Harnett County
TECHNOLOGY USE POLICY

INFORMATION TECHNOLOGY DEPARTMENT
October 7, 2024

Adopted & Effective:

Harnett County

TECHNOLOGY USE POLICY

Table of Contents

Harnett County

TECHNOLOGY USE POLICY

PURPOSE, SCOPE & OWNERSHIP

This policy covers the use of all technology resources belonging to the Harnett County, hereafter referred to as County. It includes, but is not limited to all computer systems of any size and function and their attached peripherals, software, phones, all mobile communication devices, faxes, copiers, printers, camera systems, voice mail systems, e-mail systems, network resources, user accounts, electronic door locks, time clocks, ID badges, radios, data in any format and any network accessed by these systems including the Internet. Systems containing County data, which are hosted by third parties outside of the County's network, and the personnel with access to those systems, are also subject to this policy.

All technology resources owned, rented, or leased by the County are in place to enable the County to provide its services in a timely and efficient manner. This is the primary function of these resources and any activity or action that interferes with this purpose is prohibited. It is critical that these systems and machines be protected from misuse and unauthorized access. All technology resources defined in this section, along with all information transmitted by, received from, and stored upon said systems are considered to be possessed by, and/or the property of the County. Additionally, all documents, messages and attachments composed, sent, received or stored on County Technology Systems are County property. County standards will be established for all technology (hardware and software). Any deviation from these standards may require approval of the department head, Chief Information Officer (CIO), Finance Director, HR Director, and/or the County Manager.

Because technology systems are constantly evolving, the County requires its employees to use a common sense approach to the rules set forth below, complying with not only the letter, but also the intent of this policy.

In addition to this policy, users are subject to applicable state and federal laws. Improper use or misuse of County Technology Systems on a person's work time or otherwise is a violation of the County's personnel policies. User violation could result in disciplinary action including suspension, demotion or dismissal. If a policy violation occurs, aside from disciplinary actions specified under the County's policy, system access may be revoked in whole or in part if deemed to be in the best interest of the County's Technology System security.

This policy is not intended to supersede any existing laws or policies regarding records that are confidential, including, but not limited to, juvenile records in the Sheriff's Department, certain information contained in personnel files, or medical files.

This policy is intended for internal use by County employees defined as full-time, part-time, temporary and interns, all County Boards and Commissions that may have access to County equipment or resources, and non-County employees covered under this policy, defined as contractors, vendors, and volunteers who use County owned, rented, or leased resources.

DEFINITIONS

Anti-virus/Anti-malware software – Computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software.

Applications – Computer software such as word processors, which perform productive tasks for users.

Authorized Systems – A computer network that allows entry with proper credentials.

Backup Schedule – Plan for duplicating County data and programs.

Backup Storage Area – Location where County data and programs reside, typically on a tape, disk or hard drive.

Blogging – Web log on a website where entries are written in chronological order and commonly displayed in reverse chronological order.

Chain Letter – Message that induces the recipient to forward copies of a document to other users. They may contain viruses, false information or threats.

Chatroom – A form of digital conferencing that can be real time online conversations.

Communications Equipment – Device that is physically attached to the County network and enables transmission of data.

Computer Access – Ability to utilize the computer and gain admission into the County's network.

Computer virus – A computer program that can copy itself and infect a computer without permission or knowledge of the user.

E-Mail – Electronic Mail: Messages, usually text, sent from one person to another via computer.

Group Policy – A feature of Microsoft Windows operating systems that provides centralized management and configuration of computers and remote users.

Hardware – The physical components of a computer system (monitor, CPU, keyboard).

Instant Messenger – Also known as IM, a program that facilitates live chat.

Internet – Vast collection of inter-connected networks that all use the TCP/IP protocols.

Malware- malicious software designed to damage or gain unauthorized access to a computer system.

Mobile Devices – Computing appliance that is typically handheld.

MultiFactor Authentication (MFA)- additional layer of security that authenticates your identity along with your account password. Usually authenticated by a pin sent via text, email or authenticator app.

Network – The connection of two or more computers together so that they can share resources.

Online Games – Reference to video games that are played over some form of computer network, most commonly the Internet.

Peripheral Devices – Any equipment such as printers, copiers, faxes, scanners that attaches to the network.

Public Network – Ability to access the Internet without restrictions.

Remote Access – Access to County systems from external systems, e.g. via the Internet.

Server – Computer or a software package that provides a specific kind of service to client software running on other computers.

Social Media – Commonly used websites, such as, Facebook, Twitter, , YouTube, Flickr, Blogger, Google+, Instagram, Snapchat and LinkedIn.

Software – Collection of computer programs, procedures and documentations that perform some task on a computer system.

TCP/IP – Transmission Control Protocol/Internet Protocol: A suite of protocols that defines the Internet. The method used to transmit and receive data over the Internet.

County Websites – County's collection of web pages hosted by a server.

Workstations – Microcomputer designed for technical applications.

User – Any individual who interacts with the computer at an application level.

VPN – Virtual Private Network: is a network that is constructed by using public connections, usually the Internet, to connect to a private network such as the County's internal network.

SECURITY

Security refers to the protection of all technology resources from any kind of damage and the protection of data from unauthorized access, distribution, modification or destruction. The following procedures must be followed to ensure a secure environment.

- A user will be authorized access to the County's computer systems by the appropriate user department head or designee. A request for services must be submitted by the department head or their designee to the Information Technology Department, hereafter referred as the IT Department. The CIO or their designee will establish credentials for the authorized systems, which may include but not limited to software applications, e-mail, Internet, peripheral devices, building access and time clock access. This request should be sent directly to the IT Department from the department head or designee.

- Request for services, as well as, any other document containing IT security access information, including but not limited to, usernames, passwords, security questions and answers, and user access rights shall not be considered public record and shall not be released to any person, firm, or entity without direct written permission from the CIO and County Manager.

- All County users must read and sign a copy of this policy and return it to their department heads. Department heads and Human Resources will keep a file of signed copies in the employee's personnel file.

- When an employee is suspended or terminated, a written notification will be submitted from the department head or his/her designee to the IT Department immediately. Access to all systems will be suspended immediately.

- Non-County employees, as previously defined, will be the responsibility of the department head, who will notify the IT Department when it is necessary to determine accessibility and establish system credentials.

- IT Department will ensure security of unattended workstations by utilizing a group policy to lock computer screens after twenty (20) minutes or less of inactivity. Department heads may request a modification of this procedure through written request to the IT Department. Requests will be considered based on location and access levels of the computer or user. Users must logoff all computer systems at the end of each work day.

- For security, network, and computer systems maintenance purposes, authorized individuals may monitor equipment, systems, data and network traffic at any time.

- Any hardware or peripherals not belonging to the County will not be permitted to attach to the County's internal network without written authorization from the department head and final approval from the CIO. Personal hardware includes, but is not limited to, computers, cell phones, mobile devices, cameras, iPods, MP3 players, flash drives and portable hard drives. If it is determined that a non-County owned computer or device must attach to the network, a checklist of required software will be provided by IT to the department head. Computer owners are responsible for installing all required software. County IT staff will be available for consultation and will validate all required software before non-County owned equipment can participate on the County's network. Unauthorized devices connecting to the County's internal network can create an enormous security risk leaving the County's network exposed to numerous threats and immeasurable damage. A public/guest network will be provided at all County buildings. Personal devices may connect to public/guest networks upon accepting the Terms of Use.

- For remote assistance help desk purposes, authorized individuals may connect through remote access software to equipment, systems, data and network traffic at any time.

- The County has the right to monitor, audit, and/or inspect any and all aspects of the County Technology Systems at any time, without advance notice to any users, and without the permission of any user. Failure to monitor in any specific situation does not constitute a waiver of the County's right to monitor. Users within the scope of this policy are advised that they have no privacy rights and no user of County Technology Systems has any expectation of privacy in any message, file, image, or data sent, retrieved, or received when using County Technology Systems. Employees must understand that all technology resources are County property.

- The County does not guarantee the confidentiality of user information stored on any network, computer, or communications device belonging to the County. Users should be aware that the data they create on County technology or communications systems remains the property of the County and is not private (unless the data is protected by privacy or confidentiality laws). Information that is stored on or transmitted to or from County Technology Systems may be subject to disclosure pursuant to the North Carolina Public Records Law. Users should refrain from, where possible, storing personal files and data on County Systems.

- Users are responsible for safeguarding their own credentials and computer access and SHALL NOT let another person use their credentials or access. Users are **directly** accountable for all activity connected to their user ID.

- Passwords may be required to be changed every ninety (90) days and SHALL NOT be divulged to any other person. Passwords should be memorized and not written down

unless kept in a secure place. The CIO shall determine when access will require routine password changes.

- Multi-Factor Authentication (MFA) may be required to utilize any County user account or technology. Users may use their personal or county issued devices to set up an approved authenticator app or a personal or county cell phone number to authenticate. If the user does not wish to use one of these methods, they will be issued a County Security device token. It is imperative that the user keep the device secured at all times.

- Security device tokens will be issued to County users to provide access with multi-factor authentication. Routine wear and tear or theft of the token does not incur a charge for replacement, however loss of the token carries a $40 replacement fee.

- The County has no control or access to any Authenticator apps used for MFA by the users on their personal device. All authentication is solely handled by the app provider.

- Passwords must be changed at any time a user believes their password has been compromised. Any credentials such as ID badges, proximity cards or security tokens that become lost, stolen or misplaced must be reported to the department head and IT Department immediately.

- Users SHALL NOT abuse or misuse the County's technology resources or violate any rules in other portions of the County Personnel Policy, local, state, or federal laws via the County's technology resources.

- Users SHALL NOT copy or attempt to copy any software or data from County Systems without having written authorization.

- Users SHALL NOT attempt to bypass any security mechanisms.

- No third party may be allowed access to County Systems without prior authorization and approval from the CIO.

- Users SHALL NOT engage in abuse or misuse of the County's technology resources.

- Users SHALL NOT install any computer software on any County owned computers or devices, not authorized by the County, regardless of the ownership of the software except as allowed in other sections of this policy. Users may not install software personally owned or downloaded for free from the Internet. This includes but is not limited to, music software, photo software, Internet search software, screen savers and desktop backgrounds. Many of these software applications may contain viruses and/or malware that may compromise the integrity and security of the County's network.

- Administrative rights are granted to IT staff and those departments required by state regulations to have local administrative rights. Department heads must approve software requests and submit to the IT Department. Any software that adversely affects the performance of the machine or network will not be permitted on the County system.

- Separation of duties will be practiced in all departments, to the greatest extent possible, such that no individual has total control of a process.

- Users shall disclose to their department head, who shall then notify IT of any suspected or confirmed unauthorized use or misuse of technology resources and any potential security breaches or loopholes.

- The IT Department, where possible, will work to ensure that all network infrastructures, including but not limited to communications equipment, servers, data cables and telephone cables are secured behind locked doors with limited access by authorized personnel.

- Remote access to County systems consumes technology resources above and beyond those required for local access. Remote access shall be granted on a case-by-case basis based upon the unique needs of the user and available resources. Remote access users are subject to all policies herein.

ACCEPTABLE USE

At all times when an employee is using County technology resources, he or she is representing the County. While in the performance of work-related functions, while on the job, or while using publicly owned or publicly provided technology resources, County employees shall use them responsibly and professionally, and remember that public perception is extremely important. They shall not use these resources in an illegal, malicious, or obscene manner.

When using County resources, employees shall abide by all County policies including the County's policy on sexual harassment.

County Technology Systems are intended for business use. However, employees may make reasonable, incidental or occasional, personal use of the County's computers and data communications. Any personal use must adhere to the following:

- Must not incur any additional cost to the County. If, in a critical situation, an employee must use County resources that incur costs, the employee will reimburse the County within 30 days of the occurrence.
- Must not incur security risks to the County or the County's network.
- Must not violate the County Personnel Policy.
- Must not have a negative impact on employee performance, including interfering with work duties, work performance or work productivity.
- Must not have a negative impact on system performance.
- Must not violate this Policy or any applicable laws or regulations.
- Must not violate contractual agreements or intellectual property rights.
- Must not be used for personal gain.
- Must not be used for solicitation.

Users are required:

- To respect the privacy of other users; for example, users shall not intentionally seek information on, obtain copies of, or modify files, data, or passwords belonging to other users, unless explicit permission to do so has been obtained. It shall be understood that this rule does not apply to supervisory personnel, who shall have complete authority to access any files created by users in their departments.

- To protect data from unauthorized use or disclosure as required by state and federal laws and agency regulations. (i.e., confidential information)

- To respect the integrity of computing systems; for example, users shall not use or develop programs that harass other users, or infiltrate a computer or computing system and/or damage or alter the software components of a computer or computing system, or otherwise interfere with data, hardware, or system operation.

- To respect the legal protection provided to programs and data by copyright and license. The County owns licenses to a number of proprietary programs, which allow the County to use the software but severely restricts anything other than the use of the software on a single computer or network. Any redistribution of software from the computing systems breaches agreements with our software suppliers, as well as applicable federal copyright, patent and trade secret laws. U.S. Copyright Law provides for civil damages of $50,000 or more and criminal penalties including fines and imprisonment in cases involving the illegal reproduction of software. Therefore, no copying, downloading, or distributing of any copyrighted materials, including but not limited to messages, e-mail, text files, program files, image files, database files, sound files, and music files is allowed without prior authorization by IT.

UNACCEPTABLE USE

Unacceptable uses are defined as those uses that do not conform to the purpose, goals, and mission of the County and to each user's authorized job duties and responsibilities as determined by the County Manager or his/her designee.

Examples of unacceptable activities include, but are not limited to:

- Private or personal, for-profit activities or for any illegal purpose, including but not limited to communications that violate any laws or regulations.

- The use of the County network or any device owned, leased, maintained or otherwise controlled by the County to access, transmit, store, display, or request obscene, pornographic, erotic, profane, racist, sexist, libelous, or otherwise offensive or abusive material (including messages, images, video, or sound). The County may install monitoring software or use filters to monitor or block access to any sites that would or

possibly could violate this policy. Any user who attempts to avoid such software or filter or uses a device owned, leased, maintained, or otherwise controlled by the County to access, transmit, store, display, or request such material is in strict violation of this policy and may face disciplinary action, up to and including dismissal in accordance with the Harnett County Personnel Ordinance. For the purposes of this section, "pornography" and "pornographic material" is any material depicting sexual activity as defined in N.C. General Statute § 14-190.13.

  - Any employee who becomes aware of any individual that uses the County network or uses a device owned, leased, maintained, or otherwise controlled by the County to access pornography shall report the violation to the County's Chief Information Officer.
  - Annually, no later than August 1, and in the format required by the State Chief Information Office, the County's Chief Information Officer shall report information to the State Chief Information Officer on the number of incidences of unauthorized viewing or attempting viewing of pornography on the County's network or on any device owned, leased, maintained, or otherwise controlled by the County whether or not the unauthorized viewing was by an employee, elected official, or appointee of the County.
  - This section shall not apply to an official or employee that is engaged in any of the activities permitted by N.C. General Statute 143-805(d) in the course of that official's or employee's official duties.

- Intentionally seeking information about, obtaining copies of, or modifying of files, other data, or passwords belonging to other users, unless explicit permission to do so has been obtained.

- Interfering with or disrupting users, services, or equipment. Such disruptions would include, but are not limited to (1) distribution of unsolicited advertising or messages, (2) propagation of computer worms or viruses, and (3) attempting to gain unauthorized entry to another computer or computer system whether owned by the County or outside of the County.

- Removing or relocating any computer equipment (hardware, software, data, etc.) without supervisor's prior authorization and IT notification.

- Allowing unauthorized users, including an employee's family or friends, to use the County's technology resources.

VIRUS & MALWARE PROTECTION

Every computer user is to remain vigilant and alert to the possible transmittal and infection of a computer virus. Most e-mail viruses are transmitted through attachments or embedded links. Never click on a link or open attachments that contain the following extensions: .exe, .vbs, .com, .bmt, .hta, .shs, .vbe, .cmd. Upon detecting any virus, or suspected virus, users are to cease activity immediately and report it to the IT Department. Refer to Security section of this policy for software and hardware installation requirements, procedures, and policies.

Appropriate anti-virus and anti-malware software will be made available by IT and loaded on every workstation and laptop computer.

INTERNET USE

A County Internet and network access, whether connected by cable, Wi-Fi, wireless air card, or any other means, is a resource granted to employees upon department head approval. All employees are encouraged to use the Internet to its fullest potential, providing effective services of the highest quality, discovering innovative and creative ways to use resources and improve services, and encouraging staff development. The Internet should be a primary method for the exchange of ideas and information.

The Internet provides easy access to software distributed by companies on a trial basis. The free access does not necessarily indicate the software is free or that it may be distributed freely. Users are expected to comply with the copyright policy as previously stated. Users should never use or download software from file sharing websites or services (commonly known as “P2P”). Refer to Security section of this policy on downloading and installing software.

Blogging, Instant Messaging, online games, online movie/video streaming, online audio streaming, and chat room participation are not permitted unless demonstrable benefits to productivity are proven. These types of activities place extra strain on network resources and can affect network performance for the entire site. In all cases, prior approval of the department head and the IT Department must be obtained.

A public/guest network will be provided for outside vendors, contractors, and users who need to access the Internet for the purpose of demonstrations and presentations to County Staff. County Staff may use public/guest network for personal computers and devices upon user acceptance of Terms and Use.

COUNTY WEBSITES

In order to maintain a consistent, useful and professional presence on the Internet, IT has established procedures that will assist departments in creating, publishing and maintaining

content for the official County website or any sub-website created by any County Department, Board, Commission or entity directly affiliated with the County or which is funded by County funds.

Each Department and its employees have a responsibility to make sure that all public information disseminated via the County website is accurate, current as possible, and in accordance with this policy. Employees shall provide, in association with such information, its source and the date it was published. An electronic mail address or other contact information allowing the recipient to contact public staff must be published.

Only authorized employees shall be allowed to update the website. Authorized employees are **directly** accountable for all activity connected to their user ID. Departments who have a need to create or contract for its own physical website must have approval from the County Manager and the IT Department. Links to personal websites are not allowed. Information on events will be limited to those directly sponsored by or affiliated with the County.

ELECTRONIC MAIL

Electronic mail is intended for County business; however, the County recognizes the fact that the use of e-mail for incidental purposes may occur and is not likely to strain County resources. Personal communications should not be excessive and it must be understood that the use of email passwords does not imply privacy or confidentiality. E-mail messages, made or received in connection with the transaction of public business by any agency of North Carolina government or its subdivisions are considered a public record and the property of the County. The County Manager and supervisory personnel have the right to review the contents of all employees' e-mails (personal or business related). Employees are solely responsible for how their email is used and managed.

Contents of email dictate the retention of email and each email user is responsible for the retention of their own email. Email must be retained according to the procedures defined in the "*Email as a Public Record in North Carolina: Guidelines For Its Retention and Disposition*" publication, submitted by the NC Department of Cultural Resources or other regulatory agencies as applicable.

Personal email addresses being used for County business purposes, including but not limited to employees, County Commissioners, boards and commissions, should follow the same retention guidelines as County email addresses. This policy does not attempt to monitor or manage personal computer accounts or equipment. Where at all possible, official County email addresses should be used to conduct County business.

PII or Personally Identifiable Information is any information that relates to a person's identity which includes SSN, birthdate, employer taxpayer identification number, driver's license number, passport number, state ID number, checking/saving account number, credit/debit card number, PIN code, electronic ID number, internet account number, biometric data, fingerprints, digital signatures, passwords, and any other numbers or information that can be used to access a person's financial resources. This information must be protected from any sort of data loss or disclosure. Please note that any communication of this type of information must be sent through secure communications only. Email is not a secure means of communication and should not be used to share sensitive data. If an employee needs to send out any PII, the employee shall use a secure method of communication which includes fax, encrypted email, or secure file sharing. If an employee has authorization to access sensitive information, it is =the employee's responsibility to make sure that it is handled securely and not disclosed to any unauthorized personnel. Great care should be used when transmitting or accessing PII.

Unacceptable uses of e-mail include, but are not limited to:

- Using email software that is not the County adopted standard.
- Sending or forwarding chain letters.
- Sending or forwarding copies of documents in violation of copyright laws.
- Compromising the integrity of the County and its business in any way.

- Sending or forwarding messages containing derogatory, racial, offensive, abusive, threatening, obscene, harassing, or other language inappropriate for the organization.
- Sending or forwarding messages that violate the County's sexual harassment policy.
- Willful propagation of computer viruses.
- Overtaxing the network with unnecessary group mailings or large emails (over 20 MB). Users should utilize SendThisFile, Microsoft 365,or other means of sending large files to recipients.
- Sending or forwarding confidential information including, but not limited to personally identifiable information, juvenile records in the Sheriff's Department, certain information contained in personnel files or medical files. This includes confidential information as defined by state and federal laws and agency regulations.

TELEPHONES & MOBILE DEVICES

The County may provide telephones and mobile devices to employees for business use, when the budget allows and determined necessary by the department head. A mobile device shall be used for appropriate business purposes. Such use is defined to be appropriate when an employee must utilize the device to further County operations. The County may review call logs, voicemail recordings, text messages, email transcripts, GPS data or any other data contained on or from County owned devices.

All devices and accessories provided by the County are property of the County and must be returned upon request. The department head, the Finance Department and the IT Department, shall monitor mobile device use and charges. Any intentional, deliberate misuse of any device may result in the loss of mobile device service and employee reimbursement of charges and could result in disciplinary action.

It is the responsibility of the department head, or his/her designee, to review the detailed bills for the department each month. The department head/designee should note usage patterns for both individuals and the department and investigate any unusual or questionable patterns. It is also the department head's responsibility to ensure that any required reimbursement to the County is done on a timely basis and in accordance with the requirements set forth herein.

Laptops, cell phones, and other electronic devices in vehicles must be stored in a secure location or otherwise out of sight. Devices should never be left in vehicles overnight. To the degree possible, technology resources should be protected from theft and/or vandalism, fire or other damage including natural environmental hazards. Devices damaged or stolen must be reported to department head and CIO immediately.

Landline Phones

The use of telephones is a necessary part of the day-to-day operation for many County employees. Unfortunately, inappropriate telephone use may also be a source of distraction that cause lower productivity and, in some instances, may present a safety hazard. Personal calls may be allowed on County landline phones, however, employees are expected to be good stewards of County resources and time, and therefore, personal calls should be limited and not affect job performance or duties. If personal misuse is determined, employee may be restricted to only business use or other disciplinary actions may occur.

The County may monitor and/or record phone calls made or received using the County phone systems and may access and review call logs and voicemail recordings to ensure compliance with this and other County policies. Users have no expectation of privacy when using County owned phone systems.

Cellular Phones & Smartphones

The County may provide employees with mobile phones, smartphones, or wireless Internet devices. These devices must be used primarily for business use. Personal calls and use may be allowed on County devices, however, employees are expected to be good stewards of available data. If personal misuse is determined, employee may be restricted to only business use or privileges may be revoked.

All Smartphone devices shall use passwords and must adhere to the same password standards as previously defined. It is the user's responsibility to ensure devices are property secured. All smartphone devices shall contain County management software/profile. Removal or attempt to bypass this software/profile will be in strict violation of this policy.

The County reserves the right to inspect all files stored on smartphones that are the property of the County to ensure compliance with this policy. Users should not presume to have any expectation of privacy in any matter created, received, stored in, or sent from any County issued smartphone.

Issued smartphones and all County purchased accessories must be returned to the IT Department when the user's service has ended. When the smartphone is returned, the County will conduct any appropriate backup of files in accordance with the Public Records and Retention laws. The smartphone will then be wiped clean of all information.

iPads and Tablets

The County has recognized that mobile devices, including iPads and tablets, may provide a benefit in the efficient performance of County duties and thereby improve service to the public. County issued devices will be managed under a Harnett County email. Users should not log into the device using their personal accounts. All tablets are enrolled in the County Mobile Device Management to allow applications to be installed.

Users are responsible for the general care of the mobile device issued by the County. Mobile devices that are broken or fail to work properly must be taken to the IT Department for an evaluation. Mobile devices that have been lost, stolen or damaged from misuse, neglect or are accidentally damaged, in the sole and exclusive judgment of the County Manager in consultation with the County Attorney and CIO, will be replaced or repaired by the County, with the cost borne by the issued user. Mobile devices should remain free of any writing, drawing, stickers or labels that are not the property of the County.

Software and applications installed by the County must remain on the mobile device in usable condition and be readily accessible at all times. From time to time, the County may add or upgrade software applications for use by the user such that users may be required to check in their mobile devices with the IT Department for periodic updates and synchronizing. All software purchased by the County is property of the County and may not be transferred to any other individual. Personal software purchased and installed on County mobile devices are at the risk of the user/purchaser. The County offers no guarantee, warranty or support for

personal software purchased and installed on County mobile devices nor will the County refund any purchases for personal software installed on County mobile devices.

All of the County's computer systems and devices, including iPads and tablets, are considered to be public property. All documents, files and email messages created, received, stored in, or sent from any County mobile device is considered public record, subject to disclosure to the public pursuant to the North Carolina Public Records laws (with only limited exceptions as provided by law). Users shall not use the mobile device, computer or communication devices in any way as to violate the Open Meetings law requirements, applicable governing laws, or ethical conduct and principles of an elected public official.

Issued iPads, tablets and all County purchased accessories must be returned to the department head or IT Department when the user's term or service has ended. When the mobile device is returned, the County will conduct any appropriate backup of files in accordance with the Public Records and Retention laws. The mobile devices will then be wiped clean of any and all information.

The County reserves the right to inspect any and all files stored on mobile devices that are the property of the County in order to ensure compliance with this policy. Users should not presume to have any expectation of privacy in any matter created, received, stored in, or sent from any County issued mobile device.

Mobile Data Terminals (MDTs) – Public Safety

The security of the County's computer system is of paramount importance in maintaining an efficient and well-guarded database for referencing computerized information. Users will strictly adhere to the following guidelines on the usage of MDTs, regardless of type, make, or manufacturer and associated software to ensure compliance with federal copyright laws and protection against computer viruses. Any and all policies contained within the County's Technology Use Policy shall apply to MDTs.

MDTs, regardless of type, make, or manufacturer, have been installed in public safety vehicles to assist personnel in the execution of efficient public safety functions and to reduce the amount of radio traffic necessary to conduct public safety operations. Prior to use, personnel will be trained in the use and care of MDTs and are expected to use this equipment in accordance with instructions provided. MDTs are designed and have been programmed to provide information from State and National computer files on persons, vehicles and other property.

Employees shall use the MDTs to check information on persons, vehicles, and other property and shall not request these types of transactions be conducted by Dispatch. The only exceptions will be when an officer needs a printout of the information for inclusion with other reports or does not have an MDT or the MDT is not functioning properly. If the unit is not functioning properly, users are expected to request repairs as soon as possible during the normal working hours of the IT Department.

MDTs may be programmed to allow for communication of official public safety business between public safety vehicles and between field units and Dispatch. No vulgar, obscene, or derogatory messages, racially and/or sexually derogatory remarks shall be transmitted via the MDT nor shall any private, non-public safety business conversations be conducted between units through the MDT. All transmissions may be logged and maintained for future reference and to provide education and training as deemed necessary.

Employees shall log on with their designated username and password. Employees shall never use another employee's credentials. At the end of shift, personnel shall log off the MDT system.

All Internet policies must be followed when using MDT devices even if they are not connected to County Internet sources. The use of the Internet is not a private matter and the County reserves the right to monitor all uses without notification to the member; periodic audits may be conducted by the IT Department. The County reserves the right to inspect any and all files stored on MDTs that are the property of the County in order to ensure compliance with this policy. Users should not presume to have any expectation of privacy in any matter that is created, received, stored in, or sent from any County issued MDT. All MDT devices shall contain County management software/profile. Removal or attempt to bypass this software/profile will be in strict violation of this policy.

DESTRUCTION OF PUBLIC RECORDS

No public records shall be destroyed, sold, loaned or otherwise disposed of, unless in compliance with the NC Department of Cultural Resources and in accordance with G.S. 121-5.

COMPLIANCE

The CIO, department head and County Manager will review reported and perceived violations of this policy and may impose restrictions, suspend or terminate technology access, or remove technology equipment during or as a result of an investigation. The County Manager or CIO may, at any time, inspect or request to inspect any County equipment issued to any department or to any user. The user shall, immediately produce item for inspection. Failure to produce equipment within a reasonable time may result in disciplinary action. Other appropriate action in response to abuse or misuse of technology resources may include, but not be limited to:

- Reimbursement to the County for resources consumed
- Legal action, including action to recover damages
- Disciplinary actions, including suspension, demotion, or dismissal pursuant to the County's Personnel Policy

Department heads will be responsible for the enforcement of the County's Technology Use Policy.

MISCELLANEOUS

- Procuring, leasing, receiving, maintaining, and installing hardware or software for or on County networks shall be done only by or under the direction of the CIO.

- Due to technology systems constantly evolving, it is recommended that this policy be reviewed by County IT Department on a yearly basis.

HARNETT COUNTY

TECHNOLOGY USE POLICY

UNDERSTANDING AND ACCEPTANCE OF POLICY

I _____, have received/had an opportunity to review a copy of the Harnett County Technology Use Policy. I have read the policy in its entirety and have been provided the opportunity to ask questions about it. Furthermore, I fully understand and agree to comply with this policy. I also accept that it is my responsibility to seek clarification from my supervisor or HR staff if at any time I am unclear about the policy's requirements. I fully understand that failure to comply with this policy could result in disciplinary action, up to and including dismissal.

_____

Employee's (Legal) Printed Name

_____

Employee's Signature

_____

Date

HARNETT COUNTY

INFORMATION TECHNOLOGY DEPARTMENT

PO Box 1405
201 West Front Street
Lillington, North Carolina 27546
Phone: (910) 814-6388