CHAPTER:	**7 – CONDUCT AND PERFORMANCE**	**ADOPTED: 3/7/06**
SECTION:	**10 – INTERNET USE**	**REVISED: 6/10/15**

The purpose of an Acceptable Use Policy is not to impose restrictions that are contrary to Gloucester County's established culture of openness, trust, and integrity but rather to protect Gloucester County's employees, partners, and the government from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP are the property of Gloucester County. These systems are to be used for business purposes in serving the interests of the county, and for our residents in the course of normal operations. Effective security is a team effort involving the participation and support of Gloucester County employees and affiliates who deal with information and/or information systems. While this policy defines how county employees can and can not use county electronic resources, it can not cover every conceivable situation. Consequently, common sense and professional courtesy will still be required. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

This policy provides rules and guidelines for the proper use of the Internet, Intranet, Extranet, email, fax machines, and computers. It applies to employees, contractors, consultants, temporaries, and other workers at Gloucester County, including all personnel affiliated with third parties. It also applies to all electronic resources owned or leased by Gloucester County. The intent is to prevent wasteful use of the county's electronic resources, lost time, and inappropriate behavior. It also covers the actions required of staff to enable compliance with data protection regulations, avoidance of computer fraud, security breaches, or software piracy.

The County reserves the right, to monitor, examine, copy, change, and/or delete without notice all of its systems configurations, as well as the files on those systems for such purposes as: maintaining business continuity, responding to a complaint of computer abuse, such as harassment; or protecting County resources from unauthorized misuse.

The County neither guarantees against, nor shall it be responsible for, the destruction, corruption, or disclosure of personal material on or by its computer resources. Specifically, the County reserves the right to remove, replace, or reconfigure its computer resources without formal notice to employees (despite the fact that advance notice will normally be given).

If employees are maintaining personal files on County systems with appropriate permission, they are advised to locate such files in a root directory named "personal" to facilitate the identification and backup of those files.

General Use and Ownership

It is the intent of Gloucester County to provide high-quality computing facilities to its authorized users. This will allow the County Of Gloucester to: 1) maintain its access to available local, national, and international information, 2) provide an environment that encourages both the sharing of information and the acquisition of knowledge; and 3) provide our residents with rapid access to information.

Each computer owned by the County is a business tool and County property. As such, responsible employees are accountable for the condition of that tool and for abiding by the computing provisions set forth by the county.

Use of the County Network must be consistent with the goals of facilitating and disseminating knowledge; encouraging collaborative projects and resource sharing, aiding technology transfer, fostering innovation and competitiveness, and building broader infrastructure in support of each department's goals.

The County Network (local and wide are networks including phones, fax machines, switches, routers, hubs, and other connected equipment) may be used only for lawful purposes. Transmission, distribution, or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization.

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Gloucester County or the end user does not have an active license is strictly prohibited.

The county retains the copyright to any material created by employees in the course of their official duties. Copyrighted materials belonging to entities other than the county may not be transmitted by an employee on the county Internet or E-mail systems except with permission or as a single copy for reference only.

All county employees utilizing electronic resources will be provided a written copy of this policy. The policy will be included by Personnel as part of its new employee orientation process. It will also be posted on the Intranet so it is available and conspicuous to employees at all times.

Related questions should be directed first to your supervisor and then, if necessary, to the Human Resources Department. The Office of Information and Technology (IT) will be available on request to assist the Human Resources Department with technical questions.

Note: The terms Internet, Intranet (internal County Internet for employee use only), and Extranet (business-to-business Internet interface between the county and a business partner) are interchangeable. Any rule applying to one, likewise, applies to the other.

Data Security

Employees are responsible for ensuring business critical electronic data/information is backed-up and available only to authorized personnel.

Data stored on Network server drives are automatically backed-up by IT on a daily basis. Lost or damaged file may be restored by contacting IT. If you store information on your personal computer, you (not IT) have assumed data back-up and recovery responsibility.

When information needs to be shared, the use of shared directories/files is encouraged. At you request, IT will apply security rules allowing only those authorized by the directory/file owner to access the information. Read/write access privileges may be changed for the directory/file owner at any time. Remember - If your file is on a public directory or on a non-public directory with security rights not properly defined, access to your data can be compromised.

IT recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, contact IT.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, worms, e-mail bombs, or Trojan horse code.

All PCs, laptops and workstations must be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.

In addition to Windows/e-mail/ network passwords, it is recommended that user names, passwords, and/or user level security rules be built into home-grown applications or be an integral component of off-the-shelf packages.

Sharing user names/logon IDs and passwords (Network, Windows, application, etc.) without supervisor permission (emergency basis only) is forbidden.

User names and passwords should not be posted or displayed for easy access by unauthorized users. System level passwords should be changed quarterly; user level passwords should be changed every six months

Individual users can be held accountable for knowledgeable use of their account by others. This includes family and other household members when work is being done at home.

Network Security

Use of the Internet or electronic mail for the following purposes is strictly prohibited:

- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

- Circumventing user authentication or security of any host, network, or account.

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

- Engaging in activities commonly call “hacking” or “cracking”. Examples: Password sniffing (includes dictionary and brute force password cracking attacks). Data manipulation or vandalizing of web pages. Eavesdropping on Network traffic. Scanning for computer/Network vulnerabilities without authorization. Network sniffing. Pinged floods. Packet spoofing. Forged routing information for malicious purposes. Intentionally launching denial-of-service attacks on any computer system.

- Snooping in other individual’s email or using masquerading techniques. Example: Sending email from a mailbox other than the employee’s own, in order to disguise one’s identity.

- Engaging in anonymous activity to avoid being identified in Network security systems. Internet accounts shall be accessed only by the authorized owner (or his/her designee) of the account.

- Interfering with or disrupting Network users, services, or equipment.
- Examples: Introduction of malicious programs into the network or server (viruses, worms, Trojan horses, e-mail bombs, etc.). Downloading images, audio files, and/or video files unless they relate to an explicit business purpose.

- Connecting a network hardware device (workstations, printers, scanners, etc.) to the Network without the approval of IT. IT is responsible for monitoring, tracking, maintaining, and troubleshooting all network devices.

- Allowing a modem/router to be connected to or installed on a network computer. Modem use must be approved by IT and will be installed only on computers which have no physical connection to the Network. This is necessary for preventing potential third parties from compromising network security through a back door.

- Interrupting or disabling the automatic downloading of anti-virus software, software patches, or other IT approved administrative software.

- Disabling the automatic execution of IT approved software including, but not limited to, antivirus software.

Approved Software

The County Network has been loaded with an approved software configuration. The standard configuration was engineered to provide maximum reliability and security for County business. Modification of the configuration of the software is prohibited. The following rules apply to the use of County provided personal computers:

- To mitigate the risk of potential virus infection and improper use of copyright and licensing material, copying and downloading unauthorized software is prohibited.
- Software that is not part of the County standard suite of software may not be loaded onto a Government computer unless the software has been approved in advance in writing by IT.

- Approved software must be licensed by the original manufacturer prior to being installed.
- Only screen savers that come with the computer's operating system are permitted.
- Playing computer games, including those built into the WINDOWS operating system, is prohibited.

- Non-system wallpapers, e.g., family pictures, are permitted to be installed providing there are no copyright infringements.

- Hotmail and Instant Messaging software are prohibited.

- IT will delete non-approved software detected during routine software inventories and security scans by loading a new standard disc image onto the computer.

Operation Usage

Use of the Internet or electronic mail for the following purposes is strictly prohibited:

- Accessing Internet sites with sexually explicit or hate or other inappropriate material.
- Transmitting threatening, obscene, harassing, discriminatory, or sexually explicit materials.
- Accessing gambling sites.
- Sending or forwarding chain letters. These are e-mails which either ask you to forward them on to all your friends (or to everyone you know) or which state that something bad will happen if you do not forward them. E-mails of this type, which are usually warning about something (Example: computer viruses), are almost certainly hoaxes.
- Advertising, soliciting, or selling commercial items.
- Advertising, soliciting, or selling personal items.
- Conducting personal or commercial business for profit.
- Personal announcements without management approval.
- Engaging in non-County sanctioned fund raising.
- Engaging in political activities prohibited by law.
- Accessing "chat rooms" unless specifically approved in advance for each occasion by the employee's supervisor.
- Releasing proprietary data or information to unauthorized persons.
- Posting information to newsgroups without a disclaimer stating that the opinions expressed are strictly your own and not necessarily those of Gloucester County, unless posting is in the course of business duties.
- Auto-forwarding email messages to a commercial or other personal email account.
- Accessing stock ticker, PointCast, or similar real-time applications which include streaming audio, video, and on-line games.
- Participating in message boards about the County.
- Sending messages to large groups of people without prior management approval.
- Providing information about, or lists of, County employees to parties outside Gloucester County without management approval.
- Using e-mail resulting in inadvertent commitment of the county to a contract or agreement if it appears to the other party that you have authority to do so. E-mails sent to external stakeholders must include the following disclaimer:

  > "This transmission is confidential and may be legally privileged. If you are not the intended recipient, please notify the sender by return e-mail and delete this message from your system. The County of Gloucester reserves the right to monitor e-mail communication. No contract may be concluded on behalf of the County of Gloucester by e-mail. If the content

of this e-mail does not relate to the business of the County of Gloucester, then we do not endorse it and will accept no liability."

E-Mail Etiquette

Do not send offensive jokes, pictures, frivolous messages, or anything which may be construed as discriminatory in nature.

Since the confidentiality of e-mail mail can not be assured, do not type anything you don't want repeated. Do not try to carry out confidential or sensitive tasks or air controversial views on e-mail. Ask yourself: Would I want a member of the public or a jury to read this message? Remember that all e-mails (even deleted ones) are saved and usually can be retrieved even if they have been deleted.

Respect privacy and consider this aspect before forwarding messages.

Be polite. E-mails can often seem abrupt, even when this is not the intention. Use professional courtesy and discretion.

Do not reply with history if it is not necessary especially if it incorporates a large attachment. DO not send greeting cards and the like to large distribution lists.

Voluminous data files attached to e-mails increase network traffic congestion often resulting in overall response time degradation.

Use "reply all" and distribution lists with caution in order to keep the number of your messages to a minimum and reduce the risk of sending messages to the wrong people.

Check your e-mails regularly. Set the Out-of-Office flag and arrange for someone to deal with your e-mail if you are away for an extended period.

Messages should be clearly addressed "To" those from whom an action or response is expected. "cc" or "bcc" should be used for other recipients of the message. The use of "bcc" is not recommended since many consider this to come under the heading of "dirty pool".

Delete unwanted or unnecessary e-mail. It is the user's responsibility to manage their own e-mail folders and keep within quota limits.

Unsolicited e-mail, especially with an attachment, may contain a virus. If in doubt, delete the e-mail or contact the sender to check **before opening**.

Enter a meaningful "subject" field to help the reader anticipate the content correctly, and try to keep to one subject per message.

Don't use all or part of someone else's message without acknowledgement. Don't edit someone else's message without making it clear the changes that you have made and use good judgment when considering distributing other people's messages without permission.

Avoid subscribing to unnecessary mailing lists. Unsubscribe from mailing lists when they are no longer required.

Use discretion before selecting “request read receipt” or “request delivery receipt” options as this may unnecessarily increase network traffic thereby retarding overall response time. These options should be used by exception. They should not be system default selections.

Once a message is sent, there is no way to retrieve it. Check carefully that messages are addressed to the correct recipient(s) before sending.

Following an employee termination, the e-mail account will be closed by IT and an “out of office” message set for a period of up to 8 weeks after which time the account will be deleted. The employee’s management may request access to be given to the closed mailbox by another member of staff for this duration.

Personal Use

The use of the County network, computers, and equipment to connect to the Internet and to electronic mail shall be for official use and authorized purposes only. Authorized purposes may include brief Internet searches by employees for personal purposes, when they:

- Do not adversely affect the performance of official duties by the employee or the employee’s organization.
- Are of reasonable duration and frequency, and whenever possible, made during the employee’s personal time, such as, before or after duty hours or during lunch periods.
- Serve a legitimate public interest such as keeping County employees at their desks, educating the employees on the use of the Internet and the County Network, and enhancing the professional skills of County employees.
- Do not put the County Network to any uses that would not conflict with, or reflect adversely on, County interests.
- Do not overburden the County Network.
- Do not create significant additional cost to the County.

An employee may request, through his or her supervisor, additional access time or resources for justifiable personal purposes. These include major projects for college

studies already approved and being reimbursed by the County. However, the employee must get the supervisor's knowledge and approval in advance.

All Users:

Agree to comply with this policy by signing an Electronic Resources Acceptable Use Policy.

If you feel that your rights as a computer user are being violated, or if you are aware of other users who are misusing or abusing county electronic resources, report the problem to your supervisor immediately.

Supervisors:

Ensures critical electronic data/information is backed-up and available only to authorized personnel. Employers are generally liable for what their employees do in the course of their work. Consequently, due diligence must be exercised regarding the monitoring of employee activities. This process should be communicated and enforced at all levels of management. When supervisors become aware that their employees have violated one or more of the provisions of this policy, they must take appropriate administrative action which may include, but not limited to, verbal or written contacts, revoking Internet or electronic mail privileges, and possibly termination.

IT:

In addition to network and systems monitoring, periodically monitors individual electronic resource usage and reports violations to management.

Human Resources Director/Designee:

Ensures county electronic resource users comply with the policy contained herein in the use of County computing resources including protection of information, equipment and Network infrastructure components provided for the conduct of official business.