CA-ADM-201 **JUNE 2018**

GWINNETT COUNTY GOVERNMENT
UTILIZATION OF TECHNOLOGIES POLICY

Introduction

The purpose of this policy is to ensure an information technology infrastructure that promotes the basic missions of the County. In particular, this policy aims to promote the following goals:

- To ensure the integrity, reliability, availability, and performance of IT systems;
- To ensure that the use of IT systems is consistent with the principles and values that govern the use of County assets;
- To ensure that IT systems are used for their intended purposes; and
- To establish processes for addressing policy violations and sanctions for violations.

This policy document has been created to assist users in understanding the usage of Gwinnett County Information Technology (IT) systems and assets. Examples of IT assets include (but are not limited to) computers, fax machines, projectors, copiers, scanners, cameras, desk telephones, mobile phones and communication devices, voice mail systems, televisions, software or other applications, any data stored on county computers including laptops, fileservers, memory sticks, storage media or desktop computers.

I. IT Asset Usage – Business Code of Conduct

County IT systems, including access to the public network, are provided to support business objectives and are intended solely for business use.

Limited personal use is acceptable provided:

- this activity is undertaken during employee's personal time;
- it is minimal and occasional (it is recognized that occasional, de minimus use may
- be necessary if extenuating circumstances dictate);
- incurs no or de minimus network or system costs to the county; and
- it is not for personal financial reward outside of County remuneration.

Gwinnett County has the right to audit and monitor usage of all technology assets without seeking prior approval or informing users. This monitoring includes but is not limited to Internet usage; email usage; mobile phones and communication devices; system access and data files. **Users should have no expectation of privacy for any county issued / owned technologies.** All information stored in electronic format, including that which may be personal in nature, is subject to access and disclosure by the County.

The County reserves the right to access County computers, E-mail and other information storage to ensure compliance with provisions of this policy.

Users are responsible for maintaining the security of their own IT system's accounts and passwords. Accounts and passwords are assigned to single Users and are **not to be shared** with any other person without authorization from the user's department director / office head.

NOTE: Users are entirely responsible for any activity carried out under their IT systems accounts.

II. Efficient Use of Technologies

All County employees are expected to conduct themselves in a professional manner, and work as efficiently as possible during their time on the job. Use of County provided or personal devices (computers, laptops, smartphones, televisions etc…) that is not business related and/or that cause an employee to be unproductive, or utilize their work time in an inefficient manner is prohibited.

III. IT Asset Usage – Guidelines

Gwinnett County recognizes the growing importance of technology as a means to support its mission and therefore provides staff with access to technology, which includes a highspeed local area network, access to shared network software and storage space, computing equipment, support services, and access to the Internet. In return, users of the County's technology must be committed to complying with the County's policies and applicable law on appropriate use of these systems. All users of the County's technology are expected to observe the highest standards of responsibility and ethics. In general, this means that an individual's use of technology should not infringe on the rights of other users, utilize an unfair share of system resources, or interfere with the normal operation of the computer system.

Promote a Safe and Supportive Working Environment

- Users must not access, download, store or transmit any material or content that a reasonable person would consider inappropriate in a business/government environment, or that could be considered offensive or disrespectful to others. This includes, but is not limited to: threatening, abusive, libelous, defamatory, pornographic, racist, sexist or otherwise objectionable materials and language.

Legislative Compliance

- Users must respect and adhere to applicable local, state, and federal laws which govern the use of computing and communication facilities.
- Users must not knowingly download, upload, post, transmit or otherwise distribute or reproduce any information, software or other material protected by copyright, or other intellectual property right, without the express written permission of the copyright owner or right holder.

Prohibited Use of IT Assets

The following activities are prohibited uses of IT assets:

- Interference with the operation of any County computer system or network;
- Interference with the security of any County computer system or network;
- Unauthorized use of another user's account;
- Unauthorized attempts to alter data, files or systems;

- Making unauthorized changes to the configuration or working of equipment;
- Intentionally damaging software or hardware;
- Intentionally disrupting the County's network, website, or e-mail systems;
- Disguised use of County technology;
- Distributing or installing computer viruses;
- Assisting in a campaign for election of any person to any office or for the promotion of or opposition to any ballot proposition;
- Performing unauthorized mass email distributions;
- Utilizing email for non-business purposes
- Removing software or hardware from the County's computer systems without authorization; and
- Harassing or threatening use.

IV. Software Licensing and Installation

All users of the County's technology must cooperate with the Department of Information Technology Services (DoITS) in ensuring that the County obtains all software licenses utilized on County systems. Users should refer to County policies and guidelines associated with acquiring Information Technology software. Obtaining copies of software without appropriate licenses or using software in a manner beyond the rights granted in any license are violations of this policy.

Only software or programs purchased, developed or authorized by the County may be installed and used on County equipment. All installations must be done by technical support staff, unless otherwise approved by DoITS.

County computers are scanned regularly for unauthorized and/or malicious installed software. Unauthorized and/or malicious software will be removed from the computers and the abuse of this policy will be reported to management. Any unauthorized software currently in use and required for County business should be reported to DoITS so that its use may be approved or an acceptable replacement selected.

V. Protection Against Unauthorized Access

Each individual requiring access to the County's computer system must comply with the procedures administered by DoITS for obtaining a password and system access. Each individual is responsible for choosing and protecting an appropriate password for access to the computer systems.

All County computers are protected by an enterprise version of anti-virus software. Users must not attempt to disable this software, or it could create the potential for system compromise. Users must not attach any unapproved devices (such as an external disk, personal laptop, network switch or hub, printer, or video system) to county IT equipment or systems without the approval of DoITS.

VI. Separation of Duties

To the extent possible, activities will be executed by multiple individuals so that no single person has total control of a process. System Administrators should design processes and oversee security and user access to promote the separation of duties wherever and whenever possible.

VII. Portable Storage Devices

Portable storage devices such as USB Flash Drives have gained popularity due to their data storage capacity, simplicity of use and portability. The problem with these devices, however, is their proneness to theft and thereby vulnerability to data breaches.

No portable storage device should store any sensitive information without suitable physical and technical protective measures in place. Access control mechanisms should provide appropriate safeguards to preserve the confidentiality, integrity, and availability of the information asset.

There is risk of disclosure of sensitive information through careless disposal or reuse of equipment. Formal processes should be established to minimize this risk. The contents of removable media should be permanently destroyed or rendered unrecoverable in accordance with record retention requirements when no longer required. Storage devices containing sensitive information should be physically destroyed or securely overwritten to prevent the unauthorized disclosure of sensitive information.

VIII. Data Encryption

Users are encouraged to encrypt files, documents, and messages for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks.

IX. Internet Browsing

Employees may be granted Internet browsing capabilities at the request and approval of an employee's department director / office head. The browsing function of the Internet should be used only for necessary job functions (i.e. research). Personal use, defined as any use not directly related to the performance of job duties, of Internet browsing functions is permitted on an infrequent or incidental basis only. Each department director / office head shall be responsible for developing procedures to monitor and enforce this provision of the policy within his/her department/office. At no time is an employee allowed to browse sites containing any material prohibited by this policy.

All employees are subject to monitoring of their browsing activities. The County owns the computers, network and any other equipment used by employees to gain access to the Internet. Users should be aware that any electronic records transmitted via and/or maintained on or created by any of these systems are not private records. The County reserves the right

to monitor all electronic records at any time and without prior notice to users to assure compliance with state and federal law and this policy.

Improper use of Internet browsing shall result in loss of Internet privileges, departmental reprimand, and/or such other disciplinary actions as may be deemed necessary, up to and including termination of employment. Improper use is defined as browsing of information or material that promotes or transacts any of the following:

- Non-businesslike material;
- Discrimination on the basis of race, national origin, color, sex, religion, disability, age, or political affiliation;
- Unlawful harassment in violation of County policy;
- Copyright infringement;
- Excessive personal use (not related to job duties) as defined by employee's department director / office head;
- Personal, political, or religious business or beliefs; and
- Any unlawful activity.

Each user/employee shall maintain the confidentiality and security of his/her system password and shall not permit access to any network, computer, or electronic mail account by any person via his/her (employee) password unless such access has been approved in advance by employee's department director / office head. If a user's password is disclosed to any other person, for whatever reason, or if the security of an employee's account access is otherwise breached, the employee shall immediately notify his/her department director / office head, and immediately change their password. Each employee shall be held responsible for any activity occurring under his/her password or user identification code unless his/her department director / office head has been given prior written notification of a security breach.

X. Internet Browsing Exceptions

Occasionally it may be necessary for certain job classifications (namely certain employees of the Courts, Sheriff's Department, District Attorney's Office, and/or Police Department) to utilize the Internet in a manner that is otherwise prohibited by this Policy. In that event, the employee seeking to access material prohibited by this Policy as a direct performance of job duties must have a legitimate research need, and such access must be approved by his/her department director / office head prior to such access. DoITS will maintain a log of all access exception approvals, and the employee accessing such sites must log the following information for each site visited: date, time, site address, and reason for visiting site.

Any questions regarding this policy or Internet/Intranet activities should be directed to DoITS at (770) 822-8900.

XI. Social Network Site Access/Usage

Employees are strictly prohibited from using any County owned networks, equipment, or hardware to access social networking sites (e.g. MySpace, LinkedIn, Facebook, YouTube, Twitter, etc…) at any time. In the event a particular job classification or specific employee needs to access any of these sites for a qualified County purpose, such access must be approved by his/her department director / office head prior to such access being granted. DoITS will maintain a log of all access exception approvals.

All County employees are expected to conduct themselves in a professional manner, and work as efficiently as possible during their work hours. Use of the employee's personal devices (computers, laptops, smartphones, etc…) during approved breaks is permitted if such usage is not disruptive to the workplace, does not lead to inefficiency or wasted time and does not violate any other county policy, rule or regulation. Employees who violate this policy are subject to losing all access to social networking sites during the work day on a temporary or permanent basis and are subject to disciplinary action up to and including termination.

XII. Email Use Guidelines

Email provides essential communication regarding County operations. All employees and staff are required to use the official County email account that has been provided for County related correspondence.

Improper use of electronic mail may result in loss of mail privileges, departmental reprimand, and/or such other remedies as may be deemed necessary, up to and including termination of employment. Improper use is defined as transmission, receipt, or review of information or material that promotes or transacts any of the following:

- Soliciting or proselytizing for commercial ventures, job searches, chain letters,
- religious or personal causes or outside organizations or other similar, non-jobrelated solicitations;
- Discrimination on the basis of race, national origin, color, sex, religion, disability, age, or political affiliation;
- Unlawful harassment in violation of County policy;
- Copyright infringement;
- Expression of ill will or bias against individuals or groups;
- Offensive material such as sexually explicit material, obscenity, vulgarity, profanity, jokes, sarcasm, or other non-businesslike material;
- Excessive personal use (not related to job duties) as defined by employee's department director / office head;
- Creating inefficient use of employees work time; and
- Any unlawful activity.

All employees are subject to monitoring of their electronic mail activities. The County owns the computers, network, and any other equipment used by employees to gain access to the Internet.

Users should be aware that any electronic mail transmitted via and/or maintained on or created by any of these systems are not private records, and employees should have absolutely no expectation of privacy in any electronic record, file or activity. The County reserves the right to monitor all electronic mail at any time and without prior notice to users to assure compliance with state and federal law and this policy.

All employees, except for those in specific positions with approved exemptions, will have a footnote added to the end of each email advising recipients that emails sent to/from the County's email system are public information. The following verbiage will be added to each email "NOTE: Email is provided to employees for the administrative needs of the county. Email correspondence to/from a county email account is considered public information and subject to release under Georgia laws or pursuant to subpoena."

As with the browsing function, each employee shall be held responsible for any electronic mail activity occurring under his/her password or user identification code unless his/her department director / office head has been given prior notification of a security breach. If a user's password is disclosed to any other person for whatever reason, or if the security of an employee's account access is otherwise breached, the employee shall immediately notify his/her department director / office head and immediately change their password.

XIII. Use of Intranet/Internet/Email on non-County Devices

All County employees are expected to conduct themselves in a professional manner, and work as efficiently as possible during their time on the job. Use of personal devices (computers, laptops, smartphones, etc…) to access the intranet/internet/email that is not business related and/or that cause an employee to be unproductive, or utilize their work time in an inefficient manner is strictly prohibited.

XIV. Electronic Mail Retention

Electronic mail is subject, under the Open Records Act, to the same requirements as hardcopy correspondence. Therefore, electronic mail sent from and received by any County equipment is subject to production and may be scrutinized by the public as detailed in the Open Records Act. Furthermore, departmental records retention standards apply fully to electronic mail as they apply to hard-copy records. Electronic mail correspondence and records must be maintained in either electronic or hard-copy format for the duration of the records retention period required.

Each employee is responsible for ensuring proper retention of E-mail messages in accordance with the Open Records Act. DoITS does not retain a central repository of these messages.

Although backup of E-Mail by DoITS may be done for disaster recovery/continuity of operations reasons, this backup is not designed to comply with the Open Records Act.

Employees must set up their own retention procedures to ensure compliance with the open records act. While methods for reviewing, storing or deleting E-Mail vary, employees may comply with retention requirements of the public records law by doing one of the following:

- Print the E-Mail and store the hard copy in the relevant subject matter file as you would any other hard-copy community. Printing the E-Mail permits you to keep the information on a particular subject matter in one central location, enhancing its historical and archival value. The employee must also determine if the incoming Email must be printed before being deleted from his/her system;
- Electronically store public record E-Mail on your computer system and retain it electronically pursuant to retention schedules. Any questions regarding retention can be directed to the County Clerk.

XV. Use of Gwinnett County Public Wireless Access

Gwinnett County offers unsecure wireless Public Internet access at a number of facilities for use by citizens and constituents who visit a County facility to conduct business. Use of Gwinnett County's unsecure wireless public Internet by employees who have been provided access through the secured wired or wireless network is strictly prohibited, unless authorized by their department director / office head. This prohibition also extends to the use of personal devices (laptops, smartphones, etc…) on this network unless authorized.

XVI. Use of Wireless/Mobile Devices – Guidelines

The use of wireless and mobile technology by government employees has increased over the years as the technology has matured and proved itself as an effective communication tool. Its use has changed how we do business. Appropriate use of this technology allows employees to be more responsive to the citizens they serve. The following guidelines must be adhered to:

- Wireless/mobile devices issued by the County are intended for County business purposes only. Personal calls to or from a County mobile device are prohibited. Occasional, de minimus personal calls may be necessary if extenuating circumstances dictate. Personal use, beyond that of a de minimus nature, is prohibited and subject to disciplinary action up to and including termination of employment in accordance with the Gwinnett County Merit System Rules and Regulations, Section 420.000, Item 8 (Abuse of County property).
- A copy of wireless/mobile device charges will be available to each Director/Office Head for their review in identifying abuse. The Performance Analysis Division will conduct audits every year through the IRS approved statistical sampling method to ensure compliance with County policies as well as IRS and other governing mandates.
- Wireless/mobile devices may be provided to a County employee to improve customer service, enhance business efficiency, and provide safety and/or security while on required business travel. Cellular phones, cellular radios, and other types of wireless/mobile devices such as the Blackberry and other smartphones are not a personal benefit and shall not be a primary mode of communication unless they are the most reasonable and/or cost-effective means to conduct County business.

- The most appropriate wireless/mobile device and the most economical usage plan that meets the employee's business needs will be provided.
- County provided wireless/mobile devices may not be used to initiate charge based directory assistance such as 411 and (area code)-555-1212.
- County provided wireless/mobile devices may not be used to call fee based phone services, such as 1-"900" and "976" calls.
- County provided wireless/mobile devices should not be used when fixed services devices are readily available.
    - Example: using wireless/mobile phones at an office when a desktop phone is readily available.

XVII. Criteria For Determining Need for Wireless/Mobile Devices

As an overview, a department/office is authorized to provide wireless/mobile devices to its employees in accordance with the provisions of this policy. In the remainder of this section, proposed criteria for determining the need for such device(s) and guidelines for acquiring such device(s) are presented. If it is determined that a wireless or mobile device is a necessary component of a job function, then consideration should be given to such device(s) being maintained in a pool for shared use among employees unless this is not practical.

Agencies must establish and adopt written criteria to determine which job functions have a legitimate business need for wireless or mobile devices. Agencies shall utilize their criteria prior to assigning any such devices. Where communications needs cannot be met with fixed telephone or desktop computer equipment, a department/office must use their criteria for issuing these devices. Criteria under which these devices could be issued might include the following:

- Device is required to directly enhance an employee's job responsibility of protecting the physical safety of the general public;
- Device is required for an employee to better respond to environmental emergencies;
- Device is required for additional protection for the employee in potentially hazardous working conditions;
- An employee cannot adequately meet communications needs with fixed telecommunications equipment;
- Frequent travel (e.g.>25% of time) and required to stay in contact with the office or clients. (If travel duties rotate, departments/offices should use minimum number of devices to accommodate the maximum number simultaneously on the road.);
- Job requirements are to remain mobile within multiple building/sites where 2-way communications is required (e.g. transporters, delivery personnel, desktop support technicians);
- Public Safety/Homeland Security;
- On-call personnel who are on-call more than 2 weekends a month (Departments/Offices should explore possibility of shared phones if on call duties are shared);

- Critical staff doing business and expected to do business while commuting and moving from appointment to appointment;
- Regular requirement for two-way real-time communication where stationary phones cannot be made available (e.g. new construction area, campus-type environment, highway, etc.);
- Personnel who are required to be accessible at least 80% of the time and away from their office on a frequent basis (e.g.>25% of the time); and
- Positions meeting these criteria for wireless/mobile devices should be required to use a county provided device and service and not use a personal phone for reimbursement.

XVIII. Procedure For Acquiring Wireless/Mobile Devices and Services

Once the need for a wireless/mobile device has been identified, the department/office must take diligent steps to ensure that it will be paying the lowest amount for the device and recurring monthly charges. This should include projecting the quantity and type of access service (i.e. minutes, messages, coverage area, Internet, etc.) the wireless device is anticipated to use each month. DoITS will maintain a list of supported standardized equipment and services that are allowed under the existing contracts.

Departments/Offices shall consider the costs of acquiring, replacing, upgrading or moving wireless/mobile devices and/or reallocating equipment within offices to determine the longterm fiscal impact of such decisions.

- DoITS will serve as the central office for issuance and management of wireless/mobile equipment. DoITS will be responsible for activation of all newly-requested service; any changes in existing equipment, accessories, and/or rate plans; coordinating all repair problems with the service provider; maintaining a complete inventory of wireless/mobile equipment by department/office; and coordinating the acquisition or renewal of annual wireless/mobile equipment with the department of Financial Services, Purchasing Division.
- All requests for cellular, push-to-talk and other telecommunications devices/services must be approved by the user's department director / office head or their designated representative. Such requests must be submitted to DoITS via a shopping cart request including all account coding. A justification of need, approved by the appropriate party •
- The justification must indicate how the equipment will support the County's business, improve the employee's ability to do his/her job, and/or provide efficiency that does not currently exist. The service request must also include the appropriate financial accounting information for processing of payment.
- Once a request is received, the device/services will be processed through the current provider(s) of wireless/mobile device/services. The employee will receive a "Gwinnett County Wireless/Mobile Device Agreement" (see attached) and will sign said agreement indicating acceptance of the terms of the issuance of a County wireless/mobile device. Upon completion of the Agreement, the employee will be issued the wireless/mobile device by the DoITS.

- Each department/office shall be responsible for funding their wireless/mobile expenses. The DoITS will be the central administrator for processing payments of wireless/mobile monthly bills. Monthly charges will be entered into the financial system for each department/office according to supplied accounting information.
- Each department/office shall manage and monitor the use of communications equipment and services for the purpose of minimizing costs. Each department/office should consider the costs/benefits of assigning communications devices to employees who are frequently required to be on standby status.
- Each month, the DoITS will forward copies of wireless/mobile charges to the respective departments/offices for review. Any noted discrepancies in billing should be returned to the DoITS within fifteen (15) working days of receipt. Expenses for devices and services will be charged to each department/office's telephone service account.
- Each department/office should review their bills for accuracy of accounting information and to monitor employee usage.
- The user department/office is responsible for notifying the DoITS via a request in CRM to terminate the wireless/mobile plan when the user is no longer employed by the County and when there are other changes in assignment of wireless/mobile devices.
- User departments/offices must approve and submit requests to the DoITS via a request in CRM for any changes to an employee's issued equipment and/or rate plan.
- Employees responsible for wireless/mobile devices shall not lend their equipment to others except in the case of a public safety emergency.
- The employee must report the loss or theft of wireless/mobile devices within four (4) hours to the ITS Help Desk (770-822-8915) during business and non-business hours. If a device is lost, stolen or damaged, the employee may be held responsible for replacement, and may be subject to disciplinary action as outlined in the Merit System Rules and Regulations as determined on a case-by-case basis.

XIX. Communications Monitoring

County departments/offices shall expressly reserve the right to monitor and review all communications or other transmissions made to or from a county provided device without further notice to employees to the maximum extent permissible by law.

XX. Guidelines for Use of Personal Wireless/Mobile Devices

County employees may carry personal cellular phones or other types of wireless/mobile devices with them while on County time, but excessive use of personal cellular phones and other types of wireless/mobile devices for personal business during working hours is not allowed.

When authorized in writing by an employee's department director / office head or designee, the cost of using wireless/mobile devices for official business may be a reimbursable expense to the employee. Any reimbursement will be for reasonable cost in excess of the base plan plus any additional fees such as roaming fees or other fees and taxes incurred as a direct result of

the business use. In no instance will an employee be reimbursed more than the monthly cost to the employee.

All County employees are expected to conduct themselves in a professional manner, and work as efficiently as possible during their time on the job. Use of personal devices (computers, laptops, smartphones, etc…) that is not business related and/or that cause an employee to be unproductive, or utilize their work time in an inefficient manner is strictly prohibited.

XXI. Safe Use of Wireless/Mobile Devices

Gwinnett County mandates the safe use of wireless/mobile devices when operating any vehicle or piece of machinery. Drivers shall exercise due care in operating a motor vehicle and shall not engage in any activities which shall distract the driver from safe operation of their vehicle. Employees and operators who operate a motor vehicle while conducting County business are prohibited from:

- holding or supporting, with any part of the body, a wireless telecommunications device or stand-alone electronic device; or
- writing, sending, or reading any text-based communication, including a text message, instant message, e-mail, or internet data; or
- watching, recording, or broadcasting a video or movie; or
- engaging in any other action which distracts a driver while operating a motor vehicle as prohibited by state law.

Exceptions to this policy include: first responders (law enforcement, fire, EMS) during the performance of their official duties; reporting a traffic crash, medical emergency, fire, criminal activity, or hazardous road condition; an employee acting within the scope of their duties while responding to a utility emergency; and any other instance specifically exempted by state law.

This policy applies to employees who are driving a County-owned vehicle or operating their personal vehicle while on County business; are using a County-issued mobile phone/device; and/or are talking on a personal mobile phone/mobile device while conducting official County business. Gwinnett County Government adheres to all applicable state motor vehicle regulations relating to driver responsibility.

XXII. Questions

Users of the County's technology resources are encouraged to ask questions and seek information on the topics covered in this policy. In order to better be able to comply with this policy, questions about the appropriate use of computer and technology resources should be directed to the DoITS Help desk at 770-822-8915.

Questions regarding disciplinary actions and procedures should be directed to the appropriate office, or the Human Resources department at 770-822-7910.

XXIII. Definitions

Browsing - Using a web browsing application to "move" among the Web servers within the Internet, selecting information, viewing images or moving pictures and downloading applications.

Confidentiality – A security principle that works to ensure that information is not disclosed to unauthorized parties

Copyrighted – The legal right granted to an author, composer, developer, playwright, publisher, or distributor to exclusive publication, production, sale, or distribution of a literary, musical, dramatic, or artistic work.

De minimus - Something that is so little, small, minuscule, or tiny that the law does not refer to it and will not consider it. As pertaining to personal use of Gwinnett County wireless/mobile devices, use that is infrequent in nature, including emergencies or times when no other option is available. Personal use beyond that defined in this policy is prohibited and subject to disciplinary action up to and including termination of employment in accordance with the Gwinnett County Merit System Rules and Regulations, Section 420.00, Item 8 (Abuse of County Property).

HR – Department of Human Resources

Information – Any knowledge that can be communicated or documented material, regardless of its physical form or characteristic

Integrity – A security principle that makes sure that information and systems are not modified maliciously or accidentally

Portable Storage Device – Any device used to store data/information that can be carried from one place to another with relative ease.

Proselytizing - The act of attempting to convert people to another opinion and, particularly, another religion.

Remuneration – The total of the financial and nonfinancial benefits to the employee of all the elements in an employment package

Sensitive Information – Any information, the loss, misuse, or unauthorized access to or modification of which would adversely affect the interest or the conduct of programs, or the privacy to which individuals are entitled

Sensitivity – A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection

Social Networking - A community where an individual connects and communicates with others on the Internet.

User – A "user" is any person, whether authorized or not, who makes use of any IT system from any location

Wi-Fi - Any of several standards for short-range wireless data transmission

XXIV. Compliance

Any employee violating any provision of this policy may be subject to possible disciplinary action up to and including termination.

Each department/office may, based upon its individual business needs or legal requirements, exceed the requirements put forth in this policy but must, at a minimum, achieve the objectives defined in this document.

XXV. Interpretation

The County Administrator shall have final authority to interpret and apply this policy.