ELECTRONIC MAIL/INTERNET POLICY

INTRODUCTION

Whitfield County declares the following to be its policy to provide E-mail and Internet access to employees in an effort to give its employees a tool to communicate easily and efficiently. The sole exception to the above policy is that employees must be mindful that use of the electronic communications systems should be limited to County business. The sole exception to the above sentence being that employees may make incidental and occasional personal use as long as such use does not interfere with an employee's performance of his or her job responsibilities or the business use of such systems by other employees. The County has a right of access to all E-mail and all information on County-provided computers. No individual should have any expectation of privacy with messages sent or received, since confidentiality is not readily attainable when using E-mail for making harassing or threatening statements or expressing personal opinions on non-County related matters.

DEFINITIONS

1. *E-mail* means an electronic message transmitted between two or more computers or electronic terminals, whether or not the message is converted to hard copy format after receipt and whether or not the message is viewed upon transmission through a local, regional, or global computer network.
2. *Electronic Communications* means each of the County's communications systems, including, without limitation, E-mail, the Internet and any Intranet established by or on behalf of the County. This does exclude voice telephone communications, i.e. 911 telephone call talking/dispatching.
3. *Internet* means the global computer network accessed via modem, ISDN, DSL, cable modem or T-1 line, whether directly or through an Internet service provider.
4. *Public Record* means all documents, papers, letters, maps, books, tapes, photographs, computer based or generated information, or similar material prepared and maintained or received in the course of the operation of a County office or agency. Public record also means such items received or maintained by a private person or entity on behalf of a County office or agency which are not otherwise subject to protection from disclosure.

SCOPE

All E-mail communications and associated attachments transmitted or received over the Whitfield County network and/or any computer equipment owned by Whitfield County and all use of the electronic communications systems of the County are subject to the provisions of this policy. In addition and without limiting the generality of the foregoing, since Georgia law provides that E-mail communications written in the course of operation of a public office are generally considered to be public records, all E-mail communications written and sent in the conduct of public business by Whitfield County employees and/or representatives are subject to the provisions of this policy under the heading "Application of Public Records Statutes to E-Mail", regardless of whether the communication was sent or received on a public or privately owned personal computer.

E-MAIL IS COUNTY PROPERTY

The electronic communications systems hardware and software are County property, and all messages composed, sent or received on the electronic communications systems are and remain the property of the County. They are not the private property of any individual.
Use of the electronic communications systems is reserved solely for the conduct of County business. They may not be used for personal business or gain. Personal use is limited to incidental and occasional use that does not interfere with the employee's performance of his or her job responsibilities or the business use of e-mail by other employees.

No Expectation of Privacy in Messages; Lack of Confidentiality

The County reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic communications systems for any purpose. The contents of electronic communications may be disclosed within or outside the County without the consent of any individual.

The confidentiality of any message should not be assumed. Even when a message is erased by the user, it is still possible to retrieve and read that message. Furthermore, the use of passwords for security does not guarantee confidentiality. All passwords must be disclosed to the County upon request.

Prohibited Uses

The electronic communications systems may not be used to solicit, recruit for, conduct business for, or manage any commercial ventures, religious or political causes or outside organizations.

The electronic communications systems shall not be used to create, send or forward any chain E-mails, advertisements, solicitations or non-business related messages.

The electronic communications systems shall not be used to create, send or forward any offensive or disruptive messages. Among those messages which are considered offensive or disruptive are any messages which contain profanity, sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, gender, race, religious or political beliefs, national origin or disability.

The electronic communications systems shall not be used to search or "surf" for, visit or receive (download) any sites containing any written, pictorial, audio, or other depiction of information that might be considered offensive or disruptive as discussed above. Among the prohibited sites which cannot be visited using the electronic communications systems are sites containing sexually-related material or any other sites portraying information not reasonably calculated to be of use for the County.

For materials copyrighted by third parties, the electronic communications systems should not be used to receive (download) or transmit (upload) such copyrighted materials unless the third party owner/author has granted an express right for the County and/or the user to download and/or upload. In no event shall any individual attempt to receive or download any so-called "hacker" software or other software whose purpose is to aid the user in improperly accessing secure materials, circumventing security measures or copying or downloading copyrighted material, whether such material is on an internal or external network (i.e. accessing county servers, databases or etc.).

The electronic communications systems shall not be used to breach or attempt to breach any other network containing any protected information from a third party.

The electronic communications systems should not be used to transmit or discuss information that currently is or could be the subject of a lawsuit involving the County, including conclusions or opinions as to the existence, absence or enforceability of a grievance, claim or contract or the activities of any individual on behalf of the County. The above statement shall not be used to limit or restrict the use of 911 computer aided dispatch system or mobile data computers, which can be the subject of lawsuits.

The electronic communications systems shall not be used to establish web sites or home pages without prior approval of the County Administrator.

The electronic communications systems shall not be used to post any message to an Internet message board or chat room or other public electronic forum, without approval from the Department Head.

Misrepresenting, obscuring, suppressing or replacing a user's identity on any electronic communication, including but not limited to the practice of "spoofing" (i.e., constructing electronic communications so that it appears to be from another person) is prohibited. The user's name, electronic mail address, organizational affiliation, time and date of transmission, and related information included with any electronic message posting must always reflect the true originator, time, date, and place or origination of the posting or message.

APPLICATION OF PUBLIC RECORDS STATUTES TO E-MAIL

E-mail messages are subject to many of the same statutes and legal requirements and disclosure as other forms of communication, such as the Inspection of Public Records Statute (O.C.G.A. 50-18-70 through 50-18-76). This statute treats computer based or generated information in the same manner as paper documents. All such documents are generally considered to be public records and are subject to public inspection unless they are covered by a specific statutory exemption. E-mail messages, which are public records, must be retained in either paper or electronic format. An open request received via e-mail shall be

deemed legally received at the time of opening the message; therefore, the recipient shall document the date and time of receipt for compliance purposes. E-mail messages that are not public records should be deleted after viewing. If unsolicited e-mail is received from outside the county and cannot be unsubscribed, please let the IT Department know.

UNAUTHORIZED RECEPTION OR REVIEW

Although the County has the right to retrieve and read any message sent over the electronic communications systems, messages should be treated as confidential by individual users and accessed only by the intended recipient or his/her designee. Individual users of the County's electronic communications systems are not authorized to retrieve or read any messages that are not sent to them with the following exceptions:

1. If the individual user has obtained the written permission of another individual user to access and/or read that other user's messages and transmitted the same to the IT Department.

2. If an elected official, other than those serving on the Board of Commissioners, in the management of their specific operation, requires the review of the user messages within their authority, then authorization in writing to the County Administrator is required before access is provided.

3. If the County Administrator, in the management of the departments of the Board of Commissioners authorizes the retrieval or reading of the users messages within his authority.

Unauthorized use of another person's (or group's) password, or knowingly giving passwords to others not authorized to use such passwords is prohibited. Circumventing security measures or trying to gain unauthorized access to systems, resources, programs or data is prohibited. Any attempt to destroy the integrity of computer-based information is also prohibited. Falsifying your identity on the Internet, or any malicious attempt to harm or destroy resources or data is prohibited. This includes deliberately uploading, downloading, or creating computer viruses.

COMPLIANCE

Any individual who discovers a violation of this policy shall notify his or her supervisor.
Any individual who violates this policy shall be disciplined according to the rules and procedures of the Whitfield County Merit System of Personnel Administration, or the appropriate disciplinary system.

WHITFIELD COUNTY BOARD OF COMMISSIONERS
SYSTEM ADMINISTRATION POLICY

The purpose of this policy is to set forth the guidelines and policies of the County for administration of the software systems utilized by the County. The policy seeks to protect the integrity of the system as well as the employees of the County by providing internal controls. Strict adherence to the policy is essential to insure that these goals are met.

SOFTWARE MAINTENANCE

For purposes of this policy, software maintenance shall de defined as the loading, updating and maintenance of the software on the server. This would include initial setup, new releases, updates and any changes to the menus or parameters of the system. Software maintenance is the responsibility of the Information Technology Department and all maintenance should be coordinated through this department. Prior to any maintenance, all affected departments should receive documentation of the changes. All issues relating to the maintenance should be addressed to the IT Department. Due to licensing agreements and potential viruses, no employee should load **any** software onto any computer belonging to Whitfield County without consulting the IT Department. This includes downloads from the internet and e-mail as well as screensavers, wallpaper and personal browsers. All hardware and software purchases must be approved by the IT Department. The IT Department will support the word processing, spreadsheet, presentation and web browser applications that the IT Department provides.

SOFTWARE SECURITY

For purposes of this policy, software security shall be defined as the setup and maintenance of security codes and parameters allowing users access to the software. Each department head shall have responsibility for the employees in his/her department in determining the functions to which they shall have access. All requests for changes must be in writing and must be approved by the Office of the County Administrator. Approved changes will be forwarded to the IT Department who will have the primary responsibility for making changes. Copies of all changes should be forwarded to the IT Director who shall be responsible for maintaining an updates log of all security.

FUNCTIONAL MAINTENANCE

For the purposes of this policy, functional maintenance shall be defined as those items that relate to a module specific to one functional area of the County. Maintenance of system functions or system security is not included in this area. Examples of functional maintenance would be General Ledger Module used by the Finance Department or the Payroll Module used by the Human Resource Department. In these and similar instances, the department heads shall be responsible for maintenance of the parameters of these modules to comply with regulations. It shall also be the responsibility of the department head, with the assistance of the IT Department, to insure the integrity of the information provided by those modules. Addition of a new general ledger account number or changing a parameter for tax withholding would be examples of functional maintenance.

SYSTEM SECURITY AND BREECH OF SECURITY

The purpose of system security and passwords is to provide internal control, thus protecting the employee and the integrity of the County. Employees having access to software shall be assigned a unique user code and password that will allow him/her access to those areas relating to his/her job function. This user code identifies changes that are made and the user making those changes. Therefore, users should protect their passwords. The IT Department assigns usernames and passwords. An employee that leaves his/her workstation for an extended period should save all information, exit all programs and log off to protect county information. Employees should not be allowed to work under another employee's username. Computers should be shutdown at the end of the day, unless otherwise notified by the IT Department. Any breech or potential breech of security and misuse of usernames and passwords should be reported to the department head and the IT Director immediately.

**For assistance or questions e-mail the IT Dept at ithelpdesk@whitfieldcountyga.com or call at 281-4800