidays), for systems or departments that are supported 24 hours a day, or for critical system failures, special arrangements will be made to provide IT contact information for off hour coverage.

BACKUP AND RECOVERY PROCEDURES

It shall be the responsibility of all employees who use county computers, to save all business-related information from their computer to network servers, or other storage media, e.g. flash drive. Special directories shall be created for each user to store such information. Personal computers (workstations) will not be backed up automatically, thus any information stored on the employee's personal computer may be subject to data loss or destruction.

GREEN COUNTY
INTERNET / E-MAIL USAGE POLICY

Internet access to global electronic information resources is provided to employees for the benefit of Green County and its customers. Every employee has the responsibility to maintain and enhance the work of the county and to use the Internet in a productive manner.

To ensure that all employees are responsible, productive Internet users, these general guidelines have been established. Some departments may have more specific work rules for Internet or e-mail use.

While Internet usage is intended for job-related activities; incidental and occasional, brief personal use is permitted within reasonable limits. The Internet may be used to conduct official county business, or to gain technical or analytical advice. Databases may be accessed for information as needed. E-mail may be used for business contacts. Employees are responsible for the content of all text, audio, or images that they place or send over the Internet. Fraudulent, harassing, or obscene messages are prohibited. The Internet should not be used for personal gain or advancement of individual views or needs. Solicitation of non-county business for personal reasons is prohibited.

The equipment, services, and technology used to access the Internet remain at all times the property of Green County. Green County e-mail is secure; however, the county reserves the right to monitor Internet traffic and review, audit, intercept, access and disclose all messages created, received, or sent over the e-mail system, and any data stored in our computer systems. Any data that is composed, transmitted, or received via our computer communications system is considered part of the official records of Green County and as such, is subject to disclosure to law enforcement or other third parties.

The contents of any message may be disclosed by the county without the permission of the employee. However, e-mail messages are to be treated as confidential by other employees and accessed only by the intended recipient or his/her supervisor. Employees are not authorized to retrieve or read e-mails that are not sent to them without prior approval from a supervisor.

All messages communicated on the Internet should have your name attached. No messages should be transmitted under a false name. Users may not attempt to obscure the origin of any message. Information that is composed, transmitted, accessed or received via the Internet must not violate or infringe upon the rights of others.

Messages or information should not include content that violates Health Information Privacy (HIPAA) laws, or could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating or disruptive to any employee or other person. Examples of unacceptable content may include, but are not limited to, sexual comments or images, racial slurs, gender-specific comments or any other comments or images that could offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

Social media tools may be used to enhance communication, collaboration, and information exchange; streamline processes; and foster productivity. Employees may use social media sites, such as Facebook, Twitter, LinkedIn, etc. during work hours and using work computers for business reasons, with departmental approval. Some departments may have more specific usage work rules for social media. Limited personal use is allowed; employees must use sound judgment and common sense when accessing or participating in social media during work hours, and not abuse this privilege. While participating in social media, employees shall follow all existing policies which may apply that are not specific to social media. In addition:

- Employees must respect proprietary and confidential information. Such information cannot be disclosed;
- Any personal views or opinions expressed by employees related to Green County, its facilities, operations, policies, initiatives, activities, or past or present employees must be clearly identified as personal opinions and not those of the county;
- Any personal posting to a social network site that references the business of the county is prohibited;
- No information related to Green County may be posted that violates HIPAA laws, proprietary information, copyright, or other confidential or protected information, or in any other way violates state or federal law.

If an employee's supervisor believes that improper or excessive use of social media during work hours is resulting in performance issues or is creating a risk to the county, the supervisor shall inform the department head, and has the right to take disciplinary action. Abuse of Internet access or the e-mail system provided by Green County in violation of law or departmental policies will result in progressive disciplinary action, up to and including termination of employment. Employees may be held personally liable for any violations of this policy. If necessary, the county will advise appropriate legal officials of criminal violations in the operation of the computer system, Internet, and e-mail.

The following behaviors are examples of previously stated or additional actions and activities that are prohibited and can result in disciplinary action:

- Sending or posting discriminatory, harassing, or threatening messages or images;
- Using county time and/or resources for personal gain;
- Stealing, using or disclosing someone else's code or password without authorization;
- Sending or posting messages or material that could damage the organization's image or reputation;
- Sending or posting messages that violate HIPAA laws or violate confidentiality;
- Sending or posting messages that defame or slander other individuals;
- Using the Internet for political causes;
- Using the Internet for gambling;
- Engaging in any other illegal activities.

GREEN COUNTY
COMPUTER USAGE POLICIES
ACKNOWLEDGMENT FORM

I certify that I have received a copy of the Green County Computer Usage Policies, including the Internet/E-mail Usage Policy. I understand that it is my responsibility to read and comply with these policies as established by the Information Technology Department and approved by the Finance Committee.

I agree to abide by the rules and regulations as set forth in these policies.

Employee's Name (please print)

Department

Employee's Signature

Signature of Supervisor or Department Head

Date

Date

After you have read the policies and signed this page, please detach and return it to your immediate supervisor. The original will be sent to the Finance Office and a copy retained in your department. Thank you for your cooperation.

Supervisor, please complete this portion:

Authorized Access:

- Internet
- E-mail
- I-Series (AS400)

.....