COUNTY OF BLADEN

TECHNOLOGY USE POLICY

INFORMATION TECHNOLOGY DEPARTMENT

Adopted & Effective: October 7, 2019

County of Bladen

TECHNOLOGY USE POLICY

Table of Contents

County of Bladen

TECHNOLOGY USE POLICY

PURPOSE, SCOPE & OWNERSHIP

This policy covers the use of all technology resources belonging to the County of Bladen, 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, pagers, 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 will require approval of the department head, IT Director, Finance Director, and 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.

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. This policy does not address public access issues, which are covered under *Public Information and Public Access Guidelines for the County.*

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.

Computer worms – A self-replicating computer program that can harm the network.

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 facilities live chat

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

Mobile Devices – Computing appliance that is typically handheld.

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, MySpace, YouTube, Flickr, Blogger, Google+, 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 a company'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. The IT Director or his/her 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. The Request for Services form may also be used for changes to current employee access. This request should be sent directly to the IT Director from the department head and forwarded to Human Resources for inclusion in the employee's personnel file.

- Request for Services Forms, 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 IT Director 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, an email notification followed by Waiver of Services form will be submitted from the department head to Information Technology without delay. Access to all systems will be suspended immediately. The Waiver of Services form must be sent from the department head to Information Technology, who will suspend activities and forward a copy of the form to Human Resources for inclusion in the employee's personnel file.

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

- Information Technology will ensure security of unattended workstations by utilizing a group policy to lock computer screens after five (5) minutes of inactivity. Department heads may request a modification of this procedure through written request to the IT Director. 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 IT Director. 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 Information Technology to the department head. Computer owners are responsible for installing all required software. County Information Technology 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.

- For remote assistance help desk purposes, authorized industry partners 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 must be changed at any time a user believes their password has been compromised. Credentials including ID badges or key fobs that become lost, stolen or misplaced must be reported to the department head and IT Director 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 IT Director.

- 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 contain viruses and/or malware that may compromise the integrity and security of the County's network.

- Administrative rights are granted to Information Technology staff and those departments required by state regulations to have local administrative rights. Department heads must approve software requests and submit to Information Technology. 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. Proper authority will be granted through the Request for Services form.

- Users shall disclose to their department head, who shall then notify Information Technology 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 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 Information Technology.

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. The unacceptable use policy does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the County, or of any County department whose duties include activities that would otherwise be prohibited by this policy. However, exclusions to the unacceptable use policy should not be construed as permission to the individual employee when not in the course of their work.

Examples of unacceptable activities include but are not limited to:

- Private or personal, for-profit activities (e.g., consulting for pay, sale of goods such as Avon and Amway products, etc.) or for any illegal purpose, including but not limited to communications that violate any laws or regulations.

- The use of County Systems 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 is in strict violation of this policy and may face disciplinary action up to dismissal.

- 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 Information Technology notification.

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

PASSWORDS

Your login ID and password authenticate you as an authorized user of the County of Bladen computing environment. A strong password is key to the County's overall systems security. You must protect your files and County resources by choosing a good password and protecting it.

You are responsible for safeguarding the passwords for your computing accounts. Passwords must not be shared or disclosed to anyone including friends or family. If another person learns your password,

that individual has the ability to access your e-mail, your personal files, and your online network identity, and accounts. A knowledgeable person could use your account to attempt to gain unauthorized access to other networked resources, putting them at risk. No one should be given your password—not even someone from Information Services. Bear in mind, that the IT tech will not know the user's password. Therefore, the user must remain at their computer while the tech is working on their computer. The user may not reveal their password to the tech or anyone else. If you become aware that someone else has learned your password you must change it immediately.

Hackers gain access to systems by "cracking" accounts. They typically accomplish this through the use of automated processes to discover account IDs and passwords. Using a dictionary word or your account ID for a password puts your system (and the County's systems) at higher risk of attack by hackers. Therefore, the County will enforce password complexity in sensitive areas. Password complexity will be at a minimum as follows:

Your password must be at least 8 characters
cannot repeat any of your previous 24 passwords
must contain capitals, numerals or punctuation; and cannot contain your account or full name
English uppercase characters (A through Z)
English lowercase characters (a through z)
Numerals (0 through 9)
Non-alphabetic characters (such as !, $, #, %)
Passwords will expire every 60 days and the user will have to come up with a new password

Do not use the password that you choose for your County accounts with other off-work services such as Facebook, Twitter, LinkedIN, Google and Yahoo. This is to protect your work accounts in case those services are breached or in case your service provider does not encrypt passwords during the authentication process. You must change your password immediately if you notice unusual activity on your system or account. If you suspect that someone is accessing computing resources using your identity, you must contact Computer Operations.

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. Never 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, turn off the infected computer and report it to Information Technology. 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 Information Technology and loaded on every workstation and laptop computer. Users will be expected to check their anti-virus and anti-malware software definition dates weekly to ensure their computer is updating properly. If anti-virus or anti-malware is missing or not working, it is the responsibility of the user to notify their supervisor who will then email County Information Technology. Extra precaution should be taken with all mobile units.

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 Information Technology must be obtained.

COUNTY WEBSITES

In order to maintain a consistent, useful and professional presence on the Internet, Information Technology 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.

It is the responsibility of each Department and its employees 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 Information Technology 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 e-mail 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. Any email sent from County email accounts shall have the following disclaimer: "*DISCLAIMER: Pursuant to the Freedom of Information-Privacy Acts (FOIPA) and North Carolina General Statutes Chapter 132, Public Records, this electronic mail message and any attachments hereto, as well as any electronic mail message(s) sent in response to it may be considered public record and as such subject to request and review by anyone at any time.*" 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/archiving 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 (**http://www.records.ncdcr.gov/erecords/ Email_Policy.pdf**) or other regulatory agencies as applicable.

Personal email addresses being used for County business purposes, including but not limited to employees, County Council, 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.

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 10 MB). Users should utilize Dropbox or other means of sending large files to recipients.
- Sending or forwarding confidential information including but not limited to juvenile records in the Police Department, certain information contained in personnel files or medical files. This includes confidential information as defined by state and federal laws and agency regulations.

SOCIAL MEDIA

Social media is an additional medium commonly used to communicate with the public. The following policy outlines the necessary approval process to utilize social media for County business, as well as best practices and guidelines that all County employees will follow when communicating with the public through social media outlets.

For this policy, a basic definition of social media are resources similar to, but not all inclusive of, Facebook, Twitter, MySpace, YouTube, Flickr, LinkedIn, Google+, Vimeo, and various blogs.

The usage of social media is a tool for departments to reach out to populations who do not consume traditional media. It can be used as a tool to augment the traditional means of communications, and should be considered a part of communication strategies developed by each department.

As with all communication tools, social media should be used in ways that maximize transparency, maintain the security of the network, and are appropriately professional. Therefore, the application of social media within County departments must be done in order to effectuate the following purposes:

- Social media content should be thoughtful and professional so as to leave citizens and users of the media with a good impression of the County, and have a consistent and positive message about the provision of service by the County to its citizens;
- Care should be given so that content does not propose a risk to the County, particularly with vulgar or offensive content, libelous remarks, partisan political views, or other content that does not directly relate to the provision of public services; and,
- As social media communications are considered public records, such content must be retained for the time specified by the NC Department of Cultural Resources and applicable public records laws;

Authorization

Prior to any department utilizing social media outlets for communication with the public, the department head shall have approval from the County Manager.

Departments must be able to clearly define their intentions for social media. A department should be able to answer, at minimum, the following questions before initiating a request for approval.

- Whom is the media meant to reach? Is this my target audience?
- What is the department attempting to communicate? Can it be effectively communicated using this media?
- Does the department want to elicit feedback from citizens? What media is best suited to allow for the type of interaction desired?
- Who is responsible for managing the department's account? Will this person represent the department appropriately? Have they been properly trained in the use of social media?
- What are the department's responsibilities regarding collection and records retention, including preservation of social media content? How will the content be collected and stored?
- Is existing staff in the department sufficient to keep the media up to date, or will new staff be required?
- What is the planned update frequency for the department's social media outlet?

Acceptable Professional Use

All usage of social media shall follow applicable state, federal, and local laws. Employees and site managers are not to use any County sponsored social media for personal gain or to share personal information or opinions. Great care shall be taken when posting content/comments to prevent disclosing proprietary County information, sharing personal information of any member of County staff, the governing body, or the public, posting copyrighted or trademarked

material, and disclosing identities of individuals shown in photographs, especially if the subject is a minor, without written permission. For any content that County staff is unsure about the legalities of posting, consult with the County Manager, IT Director or County Attorney.

County staff should be aware of the Terms of Service (TOS) of the particular form of social media. Each form has its own unique TOS that regulates how users interact with the company and public. Any staff member using social media on behalf of the County should continually consult the most current TOS in order to avoid violations. If the TOS contradicts County or department policy, then the County Manager, IT Director, and County Attorney should be consulted to determine whether the use of such media is appropriate.

Security Requirements

Employees should be mindful of blurring their personal and professional lives when administering social media sites. No site used to promote any County Department, Board, Commission, or other County entity shall be created and linked with a personal social media account. A separate social media account must be established.

All social media sites/outlets that are managed under County representation will be secured with a password that meets the minimum requirements of the site, as well as be at least eight characters in length, and have at least one number. The passwords shall not be the same as what is used for any County user accounts or any personal accounts in order to avoid security attacks. For example, if John Doe is the site administrator and registers the account with their County e-mail address, the password used for the County e-mail account and the social media site will not be the same. Further, the password and any security questions should not be a common word or phrase that is associated with the County and easily guessable or compromised by outsiders. All County sponsored social media account information, logins, security questions and answers, and passwords will be provided to the IT Director and HR Director so account access may be recovered due to change in staff responsibilities. Account information provided to the IT Director and HR Director will be stored in a manner in order to avoid unauthorized access.

Content

Staff using social media to communicate on behalf of a County department will be mindful that any statements made are on behalf of County government; therefore, employees need to use discretion before posting or commenting. With most social media outlets, once comments or content has been submitted, they can be seen by anyone and may not be able to be redacted. County staff is always expected to remain courteous and professional in their interactions with the public.

Staff should always consider whether it is appropriate to post an opinion, commit oneself or one's department to a course of action, or discuss areas outside of one's expertise or control. There should be great care given to screening any communication made on behalf of the County using social media as improper posting and use of social media tools can result in disciplinary action.

As with other communications, communication via County and department social networking outlets is considered public record, and there is no expectation of privacy. This means that

content posted by County representatives and the public are likely to become part of the public record. Our board members should be mindful that it may be possible to create a situation where a quorum is created if too many members join a public conversation.

Departmental site managers/moderators should not allow the public to start new topics or add new content on social media pages that belong to the County. In addition, moderators should not respond to any removable comments from sites. This may turn removable content into a public record and make the content undeletable. Do not respond to service requests or complaints that are posted by the public on social media sites. It is at the discretion of the department on whether work orders or complaint resolutions are handled internally, but the requests or complaints are eligible for deletion until such time that communication is made with the poster on the social media site.

Disclaimers

The following indemnification statements shall be included on all County and departmental social media outlets.

Public Records:

This is the official {enter social media outlet name} for the County of Bladen, North Carolina, {department or facility}. This page is updated as needed and may not be regularly monitored for questions or comments. Any communication via this site (whether by a County employee or the general public) may be subject to monitoring and disclosure to third parties as a public record.

Content Disclaimer:

The County of Bladen makes use of a variety of forms of media to communicate to the public in an accurate, timely, and open manner. To that end, the County of Bladen has a {enter social media outlet name} page as one way to provide communication. The County welcomes participation and feedback from the public on this site. Once posted, the County reserves the right to delete comments that:

- *Contain vulgar language*
- *Are personal attacks of any kind*
- *Are offensive*
- *Are prejudiced or hurtful remarks made toward any person or entity, including an ethnic, racial, or religious group*
- *Are spam*
- *Include sales/promotion of goods or services, or links to other sites*
- *Are off-topic*
- *Advocate illegal activity*
- *Promote services, products, or political organizations*
- *Infringe on copyrights or trademarks*
- *Are requests for services*

Please note that comments expressed on the County's {enter social media outlet name} page do not reflect the opinions or positions of the County of Bladen, its employees, or elected officials.

Departmental Responsibilities

Each department that has a social media site will solely be responsible for adhering to this

policy statement and public records laws. It is highly recommended that all site managers attend a form of social media training and/or consult with departments or other municipalities that have shown to successfully manage their sites. Departments are also responsible for updating, managing, and confirming the accuracy of their site's content. All sites should be routinely monitored to insure that all public comments adhere to disclaimers as outlined above. Account administrators who receive messages through the private message service offered by many social media sites should direct the user to contact them at a public e-mail address maintained by the department or a representative, and/or to contact the department by telephone during normal business hours.

Personal Use

Employees are allowed to have personal social networking sites. These sites must remain personal in nature and be used to share personal opinions or non-work related information. This helps ensure a distinction between sharing personal and organizational views. In addition, employees should never use their government e-mail account or password in conjunction with a personal social networking site.

Revision

Technology and mediums of communication with the public are constantly changing. This policy will be modified as necessary to comply with issues that arise from usage, law changes, social changes, or best practices. Policy change recommendations should initially be directed to the IT Director, who will propose and make the changes at the direction of the County Manager.

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. Mobile device use and charges shall be monitored by the department head, the Finance Department and the IT Department. 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 IT Director immediately.

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 minutes/data and use free cellular connections whenever possible. 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

The County reserves the right to inspect any and all files stored on smartphones 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 smartphone.

Issued smartphones and all County purchased accessories must be returned to the **Bladen County Operations 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 any and all information.

iPads
The County has recognized that mobile devices, including iPads, may provide a benefit in the efficient performance of County duties and thereby improve service to the public. Users who choose to use their personal email/Apple ID accounts do so with the full knowledge that the content of that account is a public record and would be subject to North Carolina public records law. The iPads may be permitted to be used for both business and personal purposes as long as the personal use does not interfere with the performance or integrity of the device or affect the job performance of the user.

Users are responsible for the general care of the iPad issued by the County. IPads that are broken or fail to work properly must be taken to the IT Department for an evaluation. IPads 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 IT Director, will be replaced or repaired by the County, with the cost borne by the issued user. IPads should remain free of any writing, drawing, stickers or labels that are not the property of the County. Only a clean, soft cloth should be used to clean the screen.

Software and applications installed by the County must remain on the iPad 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 iPads with the IT Department for periodic updates and synchronizing. Software and application purchased and installed by the County will be purchased through a volume-purchasing program and installed through a uniform program to individual or all iPads as required. This provides licensing of the applications by the County and not the individual user. 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 iPads are at the risk of the

user/purchaser. The County offers no guarantee, warranty or support for personal software purchased and installed on County iPads nor will the County refund any purchases for personal software installed on County iPads.

All of the County's computer systems and devices, including iPads, are considered to be public property. All documents, files and email messages created, received, stored in, or sent from any County iPad 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 iPad, 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 and all County purchased accessories must be returned to the proper Department of origin when the user's term or service has ended. When the iPad is returned, the County will conduct any appropriate backup of files in accordance with the Public Records and Retention laws. The iPad will then be wiped clean of any and all information.

The County reserves the right to inspect any and all files stored on iPads 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 iPad. All iPad 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 IT Director, 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 IT Director 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

- Each department shall develop a backup schedule for all workstations. A backup

storage area will be provided for each user on the server. Information Technology will back up the server nightly.

- 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 IT Director.

- Information Technology will submit to each department an inventory of hardware and software annually. The department head shall verify this list and notify Information Technology of any changes.

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

County of Bladen

TECHNOLOGY USE POLICY

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.

I have read the County of Bladen Technology Use Policy and I understand and agree to its terms.

_____ _____

Employee Signature Date

_____ _____

Department Head Signature Date