



Granville County Government

Information Technology Policy

Adopted 08/05/2019

Granville County Board of Commissioners

Zelodis Jay, Chairman (District 1)

David Smith, Vice-Chairman (District 2)

Sue Hinman (District 3)

Tony Cozart (District 4)

Owen Roberts (District 5)

Timothy Karan (District 6)

Edgar Smoak (District 7)

Granville County Staff

Michael Felts, County Manager

Debra Weary, Clerk to the Commissioners

Chris Brame, IT Director

Staff contributors:

Charla Duncan (Administration)

Lynn Allred (Administration)

Matt Katz (Animal Control)

Trent Brummitt (Sheriff's Office/Emergency Communications)

Chris Brame (IT)

Jon Bullock (IT)

Justin Ayscue (Human Resources)

Will Robinson (Granville County Library System)

Scott Phillips (Development Services)

Monique Heggie (Internal Auditor)

Adonica Hampton (Social Services)

Table of Contents

I.	Purpose	6
II.	Scope	6
III.	Governance	6
	3.1 IT Steering Committee	6
	3.2 IT Staff.....	7
	3.3 Modifications to Policy.....	7
	3.4 Responsibility	7
	3.5 Department Specific Policies	8
	3.6 Compliance.....	8
IV.	Operational Policies	8
	4.1 Assessment and Training.....	8
	4.1.A. New employees	8
	4.1.B. Regular employee training	8
	4.1.C. Baseline testing and audits	8
	4.2 Managing Electronic Public Records.....	8
	4.2. A. Definition	9
	4.2.B. Confidential Records	9
	4.2.C. General Records Schedules.....	9
	4.2.D. Records Destruction.....	9
	4.2.E. Audit and Litigation Hold	9
	4.3 Acceptable Use.....	9
	4.3.A County Ownership and User Privacy.....	10
	4.3.B Confidential Information.....	10
	4.3.C Incidental Personal Use.....	10
	4.3.D Personal Use of County IT Staff	10
	4.3.E Prohibited Use.....	10
	4.3.F Granville County Library System Acceptable Use Policy.....	11
	4.4 Information System Security	11
	4.4.A Cell Phone Policy.....	11
	4.4.B Email Policy.....	11
	4.4.C Social Media	11
	4.4.D Department Specific Policies	12
	4.5 Life Cycle Management	12

4.5.A Refresh Policy	12
4.5.B Decommissioned Equipment.....	12
4.5.C Lost, Misplaced, and Damaged Equipment	12
4.6 Third Party Access	12
4.6.A Guest Networks.....	13
4.6.B Security Clearance.....	13
4.6.C Access to County Info and Special Protection Requirements.....	13
4.6.D Monitoring Compliance	13
4.7 Software Licensing and Usage	13
4.8 Voice Over IP	13
4.9 Physical and Environmental Protection	13
4.9.A IT Environment (Server Rooms, Network Rooms)	13
4.9.B Individual Work Stations.....	13
4.10 Common Shared Folders & Inter-Departmental Folders.....	13
4.11 Storage Limitations.....	14
4.12 Change Control	14
4.13 Copies and Printers.....	14
4.14 Key Cards and Door Systems	14
V. Technical Policies.....	14
5.1 Passwords	14
5.1.A Purpose.....	14
5.1.B Scope.....	14
5.1.C Department Specific Policies.....	14
5.1.D Information Technology Department Policy	14
5.1.E General Policy.....	15
5.1.F Password Construction Requirements	15
5.1.G Password Deletion	15
5.1.H Password Protection Standards.....	15
5.1.I Password Management and Centralized Storage	15
5.2 Audit and Accountability.....	15
5.3 Backup and Contingency	15
5.4 Firewalls and Protection Services	16
5.5 Remote Access Users	16
5.6 Account Administration	16

5.7 Contingency Planning.....	16
5.8 System Data and Security Maintenance.....	16
VI. Granville County Website	16
6.1 Public Posting of Website Policy.....	16
6.2 Website Administration	18
6.2.A Authorized Users	18
6.2.B New Users.....	18
6.2.C Deleting Users	19
6.2.D ADA Compliance	19
6.2.E Style Guide.....	19
APPENDIX A- Information Technology Policy Agreement.....	20
APPENDIX B- Cell Phone Policy.....	21
APPENDIX C- Emergency Communications Electronic Devices Policy	27
APPENDIX D- Email Policy.....	28
APPENDIX E- Social Media Policy	32
APPENDIX F- Emergency Communications Social Networking Policy	40
APPENDIX G- Social Media Policy Agreement.....	41
APPENDIX H- Photo Consent Form.....	42
APPENDIX I-Granville County Library System Acceptable Use Policy.....	43

I. Purpose

Granville County Government uses information technology for effective management of government programs and administration. The Granville County Information Technology Policy provides a foundation for the security of Granville County information systems. The policy is also designed to protect the integrity and reputation of Granville County Government and to ensure that the County's digital footprint is secure and in line with a consistent brand image. This policy provides departments and all staff, elected officials, appointed committee members, volunteers, interns, contractors, and vendors with the minimum requirements and guidance for securing Granville County information systems. The policy also provides users of Granville County information systems with the minimum guidelines for acceptable use of these systems. This policy is designed to mitigate risk factors and ensure the operability, availability, continuity, integrity, confidentiality, and privacy of Granville County information and communication systems, as well as the associated data and content.

Granville County's IT infrastructure is comprised of many components which include hardware, software, data storage, internet, telephony, services, and staff members. Each of these components has a finite amount of capacity. Each of these resources has a cost to the County. If a resource is monopolized or consumed by one staff member, it will not be available for co-workers. For the success of the County and for all staff members to be successful at their jobs, it is imperative that all users of the system coexist and share the resources responsibly. The guidelines set forth in the document will lay the foundation for optimal use of all resources. It will define the foundation for identifying when additional resources are required. Ultimately it will define the process for introducing, approving, obtaining, and deploying new resources.

This document is intended to be a common sense guideline for all participants. Adherence to these guidelines will provide the best user experience for all participants while providing maximum supportability based on the capabilities and limitations of the existing information technology infrastructure. This document is intended to be a living and breathing organism and is intended to evolve as the County, and all of its resources continue to grow.

II. Scope

This policy shall apply to all Granville County departments, personnel, interns, volunteers, elected officials, appointed board and committee members, vendors, contractors, and providers that develop, implement, administer, or use Granville County information and communication systems, data, and information.

III. Governance

Information technology (IT) security and compliance is a shared responsibility among Granville County staff, elected officials, interns, and volunteers. Granville County IT systems and practices are intended to support staff and help Granville County personnel, elected officials, and volunteers conduct County business in an effective and efficient manner. Proper IT governance is needed to ensure that IT staff and all other stakeholders using Granville County information systems are doing so in a secure and legal manner while delivering services to Granville County residents, businesses, and visitors in an effective and innovative manner.

3.1 IT Steering Committee

This policy will be monitored and revised by an internal Granville County Information Technology Steering Committee, composed of a cross-section of County personnel. This committee will include:

- 1-2 Information Technology (IT) staff
- Public Information Officer (PIO)

- County Manager or designee
- Human Resources Director
- Granville County Library System Director or designee
- Social Services Director or designee
- Emergency Communications Director
- Sheriff's Office designee
- Emergency Management Director or designee
- Animal Control Director or designee
- Development Services Director or designee
- Commissioner

Other committee members will be appointed as needed by the County Manager.

One of the primary purposes of the IT Steering Committee is to bring resources together from various departments to explore the benefits of technology in the workplace. This committee will inquire and examine the possible ways that IT can improve efficiencies and capabilities for all County resources and offerings. This committee should be used to present and share new ideas, and to provide a mechanism to introduce new solutions for the betterment of the enterprise.

The IT Steering Committee is responsible for ensuring the appropriate trainings are conducted as outlined in this policy. The IT Steering Committee will review the IT Policy annually. All changes to the IT Policy will be approved by the IT Steering Committee before going to the County Manager and the Board of Commissioners.

The IT Steering Committee works with IT staff and department heads to align IT with the overall goals of each department and the County, including making recommendations to the County about IT purchasing.

The IT Steering Committee will meet twice a year at a minimum (once before budget season) and additionally on an as-needed basis. The committee chair will be set by the County Manager.

3.2 IT Staff

Granville County operates with a full-time IT staff and works in conjunction with contract staff to provide IT services.

3.3 Modifications to Policy

At a minimum, this policy will receive an annual in-depth review by the IT Steering Committee to ensure that all policies and guidelines listed are up-to-date with current trends and needs of Granville County. All revisions to this policy will be approved by the IT Steering Committee, the County Manager, and the Board of Commissioners. Notice of any revisions to the policy will be sent via electronic mail to all personnel, elected officials, appointed board and committee members, and volunteers within 5 business days of revision approval.

Outside of an annual review or any regular Information Technology Committee meetings, any modification requests of this policy are to be made to the IT Steering Committee Chair and/or their designee and the County Manager.

The addition and/or updates of department specific policies can be added and/or amended and/or updated without the entire Countywide policy needing to go before the Granville County Board of Commissioners for an updated adoption. The appendix of the Granville County Information Technology and relevant references can be updated as needed.

3.4 Responsibility

Information technology security, integrity, and brand consistency is a shared responsibility among all users of Granville County information systems.

3.5 Department Specific Policies

Department heads may implement a departmentally specific information technology policy. These department specific policies must meet the Countywide policies at a minimum. Department specific policies must be approved by the County Manager and/or the respective departments' governing boards.

3.6 Compliance

All Granville County personnel are expected to comply with this policy at all times. Violations and non-compliance may be subject to disciplinary action according to the Granville County Personnel Ordinance (found on the Granville County website).

Granville County elected officials, appointed board and committee members, interns, volunteers, contractors, and vendors may be subject to any and all remedies allowed by law for any violations and non-compliance of this policy.

IV. Operational Policies

4.1 Assessment and Training

Granville County Government's information technology security and compliance is a shared responsibility among all personnel, elected officials, interns, and volunteers. It is important that all individuals responsible for conducting County business do so in a secure manner that is compliant with the all local, state, and federal laws.

4.1.A. New employees

New employees will receive training in Granville County information technology and compliance within 45 days of their hire. All new employees will sign the Granville County Information Technology Policy Agreement (Appendix A) stating that they received training on County information technology security and compliance and that they will abide by the items outlined in this policy.

New employees should complete an initial email security awareness training before access is granted to a Granville County email account.

New employees should complete training on cell phone use and social media. Upon completion, new employees will sign the Granville County Cell Phone Policy Acknowledgement and Agreement (Appendix B) and the Granville County Social Media Policy Acknowledgement and Agreement (Appendix G).

4.1.B. Regular employee training

Employees of Granville County will receive ongoing and regular training on topics related to information security and compliance from the IT Department. Trainings will happen a minimum of once per year and may occur in-person or online. Employees will annually sign the Granville County Information Technology Policy Agreement at their annual training.

4.1.C. Baseline testing and audits

Reserved for content.

4.2 Managing Electronic Public Records

The management of electronic public records is a matter of legal, ethical, and organizational importance.

4.2. A. Definition

An **electronic record** is a record that is created or reproduced in any medium by means of any system requiring the aid of electronic technology to make the record intelligible by a person, and which is dependent upon a combination of hardware, software, and computer files. “Electronic record” refers to both records created electronically and digitalization of records created in other formats. Electronic records must meet the same legal requirements as paper records (the State Archives of North Carolina provides this information). To read more about public records, read the NC General Statute 132, which covers public records.

4.2.B. Confidential Records

Confidential records include, but are not limited to:

- Medical and mental health records
- Personnel records
- Prison records
- Student records
- Blueprints for public buildings
- Bank account records
- Social Services records deemed confidential according to DSS Policies

4.2.C. General Records Schedules

Records produced by local agencies must be retained for the period of time required by local records retention and disposition schedules. County records retention and disposition schedules are available on the State Archives website under the “For Government” tab (www.ncdcr.gov/archives).

4.2.D. Records Destruction

According to the state’s General Statutes, no public official may destroy, sell, loan, or otherwise dispose of any public record, except in accordance with G.S. 121-5 and G.S. 130A 99, without the consent of the Department of Cultural Resources.

4.2.E. Audit and Litigation Hold

If there’s a lawsuit, or even a possible lawsuit, the County may be required to retain records, including the metadata associated with electronic records, even if the records could be destroyed legally under the retention rules.

4.3 Acceptable Use

Granville County information systems are intended for performing Granville County business. All staff, elected and appointed officials, interns, and volunteers are expected to abide by this policy, as well as any other applicable local, state, and federal laws, regulations, and policies.

Granville County information systems include, but are not limited to:

- Desktop PC’s
- Mobile devices such as laptops and tablets
- Granville County issued cell phones and other data devices (including MiFis)
- Granville County email systems
- Granville County Wifi and internet

4.3.A County Ownership and User Privacy

Information systems that are provided by Granville County Government are provided for government use and Granville County owns all property rights to any content or other matter created, received, transmitted, stored on, or deleted from any Granville County information system.

Users of Granville County information systems should not have any expectation of privacy in any message, file, image, or data created, sent, or retrieved from use of these Granville County systems. Storage of user's personal information on Granville County systems is done at the user's risk. Such information may also be subject to public disclosure or review by Granville County officials, including personal cell phones.

4.3.B Confidential Information

All users of Granville County information systems shall comply with all laws, regulations, and Granville County policies and procedures around confidential and sensitive information.

4.3.C Incidental Personal Use

Personal use is when an employee, elected official, intern, or volunteer uses a Granville County information system for a reason that is not related to the purpose for which that user was granted access to that system. Incidental personal use of Granville County's information systems is permitted unless the department for which the user works or volunteers sets additional restrictions on personal use of Granville County information systems.

Personal use of Granville County information systems is prohibited when it:

- Interferes with the user's productivity or work performance
- Interferes with the productivity or work performance of others
- Has an adverse effect on Granville County information systems
- Is illegal or violates Granville County policy
- Violates State or Federal information systems policies governing departmental services

Staff, elected officials, interns, and volunteers are discouraged from using government systems for personal use. Users must present their personal communications using Granville County information systems in such a way to make it clear that those communications are personal and are not made as a representative of Granville County.

Storage of personal records on Granville County information systems shall be kept to a minimum. Any personal storage that IT determines interferes with efficient operations of Granville County's information systems is subject to removal.

4.3.D Personal Use of County IT Staff

Granville County IT personnel should not be used to address issues on a staff member's personal equipment during work hours. IT personnel are free to work jobs outside of their Granville County duties as long as these jobs are not in violation of the Granville County Personnel Ordinance (§175). IT personnel that are asked to work on the personal devices of elected officials and appointed committee members in relation to official Granville County business should do so during work hours; these devices should be deemed necessary for conducting Granville County business.

4.3.E Prohibited Use

Certain activities are prohibited when using Granville County information systems (including Granville County Wi-Fi) and resources, except when the County Manager has determined it necessary for the performance of a user's official duties. These activities include:

- Accessing, downloading, transmitting, printing, or storing information with sexually explicit content
- Downloading or transmitting defamatory, harassing, or discriminatory messages or images
- Accessing or downloading gambling sites
- Engaging in violation of any Granville County policy
- Accessing/downloading illegal software

4.3.F Granville County Library System Acceptable Use Policy

The Granville County Library System use information systems for both employees and library patrons. To view the full Granville County Library System Acceptable Use Policy for employees and patrons, see Appendix I.

4.4 Information System Security

Granville County information systems include cell phones and electronic devices, electronic mail, and social media. Employees, elected officials, volunteers, and interns may use all of these types of information systems in both their professional and their personal life. The policies set forward in this section are meant to secure Granville County information systems, as well as protect both the County and the employee.

4.4.A Cell Phone Policy

Cell phone technology is a valuable communication tool for Granville County employees. Voice, text, and data functions-as well as other cell phone and smart phone features-make this tool necessary and effective for certain Granville County employees in transacting official Granville County business.

The full Granville County Cell Phone Policy can be found in Appendix B.

Department heads may implement a department specific cell phone policy. These department specific policies must meet the Countywide policies at a minimum. Department specific policies must be approved by the department head and the County Manager and/or the departments' governing boards.

4.4.B Email Policy

Granville County employees, elected officials, interns, and volunteers rely on electronic mail (email) as a major communication tool to carry out government business. Most email messages have administrative, fiscal, legal, reference, and/or archival value. This policy ensures that records created, sent, and received through email are managed in accordance with established laws for creating, maintaining, and disposing of all government records. Following this policy will also help to ensure that email messages are available for public records requests. This policy and the mandates and guidelines within it are here to ensure effective management and retention of electronic messages.

Full Email Policy located in Appendix D.

4.4.C Social Media

Granville County Government uses social media as tool not only to broadcast information, but to actively engage our citizens, businesses, partners, and visitors in the County's daily activities and strategic objectives. Social media platforms are used to create a more efficient government, as well as to actively recruit talent to our County and partner strategically with other organizations.

In using social media platforms, Granville County hopes to have a more fluid and informal method of communicating with stakeholders and to use social media to create trust and build a positive reputation with all stakeholders. In order to achieve all of these things, all staff, elected officials, and

volunteers are expected to maintain a consistent agency and organizational identity established by Granville County Government.

View the entire Granville County Social Media Policy located in Appendix E. A Social Media Policy Acknowledgement and Agreement Form is located in Appendix G.

Department heads may implement a department specific social media policy. These department specific policies must meet the Countywide policies at a minimum. Department specific policies must be approved by the department head and the County Manager and/or the departments' governing boards.

See Appendix F for the Granville County Emergency Communications Social Media Policy.

4.4.D Department Specific Policies

- **Emergency Communications:** See Appendix C for the Granville County Emergency Communications department specific Electronic Devices Policy. All Granville County Sheriff's Office personnel will follow the Granville County Policy as the minimum standard, as well as comply with the department specific Emergency Communications policy.

4.5 Life Cycle Management

In order to maintain the highest degree of security and productivity, Granville County staff will manage the life cycle of equipment in accordance with a Countywide refresh policy. A support contract will be purchased and maintained for all business critical systems, servers, and software.

4.5.A Refresh Policy

- Standard Desktop Systems & Laptops: Maximum Lifetime should not exceed 5 years; recommended to replace every 4 years
- Power Desktops - 24/7 usage: Should not exceed 4 years; recommended to replace every 3 years to retain warranty coverage
- Servers: Should not exceed 8 years with an upgrade performed at the midterm (4 years); warranty is 5 years
- Standard Desktop Printers: Should not exceed 5 years

4.5.B Decommissioned Equipment

Computer Equipment that has hit EOL (end of life) should be disposed of by the IT department to ensure all sensitive data has been correctly removed. Non-computer equipment, such as printers, phones, etc. can be disposed of through the electronic recycling contract.

4.5.C Lost, Misplaced, and Damaged Equipment

Lost/stolen equipment should be reported to the IT department immediately. A disclosure of what sensitive information could reside on the equipment should be reported.

Damaged equipment should be reported to the IT department.

4.6 Third Party Access

Vendors, contractors, partners, interns, and/or volunteers when connecting remotely should use an approved remote software client. When accessing the network-both remotely and on premise-third parties should use a unique login with correct access permissions. A third party should never have access to an administrator account.

4.6.A Guest Networks

General public should only connect and use designated *guest networks* to isolate their devices from county equipment. Interns and volunteers are considered guests and need to use guest networks.

4.6.B Security Clearance

See section 4.10.

4.6.C Access to County Info and Special Protection Requirements

Access to County equipment may be monitored and audited at any time by the IT department (and/or the Internal Auditor) for unauthorized access.

4.6.D Monitoring Compliance

Reserved for content.

4.7 Software Licensing and Usage

Software installs should be performed by the software vendor or the IT department to ensure connectivity and functionality.

Software inquiries should funnel through the IT department to determine if Granville County already owns a comparable software.

All software licenses should be funneled through IT department to maintain standardization.

Software agreements should be between Granville County and the third party (not individual departments and the third party) with the exception of necessary arrangements between the Granville County Sheriff's Office, Granville County Emergency Communications, and Cooperative Extension (as needed).

Software should stay up-to-date with the latest stable release from the respective vendor.

4.8 Voice Over IP

Reserved for content.

4.9 Physical and Environmental Protection

Reserved for content.

4.9.A IT Environment (Server Rooms, Network Rooms)

The physical locations of the network and server equipment should remain locked and secure at all times. Access to the equipment rooms should only be given to the required personnel. Equipment rooms should not store unrelated objects (for example: trash, shovels, lawn equipment, vacuums, mops, etc.). Equipment rooms should be monitored and maintained by the IT department to ensure their functionality and security. In the event of power, AC, or general functionality outage, the IT environment rooms should become a priority for the maintenance department in order to get the outage resolved.

4.9.B Individual Work Stations

Reserved for content.

4.10 Common Shared Folders & Inter-Departmental Folders

No sensitive documents may be stored in commonly shared folders. These folders are accessible by any County employee and are not protected.

Sensitive documents may be stored in protected department folders. Access to these folders should be monitored and maintained. Any documents considered stale (5 years) should be moved to archival long-term cold storage or other long-term archival method.

Scanner files can be accessed by all County offices; therefore, use extra caution when scanning confidential information. Scanner files will be cleared every 24 hours. Departments interested in setting up special scan folders with longer storage time should contact IT for set-up.

4.11 Storage Limitations

Departments shall be given a storage quota. If this quota is nearing capacity, an increase may be requested through the IT department and approved by the County Manager (additional purchase may be required). Users should not store unrelated files to the storage location on storage devices. Any personal documents stored on Granville County equipment may be removed by IT to clear storage space.

4.12 Change Control

Reserved for content.

4.13 Copies and Printers

Reserved for content.

4.14 Key Cards and Door Systems

Reserved for content.

V. Technical Policies

5.1 Passwords

Passwords are an important part of security. All Granville County employees, elected officials, interns, and volunteers (as well as contractors and vendors with access to Granville County systems) are responsible for taking the appropriate steps to select and secure their passwords.

5.1.A Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

5.1.B Scope

The scope of this policy includes all personnel who have or are responsible for an account on any system that resides at any Granville County facility and/or has access to the Granville County network.

5.1.C Department Specific Policies

Department heads may implement a departmentally specific password policy. These department specific policies must meet the Countywide policies at a minimum. Department specific policies must be approved by the County Manager and/or the respective departments' governing boards.

5.1.D Information Technology Department Policy

Passwords required for servers and network equipment, including Administrator and root passwords, will have their password changed at a maximum of every 90 days. Administrator and root

level passwords shall not be disclosed outside of the IT department with the exception of the County Manager.

IT Director will store each Administrator passwords inside a two-factor authentication password database (KeePass). At least one external authentication key will be given to the County Manager for safe keeping.

5.1.E General Policy

- All user-level passwords must be changed at least every 90 days.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level passwords must conform to the guidelines described below.
- User accounts will be locked after 5 incorrect tries; contact IT for assistance

5.1.F Password Construction Requirements

Passwords must be a minimum of 8 characters, including at least 1 capital letter and at least 1 number. Passwords should not contain the user's account name.

5.1.G Password Deletion

When a user leaves, IT will reset the password to all Granville County domain accounts for that user. Department heads are responsible for ensuring all other passwords protections and deletions are put in place for exiting employees.

5.1.H Password Protection Standards

- Do not share Granville County passwords with anyone outside of IT, including administrative assistants or secretaries.
 - This would also include setting up a new phone at Sprint, Verizon, BestBuy, etc.
- Don't reveal a password in an email message.
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members
- Don't reveal a password to a co-worker while on vacation.
- Don't write passwords down and store them anywhere unsecured in your office.

If someone demands a password, refer them to this document or have them call the County Manager.

If an account or password has been compromised, report the incident to IT and change all passwords.

5.1.I Password Management and Centralized Storage

All employees are strongly encouraged to track passwords to all accounts used for Granville County business, complying with the Granville County password policy. Department heads are encouraged to work with IT staff to discuss appropriate options for password management and storage. Password management is strongly encouraged to be a part of a department's onboarding and exiting process. The County Manager will work with department heads to track critical passwords for departments.

5.2 Audit and Accountability

All network access should be monitored by the IT department; unauthorized or improper use will terminate and report to the County Manager for review and accountability.

5.3 Backup and Contingency

End users should be responsible for their own backups. End users should consult IT staff before using a new backup device.

All end user backup devices should be dedicated for use on Granville County systems and Granville County equipment. Backup devices used for Granville County business should be not used on unapproved personal devices or non-County equipment.

5.4 Firewalls and Protection Services

All County-owned devices connected to Granville County's network should have Granville County's anti-virus software installed prior to connection.

In the event that a department head chooses to have a staff member use their personal device to conduct Granville County business, the department head should purchase anti-virus software for protection on personal devices.

5.5 Remote Access Users

Access to the Granville County networks via remote access is to be controlled by using either a Virtual Private Network or a form of an advanced authentication.

5.6 Account Administration

Reserved for content.

5.7 Contingency Planning

All Granville County departments must have a Continuity of Operations Plan in place. Department heads are strongly encouraged to consult the IT department in regard to contingencies involving information systems and technology.

5.8 System Data and Security Maintenance

Desktop computer systems should stay current on security patches and on the latest supported version operating system for their workload. Servers should have a scheduled monthly maintenance window to perform any security patches and software updates.

VI. Granville County Website

Granville County uses its website as a source of information dissemination for community, businesses, and visitors; it is also as a communication tool for the public to reach Granville County personnel and elected officials.

6.1 Public Posting of Website Policy

The following information should be posted on the Granville County website:

The information contained in the Granville County web site is provided as a public service. The contents of this web site are subject to periodic change. Information represented is not intended to replace official sources. Although every attempt will be made to ensure that the information is accurate and timely, the information is presented "as is" and without warranties. Information contained on the Granville County web site should not be mistaken for legal advice. Information on the website should not be considered error-free and should not be used as the exclusive basis for decision-making. Use of web site information is strictly voluntary and at the user's sole risk.

Other resources linked from these pages are maintained by independent providers. The County does not monitor all linked resources and cannot guarantee their accuracy. Statements, views, and opinions included in an independent provider's material are strictly those of the authors. These views may not necessarily represent the opinions or policies of the County, its elected officials, agents, officers, or employees.

Privacy Policy

Purpose

This policy describes privacy practices regarding information collected from the Granville County web site. It contains information about what data are collected and how that information is used. This policy may be updated periodically, so please check back from time to time.

This policy applies only to the official Granville County web site. When you follow a link to another web site, even the site of another governmental agency, you are subject to the privacy policy of that site. You should check the privacy policies of each of these sites if you have questions about how they handle personally identifiable information.

Automatic Collection of Certain Information

No personally identifiable information is collected from visitors who simply browse this site or who download information from it. While our web servers maintain logs of user activity to help us manage the web site, information stored in these logs does not identify you personally. The logs store things such as the domain name and IP address from which you access our site, the type of browser and operating system you used, the date and time you accessed our site, the pages visited and the address of the site that you linked to us from (if you linked to our web site from another web site). We use this information to learn how many visitors we have, where they are coming from, which parts of our web site are of most interest to visitors, and other facts that will help us improve the web site and the services we offer.

If You Send Us Personal Information

Visitors who request services through this site may be required to furnish additional information in order for us to provide the service requested. The additional information collected will be no more specific than if the visitor were requesting the service by any other means, including by telephone or an in-person visit to a County facility. If you participate in a survey or send us an email, your email address and the other information you volunteered will be collected. We may share this information with other governmental agencies or organizations to provide the help you are requesting. We may also use that information to help assess user needs and analyze trends.

Privacy and Security

We will not rent, sell or give away any information identifying you individually (name, address, phone, number, etc.) to third parties for marketing or mailing list purposes without your permission. We will not send you unsolicited e-mail regarding any commercial offers or advertisements at any time.

Some information that you submit to us through this web site may be protected by encryption technology, whereas other information may not. Unless a particular web page on this site indicates that encryption technology is being used, you should not assume that information you submit through that web page will be secure. If you submit information to our server through a web page containing visible indicators of active encryption technology, we will take reasonable precautions to safeguard the confidentiality of such information. However, no web site can protect itself against all eventualities. Granville County will not be held liable for any injury caused by the disclosure of your information, whether by security breach, accident, inadvertence, or any other act resulting in disclosure.

Use of Cookies

Cookies or other technology may transfer information from this web site to your hard disk for record-keeping purposes. Cookies or similar technology can make the Internet more useful by storing information about your preferences on a particular site. The use of cookies or similar technology is an industry standard, and this web site, like many other web sites, uses them to provide useful features for our users. Cookies in and of themselves do not personally identify you, although they do identify your computer. Most browsers are initially set up to accept cookies. If you prefer, you can set your browser to refuse cookies. However, you may not be able to take full advantage of this web site if you do so.

Public Records

Granville County is governed by the North Carolina public records laws. This means that the information we receive online might be disclosed to any person making a public records request. Certain types of information are exempt from disclosure as public records. If you have questions about the North Carolina public records laws, refer to N.C. General Statute Chapter 132. For purposes of determining whether information is a public record, information sent to us through this web site is treated the same as information sent to us by mail or delivered to us in person.

Choices and Opting Out

While accessing our site, you may decline participation in any activity that asks for information (i.e. survey or e-mail). Your choice not to participate will in no way affect your ability to use any other feature on our site. You can “unsubscribe” to notices sent to you automatically by e-mail in one of the following ways:

- Each e-mail sent to you provides an automatic way to unsubscribe to a mailing list;
- You can unsubscribe by clicking the “Unsubscribe” link from the Granville County home page.

Altering Forms Warning

Unauthorized attempts to upload information or change information on this web site including unauthorized alterations to the wording of any online forms available on the site, are strictly prohibited. Alteration of the wording of downloadable or online forms renders the forms invalid. Unauthorized interference with the operations and functions of this web site, by electronic or other means, is strictly prohibited. Any attempt to use any information, feature, or other aspect of the site to engage in criminal conduct will be vigorously prosecuted. Any unlawful actions may be subject to criminal prosecution under the Computer Fraud and Abuse Act of 1986, and other criminal laws, and may also result in civil liability.

Questions and Comments

Web site content is maintained and updated by each individual County department. All questions regarding specific contents should be directed to the manager of the department for which the question is related. General comments from the public about our website are welcome and can be directed to Granville County Administration.

6.2 Website Administration

The Granville County website will be administered by an administrator appointed by the County Manager. Each department is responsible for the content of web pages pertaining to their department. Departments are expected to comply with the listed public policy in section 6.1.

6.2.A Authorized Users

Department heads are strongly encouraged to have no more than 3 authorized users with access to the Granville County website. It is strongly encouraged that users be identified as the primary user, secondary user, and tertiary or back-up user and/or that the department head has a plan in place involving the creation and oversight of content within their department.

6.2.B New Users

Department heads may not create new user logins. Requests for new user logins go to the website administrator. New users should receive a website training from the Administration Office before access is granted to the website. Exceptions to this policy should be cleared by the website administrator and/or the County Manager.

6.2.C Deleting Users

Department heads may not delete user logins. Any change in administrative access to the website must be made by the website administrator. If an employee leaves Granville County or if an employee is no longer responsible for updating the website, department heads must notify the website administrator of the needed change.

6.2.D ADA Compliance

The Granville County website will work to achieve and maintain ADA compliance.

6.2.E Style Guide

Reserved for content.

APPENDIX A- Information Technology Policy Agreement

Granville County Information Technology Policy Agreement

Employee Name: _____ Employee ID: _____

Job Title: _____ Dept: _____

I have received training on Granville County Information Technology Policy. I have read, understand, and agree to comply with the Granville County Information Technology Policy.

- Check this box if form is signed at initial training for new employees.
- Check this box if form is assigned as a part of an employee's annual training.

Employee's Signature

Date

APPENDIX B- Cell Phone Policy

Granville County Employee Cell Phone Policy

I. PURPOSE:

Cell phone technology is a valuable communication tool for Granville County employees. Voice, text, and data functions-as well as other cell phone and smart phone features-make this tool necessary and effective for certain Granville County employees in transacting official Granville County business. The purpose of this policy is to outline legal requirements for electronic records and open meeting laws regarding cell phone technology, as well as to establish policies around cell phone use by employees of Granville County.

II. ELECTRONIC MESSAGES AS PUBLIC RECORD

Electronic messages, including texts and emails, are considered public record under North Carolina General Statutes Section 132 and will be managed as such.

G.S. § 132-1(a)

"Public record" or "public records" shall mean all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions.

Public records include anything created in the course of public business *regardless of format*. Granville County business that is conducted on a cell phone is subject to public record law. Any record made or received in the transaction of public business is subject to public access unless an exception applies. Records created by government staff on personal devices are public records if the content involves public business.

Retention schedules for electronic records may vary by department and/or topic. Content created by Granville County staff, elected officials, appointed boards members, and volunteers conducting county business is subject to state retention schedules.

In certain circumstances it is possible for an employee to be required to turn their cell phone over to County administration, law enforcement, and/or the court system

III. OPEN MEETINGS

Granville County elected officials and appointed board and committee members are subject to open meeting laws. A quorum of board members holding a discussion about public business through text messaging or on a group call (or by email) may constitute a meeting that is subject to the open meetings law.

IV. EMPLOYEE CELL PHONE STIPEND

Employees requiring cell phones to perform their work will receive a stipend to compensate for business use of an employee purchased, employee owned, and employee operated cell phone. The stipend will be included in the employee's pay check. This is a non-accountable plan; therefore, additional receipts and documentation are not required once the stipend has been approved by the Department Manager and Human Resources.

Employees that conduct official Granville County business on their personal cell phone devices are subject to public records and open meeting laws.

Requirements for the stipend include:

- Employees must retain an active cell phone contract as long as they receive a cell phone stipend. Department heads and the Internal Auditing Department retain the right to receive a copy of an employee's cell phone payment invoice to verify an active contract.
- Employees are responsible for all costs related to the phone including accessories.
- The County makes no distinction between brand or type of phone that an employee may choose to use.
- Granville County Government is not responsible for any damages that occur to an employee's personal cell phone.
- Employees receiving a cell phone stipend will not also receive a county purchased and county owned phone. Exceptions to this rule must have a documented need and must be approved by the County Manager.
- Any costs incurred over and above the stipend are the responsibility of the employee.

If cell phone stipends are discontinued, Granville County will give employees a 90-day notice of termination.

4.A Exceptions

There are two exceptions to the employee cell phone stipend.

Exception 1: County Purchased, County Owned, Employee Operated

The first exception to this policy will be cell phones that are County purchased, County owned, and employee operated. Example: The employee requires a cell phone to perform their work but does not wish to use a personal phone and receive a stipend.

With this option, cell phones supplied by the County are meant to be used for County business. Personal calls (outgoing and incoming) will be allowed in limited and infrequent instances, namely emergencies. Incidental personal use of Granville County equipment should be kept to a minimum and in compliance with Granville County Information Technology policies. Call logs (of personal calls only) will be audited each month by the Internal Auditing Department. The employee may also be subject to disciplinary action for violations of policies regarding a County-owned cell phone.

Training on the Granville County Cell Phone Policy and completion of the necessary forms must be completed before employees receive a cell phone.

A screen lock code is highly encouraged on all County-owned cell phones.

Exception 2: County Purchased, County Owned, Department Group Use

The second exception will be cell phones that are County-purchased, County-owned and maintained by departments for group use and are not assigned to specific individuals.

With this option, departments will be required to maintain a detailed log of employees checking in and out the assigned phone. The log will be subject to review each month by the Internal Auditing Department. Employees may be subject to disciplinary action for violations of policies regarding a County-owned cell phone

A screen lock code is highly encouraged on all County-owned cell phones.

Training on the Granville County Cell Phone Policy and completion of the necessary forms must be completed before employees receive a cell phone.

Incidental Personal Use of County Systems

Personal use is when an employee, elected official, or volunteer uses a Granville County information system for a reason that is not related to the purpose for which that user was granted access to that system. Incidental personal use of Granville County's information systems is permitted unless the department for which the user works or volunteers sets additional restrictions on personal use of Granville County information systems.

Personal use of Granville County information systems is prohibited when it:

- Interferes with the user's productivity or work performance
- Interferes with the productivity or work performance of others
- Has an adverse effect on Granville County information systems
- Is illegal or violates Granville County policy
- Violates State or Federal information systems policies governing departmental services

Staff, elected officials, and volunteers are discouraged from using government systems for personal use. Users must present their personal communications using Granville County information systems in such a way to make it clear that those communications are personal and are not made as a representative of Granville County.

Storage of personal records on Granville County information systems shall be kept to a minimum. Any personal storage that IT determines interferes with efficient operations of Granville County's information systems is subject to removal.

4.B Eligibility for Cell Phone Stipend

Eligible positions are identified in the Granville County Pay and Classification Plan on file with Human Resources. Exceptions to eligible positions must be approved by the County Manager. General eligibility involves:

Voice Plan:

- 30% or more of work hours are outside of the office
- Job duties require on-call status
- Job duties are in public safety requiring immediate or emergency response
- Primary mode of communication is the cell phone to stay in contact with county offices, contractors, etc.

Data Plan:

- Frequent need to information such as email, contacts, calendar, etc. while away from the office.

Data plans must be approved by the County Manager. Department Managers are responsible for determining the need for eligible employees prior to employee applying for stipend.

Training on the Granville County Cell Phone Policy and completion of the necessary forms must be completed before employees receive a cell phone stipend.

V. NON-EXEMPT EMPLOYEES

Department heads are responsible for orienting non-exempt employees to FLSA regulations, especially in regard to cell phone use per this policy.

VI. DEPARTMENT DISCRETION OF CELL PHONE POLICY

Department heads may implement a department specific cell phone policy. These department specific policies must meet the Countywide policies at a minimum. Department specific policies must be approved by the department head and the County Manager and/or the respective departments' governing boards.

**Granville County Employee
Cell Phone Stipend Authorization**

Employee Name: _____ Employee ID: _____

Job Title: _____ Dept: _____

Indicate choice by circling A or B

Option A) Employee Purchased, Employee Owned & Employee Operated

The employee listed about is eligible and authorized to receive a monthly calling plan allowance as indicated below:	
<input type="checkbox"/> Voice Plan \$30	Department Manager's Initials: _____
<input type="checkbox"/> Data Plan \$30	County Manager's Signature: _____
This is a non-accountable plan therefore additional receipts and documentation are not required. Cell phone allowance is taxable income and it subject to applicable payroll taxes. By accepting the monthly cell phone allowance, I do hereby agree to use my own personal cell phone so that I may be reached during regular business hours and/or during emergencies when applicable. I agree to have a working cell phone and to furnish the County of Granville with a valid working cell phone number at all times. I further agree to contact my Department Head/Manager and payroll office if I change or cancel cell phone services. Failure to contact the payroll office may result in a repayment of the allowance.	
Cell Phone Number: _____	Employee's Initials: _____

Option B) County Purchased, County Owned & Employee Operated

Employee agrees to using phone for primarily for County business. The employee will maintain a log of incoming and outgoing personal calls. Cell phone bill for log period must be kept with the log by the Department for audit purposes for 1 year.
Employee's Initials: _____

I have read, understand, and agree to comply with the Granville County Cell Phone Policy for cellular device use. I acknowledge that my cell phone account records may in certain circumstances be considered public records in accordance with NC General Statutes and may need to be turned over to the County upon request.

Employee's Signature _____
Date

Department Manager's Approval _____
Date

Human Resources/Payroll Approval _____
Date

Stipend Total Amount: \$ _____

Effective Start Date: _____

**Granville County Employee
Cell Phone Policy
Acknowledgement and Agreement**

Employee Name: _____ Employee ID: _____

Job Title: _____ Dept: _____

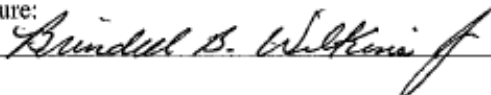
I have read, understand, and agree to comply with the Granville County Cell Phone Policy. I acknowledge that my cell phone account records may in certain circumstances be considered public records in accordance with NC General Statutes and may need to be turned over to the County upon request.

Employee's Signature _____
Date

Department Manager's Approval _____
Date

APPENDIX C- Emergency Communications Electronic Devices Policy

Granville County Sheriff's Office Emergency Communications

Policy Number: 2019-001	Effective Date: 3-07-19
Policy: Electronic Devices	Revised Date: 7-03-19
Signature: 	Page 1 of 1

Purpose:

Granville County Sheriff's Office Emergency Communications recognizes the importance of allowing employees to remain in contact with family and friends for personal matters while at work. This policy outlines requirements to prevent distractions within the Emergency Communications Center, as well as ensure responder safety and maintain proper safeguarding of information.

Policy:

1. All permitted electronic devices are to be fully muted or on vibrate while inside the Communications Center.
2. Personnel working console positions shall take all personal phone calls outside the Communications Center with the permission of the supervisor on duty. All personal calls shall be limited to a reasonable time, and shall not distract from the employee's primary duties or distract other employees from their primary duties.
3. Text messaging or use of the internet on a personal device, while not prohibited from use within the Communications Center, is strongly encouraged to occur during the employee's break/meal time or before or after work whenever possible. Employees should use their best judgement when texting and accessing the internet from personal devices within the Communications Center. Supervisors may exercise their discretion in addressing inappropriate use of texting and the internet.
4. Supervisors, Trainers, and the Emergency Communications Director reserve the right to remove an employee or their personal device from the Communications Center at any time in order to prevent distractions.
5. For security and privacy reasons, at no time is an employee allowed to take pictures or record audio or video from inside the Communications Center without the express permission of the Emergency Communications Director.
6. Laptops and tablets require prior permission from the Emergency Communications Director to be used inside the Communications Center.
7. There will be no cellular telephone calls with responding law enforcement units regarding the calls for service to which they are responding, including providing directions to the call. All telephone conversations with law enforcement units shall be conducted on recorded telephone lines.
8. Televisions inside of the Communications Center are to be on the Weather Channel or a news channel from 0630-1700 Monday-Friday when county offices are open or during tours of the Communications Center unless you receive prior permission from the Emergency Communications Director. Regardless of the time of day, the volume is to be kept at a low level so as not to interfere with operations.

APPENDIX D- Email Policy

Granville County Email Policy

Purpose

Granville County employees, elected officials, and volunteers rely on electronic mail (email) as a major communication tool to carry out government business. Most email messages have administrative, fiscal, legal, reference, and/or archival value. This policy ensures that records created, sent, and received through email are managed in accordance with established laws for creating, maintaining, and disposing of all government records. Following this policy will also help to ensure that email messages are available for public records requests. This policy and the mandates and guidelines within it are here to ensure effective management and retention of electronic messages.

Ownership of Email Messages

Any email messages created, received, and/or used on Granville County email systems are owned by Granville County. Employees of Granville County who use government equipment and systems should have no expectation of privacy.

Use of Personal Email Accounts

The use of personal email accounts to conduct official government business is strongly discouraged. If a personal email account is used for government business then employees, elected officials, and volunteers are required to forward all email messages to their government email account. It is very challenging to capture information from personal email accounts; due to legal requirements around public records and retention, government employees, elected officials, and volunteers that use personal email to conduct official business make it very difficult to comply with the law.

Elected officials and appointed members of committees must also abide by public record and open meeting laws. Members of governing boards who use personal accounts to conduct official government business should forward the email messages to the board's official record keeping entity so that proper and legal record keeping can take place.

It is the content of the email message and not the system or account used to create the email message that matters when it come to the legal framework involving public records and retention.

Volunteers Conducting Official County Business

Volunteers that conduct official Granville County business (any business related to their work as a volunteer with Granville County) should use official channels of communication with the public. Because Granville County emails are not guaranteed for volunteers, department heads should put measures in place to ensure that volunteers are not using personal email and messaging systems to conduct county business. While volunteer work that happens within Granville County departments is unpaid, it is still Granville County business, and therefore it is subject to laws such as public records and open meetings.

Emails as Public Records

An email message is public record when made or received pursuant to law or ordinance in connection with the transaction of public business by any department. North Carolina General Statutes 121-2(8) and 132-1(a) provide the following definition:

“Public record” or “public records” shall mean all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or

ordinance or in connection with the transaction of public business by an agency of North Carolina government or its subdivisions.”

Classifying Email Messages

Not every email message that enters or leaves the Granville County email system is a public record as defined by North Carolina General Statute (N.C.G.S.) 132. Some email messages may be public record but may also be considered confidential by statute and should be treated accordingly.

If an email message is not created or received as part of the business of government, it is considered to be non-record material. This includes personal messages, spam, and unsolicited emails.

Emails and Open Meeting Laws

The North Carolina Open Meetings Law provides the public with the right of access to the meetings of Granville County public bodies¹. A meeting of a public body is defined as a gathering of the majority of the members of a public body for the purpose of conducting Granville County business. Email exchanges could constitute a meeting of a public body. Therefore, elected officials and appointed members of public bodies should refrain from using electronic messaging as a meeting space for the majority of a public body to conduct Granville County business.

The North Carolina Open Meetings Law does not apply to professional staff of a public body.

Managing Retention and Disposition

Local governments are mandated by state law to manage and preserve records, including emails.²

¹ The North Carolina Open Meetings Law covers **public bodies**. The law defines a "public body" as any elected or appointed authority, board, commission, committee, council, or other body of the State, or of one or more counties, cities, school administrative units, constituent institutions of The University of North Carolina, or other political subdivisions or public corporations in the State that (i) is composed of two or more members and (ii) exercises or is authorized to exercise a legislative, policy-making, quasi-judicial, administrative, or advisory function.

² § 132-8.1. Records management program administered by Department of Natural and Cultural Resources; establishment of standards, procedures, etc.; surveys.

A records management program for the application of efficient and economical management methods to the creation, utilization, maintenance, retention, preservation, and disposal of official records shall be administered by the Department of Natural and Cultural Resources. It shall be the duty of that Department, in cooperation with and with the approval of the Department of Administration, to establish standards, procedures, and techniques for effective management of public records, to make continuing surveys of paper work operations, and to recommend improvements in current records management practices including the use of space, equipment, and supplies employed in creating, maintaining, and servicing records. It shall be the duty of the head of each State agency and the governing body of each county, municipality and other subdivision of government to cooperate with the Department of Natural and Cultural Resources in conducting surveys and to establish and maintain an active, continuing program for the economical and efficient management of the records of said agency, county, municipality, or other subdivision of government. (1961, c. 1041; 1973, c. 476, s. 48; 2015-241, s. 14.30(s).)

§ 132-8.2. Selection and preservation of records considered essential; making or designation of preservation duplicates; force and effect of duplicates or copies thereof.

In cooperation with the head of each State agency and the governing body of each county, municipality, and other subdivision of government, the Department of Natural and Cultural Resources shall establish and maintain a program for the selection and preservation of public records considered essential to the operation of government and to the protection of the rights and interests of persons, and, within the limitations of funds available for the purpose, shall make or cause to be made preservation duplicates or designate as preservation duplicates existing copies of such essential public records. Preservation duplicates shall be durable, accurate, complete and clear, and such duplicates made by a photographic, photostatic, microfilm, micro card, miniature photographic, or other process which accurately reproduces and forms a durable medium for so reproducing the original shall have the same force and effect for all purposes as the original record whether the original record is in existence or not. A transcript, exemplification, or certified copy of such preservation duplicate shall be deemed for all purposes to be a transcript, exemplification,

Backups

Granville County email system is backed up nightly. This backup includes all data stored within the email system (email messages, calendar, contacts, tasks, notes). Outlook settings, such as signatures and view settings, are stored on individual workstations and are not included in this nightly backup.

Access to Email Messages

Email messages are public records. All employees, elected officials, and volunteers must assume that all non-confidential information on government email systems is subject to public view. Confidential information is protected by the N.C.G.S. 132-1.2 or other applicable statutes. If email messages contain both confidential and non-confidential information and a public records request is received, an employee must provide access to the non-confidential information and redact the confidential information.

No employee should directly login to view another employee's email messages without proper notice and permission. Granville County strives to operate with transparency while also maintaining trust among its employees, elected officials, and volunteers. Department heads and supervisors should establish protocols for accessing emails of employees that will be out of the office for an extended amount of time.

Apart from vacation and extended leave protocols, supervisors of employees may submit a request to the County Manager to view an employee's email messages. All approved requests will be processed through the IT department. Apart from department heads, employees that wish to view another employee's emails must file a public records request. Any individual may request access to public records through procedures defined in N.C.G.S. 132-6 by application made to the legal custodian of the record as defined by N.C.G.S. 132-2 and 132-6.

Confidentiality

An email message having confidential information should not be shared unless proper, formalized security precautions have been established. This include confidential information covered by HIPAA (Health Insurance Portability and Accountability Act), information covered by FERPA (Family Educational and Rights to Privacy Act), social security numbers and other personal identifying information as defined in N.C.G.S. 132-1.10 and 14-113.20, and trade secrets as defined by N.C.G.S. 132-1.2.

Appropriate Use of Email Systems

The Granville County email system is provided to employees, elected officials, and volunteers to assist in carrying out government business. The Granville County provided email system should be used primarily to carry out government business. Inappropriate use of email messages can merit legal action. Inappropriate email messages can also result in negative reputation and publicity and lost productivity. Granville County staff, elected officials, and volunteers are discouraged from using Granville County email systems for anything other than official Granville County business.

After Hours Use of County Email Systems

Department heads will educate non-exempt employees on County email use in accordance with FLSA requirements.

or certified copy of the original record. Such preservation duplicates shall be preserved in the place and manner of safekeeping prescribed by the Department of Natural and Cultural Resources. (1961, c. 1041; 1973, c. 476, s. 48; 2015-241, s. 14.30(s).)

Standardized Versions of County Email Systems

Maintain at least the minimum version supported by Granville County email service. Access of outdated email clients may be revoked.

Password Security

Passwords are an important part of email security. Employees, elected officials, and volunteers should comply with the Granville County Password Policy located in the Technical Policies section of the Granville County Information Technology Policy.

Staff Departure

When a public employee, public official, or volunteer separates from Granville County, a hold will be placed on the mail account of the individual until the account and computer can be reviewed for record content.

The Human Resources department will notify the IT department within the next business day of departing employees that have submitted their notice or been terminated from Granville County.

Technical Security

The security of an email system is a shared responsibility. Individual users should take all reasonable precautions to prevent the use of their email by unauthorized individuals. Users must assess risk before sending confidential information over an open network.

Email security training should be completed for all users with a Granville County email address. Please see the following section on training.

Training New Employees, Elected Officials, and Volunteers

New employees, elected officials, and volunteers with Granville County email accounts must be trained on the Granville County email policy within 30 days of their start date. All new employees, elected officials, and volunteers with Granville County email accounts must sign a form documenting that they have received the appropriate training and agree to comply by the Granville County Email Policy.

APPENDIX E- Social Media Policy

Granville County Social Media Policy

Social Media Vision and Brand Consistency

Granville County Government uses social media as tool not only to broadcast information, but to actively engage our citizens, businesses, partners, and visitors in Granville County's daily activities and strategic objectives. Social media platforms are used to create a more efficient government, as well as to actively recruit talent to our county and partner strategically with other organizations. In using social media platforms, Granville County hopes to have a more fluid and informal method of communicating with stakeholders and to use social media to create trust and build a positive reputation with all stakeholders. In order to achieve all of these things, all staff, elected officials, and volunteers are expected to maintain a consistent agency and organizational identity established by Granville County Government.

Policy Purpose

Granville County officials, agents, employees, and volunteers use social media and networking sites as a means to communicate with stakeholders, media, employees, constituents, and visitors. Social media sites provide an avenue to disseminate timely information to the public and enables Granville County to receive feedback easily. This policy is designed to give direction on the rights and responsibilities for using these platforms, as well as a guideline for representing Granville County in the social media sphere. Social media is constantly evolving; therefore, this policy will evolve as needed.

Establishing Accounts

All proposed official (sanctioned by Granville County department heads and the County Manager) Granville County social media and networking sites are to be submitted for approval to the County Manager's Office. Requests submitted by staff to the County Manager will already have the department head's approval. Any Granville County social media and networking sites existing prior to this policy being adopted need to be reported to the County Manager's Office within 5 working days of this policy's adoption.

While departments are encouraged to develop departmental accounts specific to department needs, goals, and targeted audience, Granville County Administration will work simultaneously with departments and account administrators to ensure government-wide brand consistency is maintained and that the Social Media Policy is followed. The Public Information Officer will frequently check-in on department specific accounts. The Public Information Officer has the right to ask all social media account administrators to make adjustments to accounts and content as needed.

Before starting a social media account, departments should consider their capacity to adequately monitor these accounts. Accounts should be monitored, at a minimum, once a day. Frequent check-ins throughout the work day and even during non-office hours are encouraged. It is strongly encouraged that non-exempt employees are not responsible for administering social media accounts as they may need to make adjustments outside of scheduled work hours.

Administrative Roles

Department heads will update the Public Information Officer (Granville County Administration) on the names of the staff and/or volunteer administrators for official department social media accounts. Department heads will update the Public Information Officer on any changes in administrative roles for official Granville County social media accounts.

The Public Information Officer will act as an administrator on social media accounts for all departments as

a back-up plan for emergencies. The Public Information Officer will not take an active role in updating or editing content on a department's page outside of Administration. This measure is simply a back-up measure for emergencies.

When an administrator of a social media account leaves the department/Granville County Government, the department head must notify the Public Information Officer. Department heads will immediately change administrative access to the departmental account as soon as the social media account administrator departs.

All social media administrators will complete the appropriate annual training and sign and submit the Granville County's Social Media Policy Acknowledgement and Agreement Form (Appendix G).

It is strongly encouraged that all social media administrators use a device separate from their personal device to update social media accounts. This tactic will help ensure that administrators don't accidentally post to an official Granville County account from their personal account.

Passwords and IT Security

Security related to social media is largely a behavioral issue. Employees, elected officials, and volunteers are asked to minimize security risks via social media sites by following the Granville County Social Media Policy and all other rules and guidelines outlined in the Granville County Information Technology Policy.

Granville County social media account administrators are strongly encouraged to use the Granville County Password Policy for passwords tied to official social media accounts. This policy can be found in the Granville County Information Technology Policy.

Training

Granville County Administration will host a minimum of one social media staff training a year for all employees (in person, by video, or webinar). All new administrators and all content contributors (staff and volunteers) for official social media accounts will meet with the Granville County Public Information Officer and/or Management Analyst before administering any official accounts. Department heads are responsible for training volunteers on the Granville County Social Media Policy.

Legal Requirements

4.1 Social Media as Public Record

Granville County social media sites are considered public record under North Carolina General Statutes Section 132 and will be managed as such. Non-employees may not know that social media sites are public record. To assure that the public is aware of this, departments with social media sites should include language on their social media page that identify it as subject to public record laws.

G.S. § 132-1(a)

"Public record" or "public records" shall mean all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions.

Public records include anything created in the course of public business *regardless of format*. Content created on social media accounts is subject to public record law. Any record made or received in the transaction of public business is subject to public access unless an exception applies. Records created by government staff on personal devices or personal social media and personal email accounts are public records if the content involves public business.

The following statement should be included on all official Granville County social media accounts:

"Representatives of Granville County Government communicate via this account. Consequently, any communication via this account (whether by county employee or the general public) may be subject to monitoring and disclosure to third parties."

Granville County official accounts should regularly post this statement on their timeline.

Employees and volunteers receiving messages or comments from the public on personal social media accounts or in personal email that involves public business should refrain from replying other than to redirect messaging to an official government account or phone call. Elected officials are strongly encouraged to act consistently with County policy.

Social media content is subject to public record retention schedules. All official government accounts should be reported to the IT department for archiving and retention.

4.2 Content Retention

Retention schedules for social media may vary by department and/or topic. Content created by Granville County social media admins AND content created by the public on county social media accounts are subject to state retention schedules.

Department heads must notify IT of all account administrators so that the proper retention software may be applied to those account administrators.

4.3 Open Meetings

Elected officials and appointed board members are subject to the state's open meetings laws with the use of social media. A quorum of lawmakers holding a discussion about public business through social media may constitute a meeting that is subject to the open meetings law.

Operational Policies

5.1 Content Generation

Officials, agents, employees, and volunteers using Granville County social media and networking sites to communicate with citizens do so on behalf of Granville County. Therefore, administrators should use their professional judgement before posting or commenting, as content can be seen by anyone and may not be able to be recanted. A successful representation of Granville County will:

- Be honest and transparent.
- Post only within one's area of expertise
- Post only useful information
- Keep it professional - avoid confrontation
- Be accurate
- Correct errors, and if modifying an earlier post, identify the change
- Be responsive to citizen concerns
- Follow Granville County standardization guidelines listed below.

Employees are prohibited from posting the following on official Granville County sites:

- Information about actual or potential claims and litigation involving the government
- The intellectual property of others, without written permission; a successful representation of Granville County will utilize original content
- Photographs of members of the public without written permission (see the Photo Consent Form in Appendix H)
- Defamatory material
- Any personal, sensitive, or confidential information about anyone
- Obscene, pornographic, or other offensive/illegal materials or links
- Racist, sexist, and other disparaging language about a group of people
- Sexual comments about, or directed to, anyone
- Political campaign materials or comments
- Threatening or harassing comments
- Other information that is not public in nature.

While Granville County Government is supportive of our local businesses and non-profits, the county cannot operate as a message board or advertising outlet for all. Official Granville County Government accounts will refrain from promoting or endorsing any private business or non-profit organization without legitimate reasoning. Legitimate reasoning may include partnering with a specific business or organization in providing services to the county. Promotions and endorsements must be related to a county benefit. Official accounts are strongly discouraged from advertising for partner entities on events/activities/etc. that are not tied to County services.

When in doubt

When in doubt, social media administrators should check with their department head and/or the Public Information Officer before posting content, “liking” other pages, etc.

Official accounts should post regularly and at a minimum of at least once every two weeks. Departments that cannot maintain frequent contact with their social media accounts should not have accounts.

5.2 Photos, Videos, and Other Images

Any photographs or videos using identifiable images and/or small group shots of children under the age of 18 are strongly encouraged to use a photo release form and/or to get written permission to use the image of subjects under the age of 18.

Social media administrators and content generators should use original photos, videos, and images whenever possible. When original content cannot be created, administrators and content generators should obtain permission before using photos, videos, and images that do not belong to Granville County Government.

Permission form in Appendix H of the Granville County Information Technology Policy.

5.3 Public Commentary

While some departments may choose a strategic presence that is purely informational and non-transactional, a public forum strategy that allows commentary and engagement may be a more effective and desired strategy for some. The County Manager will leave this strategy to the professional judgement of the department heads with the understanding that engagement with the public will adhere to the guidelines.

Departments and their social media designee(s) will operate platforms in compliance with the Granville County comments policy.

All official Granville County social media accounts are considered a public forum transacting government business and therefore viewpoint discrimination is prohibited. Visitors leaving comments on official Granville County social media sites are protected by the First Amendment with a few exceptions. The comment moderation policy must be posted on each social media site.

5.3-A Comment Moderation Policy

Official Granville County social media and networking sites will post the following social media and networking comments policy:

- This site is moderated and comments are reviewed.
- Any communication on this site is considered public record.
- The appearance of external links or advertisements on this site does not constitute official endorsement.
- Please note that the public comments expressed on these sites do not reflect the opinions and position of Granville County government or its officers and employees. If you have any questions concerning our Social Media Comments Policy, please contact Granville County Government.
- Solicitations/advertisement are not allowed and will be removed from this site.
- Granville County reserves the right to delete unacceptable submissions by members of the public. We will remove comments that are or include:
 - Spam and Solicitations of Commerce: Comments focused on selling a product or service, or comments posted for a purpose of driving traffic to a particular website for personal, political, or monetary gain, will be excluded.
 - Personal Attacks: If you disagree with the content, we'd like to hear from you, but ask that you refrain from comments that attack others.
 - Illegal: Comments that suggest or encourage illegal activity are not allowed.
 - Offensive Language: Comments including, but not limited to, graphic, obscene, explicit, abusive, derogatory, or racial content will be excluded.
 - Content that promotes, fosters, or perpetrates discrimination on the basis of race, creed, color, age, religion, gender, marital status, physical ability, mental ability, marital status with regard to public assistance, national origin, sexual orientation.
 - Infringement on copyrights or trademarks

Private or Confidential Information: You participate at your own risk, taking personal responsibility for your comments, your username and any information provided. Please do not provide any specific personal information about yourself or other individuals.

5.3-B Responding to Public Commentary and Deletion Rules

Granville County social media account administrators may not remove or censor comments simply because they are critical of the department, staff, the government, etc. or because the administrator disagrees with the comments. Account administrators are allowed to delete comments that are in violation of the comment moderation policy.

If the social media administrator (s) finds a public comment in violation of the Social Media Comments Policy, the designee is to immediately remove the comment from the site. All comments should be archived with the IT archival program.

When in doubt

When in doubt, social media administrators should check with their department head and/or the Public Information Officer before posting or deleting comments.

5.4 Volunteer-Run Social Media Accounts

Department heads and/or their staff designee(s) will oversee volunteer programming and all volunteers that transact Granville County business. Social media content that is gained due to a volunteer's access to Granville County departments should be monitored by the department head.

5.4-A Volunteers and Official Social Media Accounts

Volunteers will not oversee official Granville County accounts. Volunteers may be used to assist in operating an official Granville County account. Any volunteers that are used to assist in operating official Granville County accounts must be approved by the department head and County Manager; the department head is responsible for monitoring official Granville County accounts and volunteers associated with those accounts at all times.

Volunteers assisting in transacting official Granville County business may not use personal social media accounts to conduct official Granville County business. The transaction of Granville County business via social media is subject to public record law and retention schedules.

Use of personal accounts does not ensure that IT staff can archive and retain public records related to official Granville County business. Volunteers receiving messages or comments from the public on personal social media accounts that involves official public business will refrain from replying other than to redirect messaging to an official government account.

5.4-B Volunteers and Unofficial Social Media Accounts

Official volunteers of Granville County departments that operate social media accounts related to Granville County departments will follow the policies and procedures outlined for volunteers. Official volunteers are expected to properly represent Granville County departments.

Official volunteers of Granville County departments that operate unofficial social media accounts related to Granville County departments are strongly encouraged to conduct these accounts in accordance with the Granville County Social Media Policy.

Social media content that is gained due to a volunteer's access to Granville County departments should be monitored by the department head.

Department heads may exercise discretion over volunteers that uses their work with Granville County to inform any unofficial social media account. Department heads retain the right to no longer use an individual as a volunteer based on misuse of information and inaccurate portrayals of a Granville County department.

Official volunteers of Granville County that establish non-official social media accounts must clearly state that they do not represent Granville County Government with the following statement "This account is not affiliated with Granville County Government. This account is an unofficial account and does not represent the views and actions of Granville County Government."

Official volunteers of Granville County that operate unofficial social media accounts must regularly post the state of non-representation (at a minimum rate of once per week), redirecting the public to official channels of communication.

5.5 Partner Organizations

Department heads are strongly encouraged to work with partner organizations to make sure their department is accurately represented in social media communications from partners. While department heads cannot dictate what organizations outside of Granville County Government say and do with their social media accounts, department heads can work to ensure that all partnerships with Granville County Government maintain the integrity and reputation of the county. Department heads that partner with outside organizations are encouraged to ask partners to share official county communications from official county social media accounts and/or the Granville County website.

5.6 Standardizing Accounts

An official Granville County social media is approved by the department head and the County Manager. An official account will display the any markings allowed by the platform to represent that account as official (for example, the grey check on Facebook).

Usage standards below apply to all social media and networking accounts:

- Display being the "official account"
- Display official county or department logo or program graphic
- Contain a link to official county website and post the Social Media Comments Policy (if applicable)
- Contain an official county email and/or contact number
- Review site daily for exploitation or misuse

5.7 Elected Officials

Elected officials who use the county's official social media are subject to the same requirements as employees. Elected officials are subject to the state's open meetings laws with the use of social media. A quorum of lawmakers holding a discussion about public business through social media may constitute a meeting that is subject to the open meetings law. Elected officials use of their own social media to communicate in their official capacity with members of the public can produce some risk. Discussion of public business, especially if it involves other elected officials, can be difficult to track and keep in accordance with open meeting laws.

Elected officials who use social media and networking for campaigning are highly encouraged to use a separate account for that purpose and not access social media through government technology and the use of government social media resources.

Elected officials are highly encouraged to include a link back to the county's official website for detailed information. Elected officials who use the same social media for communicating with constituents as they do to campaign risk violating the law against using government resources for political purposes.

5.8 Employee Use of Personal Accounts

All county employees, agents, and officers are asked to access their personal social media and networking accounts in a responsible and professional manner during office hours. Accessing personal accounts should not detract from workplace responsibilities and productivity.

Employees are strongly discouraged from using their personal accounts to conduct official Granville County business. The transaction of County business via social media is subject to public record law and retention schedules.

Use of personal accounts does not ensure that IT or any department can archive and retain public records. Conducting official County business from personal accounts risks confusing County residents and visitors as to the content that is public business and the content that is of a personal nature.

Employees should make every effort to refrain from using their personal accounts to transact County business related to their professional role. If an employee is contacted about government business via a personal account, employees should make every effort to redirect communication through an official Granville County channel.

Employees should refrain from creating original content on their personal accounts that directly relates to their job responsibilities and is meant to be received in a professional capacity.

Sharing content generated by an official Granville County account on one's personal page does not count as conducting official Granville County business.

When accessing personal accounts during and outside of office hours:

- Employees include in any post related to the government or their job on a personal or professional site a disclaimer that the posting reflects their own opinion, and not that of the government
- Policies that relate to conduct and ethics, privacy and confidentiality, harassment, retaliation and other relevant conduct apply
- Employees have no reasonable expectation of privacy when using government technology
- Employee use of personal social media at work must be brief, not interfere with performance of the employee's duties or with the workplace, and not involve commercial, political or other prohibited activities

5.9 Departmental Discretion of Personal Use

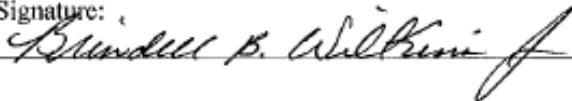
Department heads may implement a departmentally specific social media policy. These department specific policies must meet the Countywide policies at a minimum. Department specific policies must be approved by the County Manager and/or the respective departments' governing boards.

5.10 Violations

Violating the guidelines of this policy could jeopardize the integrity of the Granville County Government brand and work against the goals established in the county's vision for social media use. In some cases, a violation of elements outlined in this policy is a matter of legal concern. Violations of this social media policy will be brought to the attention of the department head and/or the County Manager.

APPENDIX F- Emergency Communications Social Networking Policy

Granville County Sheriff's Office Emergency Communications

Policy Number: 2019-002	Effective Date: 3-07-19
Policy: Social Networking	Revised Date: 3-06-19
Signature: 	Page 1 of 1

Purpose:

The safety and reputation of the Granville County Sheriff's Office and its employees are of the utmost importance in serving the citizens, responders, and visitors of Granville County. This policy outlines requirements for Emergency Communications employees accessing social media networks during work hours, as well as an employee guideline for posting on social media while serving as an employee of the Granville County Sheriff's Office Emergency Communications Center.

Policy:

1. During work hours **AND** when off-duty, employees are prohibited from posting, transmitting and/or disseminating any photographs, video images, audio files, text documents, logos, badges, emblems, uniforms or any other material on social media platforms that specifically identifies Granville County Sheriff's Office Emergency Communications. This includes, but is not limited to: Facebook, Twitter, Instagram, and Snapchat. If an employee wishes to post any content identifying the Granville County Sheriff's Office on any social networking site, that employee can only do so with written permission from the Sheriff or his/her designee.
2. While on duty, employees working console positions shall not post to any personal social media sites or generate any content for personal social media networking platforms.
3. Employees shall not access any social media site from Granville County computers within the Emergency Communications Center.
4. Employees are reminded that any and all information obtained in the course of their duties, whether directly or indirectly, is considered **confidential**. Employees are prohibited from posting any content to social media accounts that could interfere with or undermine the operation of the agency.

APPENDIX G- Social Media Policy Agreement

**Granville County Employee
Social Media Policy
Acknowledgement and Agreement**

Employee Name: _____ Employee ID: _____

Job Title: _____ Dept: _____

I have read, understand, and agree to comply with the Granville County Social Media Policy. I acknowledge that my cell phone account records may in certain circumstances be considered public records in accordance with NC General Statutes and may need to be turned over to the County upon request.

Employee's Signature

Date

APPENDIX H- Photo Consent Form



141 Williamsboro Street, PO Box 906
Oxford, NC 27565

PHOTO CONSENT FORM Granville County Government

Granville County Government often uses photographs, video and audio recordings of local residents and/or visitors to the area for informational purposes. These materials may appear in print or online. All use of such items will be for informational use only.

This form will allow you to give consent for your image to be used. For those under the age of 18, a parent and/or guardian can give consent by signing this form.

PLEASE CHOOSE ONE:

For anyone younger than 18 years old:

I give permission for Granville County Government to make photographs, videos or audio recordings of my child. Furthermore, I understand that I may not have the opportunity to inspect or approve the final product for its specific use before publication.

For anyone 18 years of age or older:

I give permission for Granville County Government to make photographs, videos or audio recordings of me. Furthermore, I understand that I may not have the opportunity to inspect or approve the final product for its specific use before publication.

Signature _____

Printed name _____

Name of minor child (if applies) _____ Age _____

City of Residence _____ State _____ Zip _____ Phone _____

Today's Date _____

APPENDIX I-Granville County Library System Acceptable Use Policy

Granville County Library System Acceptable Use Policy

Computer Use (Granville County Library System)

The Library provides personal computers so that employees may better perform their jobs. The PCs provided are to be used for Library or County business only. Internet surfing and email are allowed when assisting patrons or when performing job duties. In general, incidental and occasional personal use of the library's Internet access is permitted; however, personal use is prohibited if it:

- interferes with user's work performance, or with any other employee's work performance,
- adversely affects the efficient operation of the computer system or computer network,
- or violates any provision of this policy.

Employees should remember that, as the Library is an agency of Granville County government, it is possible that any document read or composed on employee computers may be considered public documents.

Internet homepages on employee computers should be set to the Granville County Library web page (www.granville.lib.nc.us) if the computer is visible to the public. Other computers may have Internet homepages set to other sites that are frequently used professionally –i.e., Library of Congress, Baker & Taylor, etc.

Staff PCs should not have homepages set to sites that are personal or entertainment (weather, local TV stations, etc.) Wallpaper may be individually set, but should generally be considered appropriate and may not reflect themes that are religious, political, or potentially controversial.

The Library has not monitored the use of software by its employees on PCs provided for staff use. However, some programs interact with others on the same PC after installation and can cause multiple problems. In these cases, it is not always possible to determine which programs are causing the problems. In order to maintain staff computers at an optimal level of performance, software on staff PCs will be strictly regulated. In addition, only certain employees will be designated to troubleshoot PCs when there are problems; non-employees are not authorized to troubleshoot unless called by the library staff.

It is strongly recommended that employees save important files on the shared (S) drive, which is backed up daily. Employees who elect to save files on their local hard drive are responsible for performing regular backups of their files. Employees are also responsible for periodically cleaning up their hard drives and clearing Internet history folders. Antivirus software is installed and maintained by the county IT Department.

Internet Use (Granville County Library System)

The Granville County Library System makes the Internet available as part of its continuing effort to provide collections, resources, and services that meet the cultural, informational, recreational and educational needs of Granville County's diverse, multicultural community.

Basic to our Policies are the Library Bill of Rights and The Freedom to Read Act. The Granville County Library System's Internet Use Policy affirms the following rights as outlined in the American Library Association's Library Bill of Rights and applied to electronic resources:

- Electronic information, services, and networks provided by libraries should be readily, equally, and equitably accessible to all library users.
- Libraries and librarians should not deny or limit access to information available via electronic resources because of its controversial content or because of personal beliefs or fears of confrontation.
- Information retrieved or utilized electronically should be considered constitutionally protected unless determined otherwise by a court with appropriate jurisdiction.
- Parent and legal guardians who are concerned about their children's use of electronic resources should provide guidance to their own children.

Because the Internet is a vast and unregulated information network, the Library's selection criteria and collection development policies cannot be applied to this resource. Information located on the Internet can be personally, professionally and culturally enriching but users are cautioned that some ideas are controversial, divergent and inflammatory. The Library makes no guarantees, implied or stated, about the accuracy or appropriateness of the information found on the Internet nor can it protect users from information and all images that they might find offensive or disturbing. Users are urged to be informed consumers by evaluating all information retrieved from the Internet.

All library users, regardless of age, background, or sensibilities, share the Library's access to the Internet. Users are asked to be sensitive of other's beliefs and values when accessing potentially controversial information. Users are also cautioned that security on the Internet cannot be guaranteed and that all transfers and files should be considered public.

Child Safety on the Internet (Granville County Library System)

Parents or legal guardians are responsible for the information accessed by their children on the Internet. Parents are encouraged to discuss the use of the Internet in relation to their family values and to provide guidance and boundaries for their children.

In addition, the Library adheres to the requirements of the Children's Internet Protection Act of 2000 that requires public and school libraries receiving specific federal and state funding for Internet access to use "technology that blocks Internet access to visual depictions that are - (A) obscene...; (B) child pornography ...; (C) harmful to minors ..." Parents and guardians should be aware that filtering technology is not 100% foolproof and is not a substitute for their guidance.

User Responsibilities (Granville County Library System)

All users of the Internet are expected to use this resource in a responsible and courteous manner, consistent with the purposes for which it is provided. Responsible and courteous use includes, but is not limited to, the following:

- Respecting the legal protection provided by copyright and license to programs and data.
- Respecting the computers and computer systems and not interfere with or disrupt network users, services, programs software or equipment.
- Refraining from using the Internet for illegal or unethical use.
- Respecting the privacy of others.
- Refraining from transmitting threatening, harassing or abusive language or images.

- Respecting the Library's Internet capabilities as public access and understanding that not all Internet sources are appropriate for public viewing by all ages.

Noncompliance may result in suspension or loss of privilege to use the Library's access to the Internet.

Tampering with the library's computers and other illegal activities violate library policy and state and/or federal laws. NC General Statute § 14-398.

Staff Assistance (Granville County Library System)

Staff assistance is available to provide limited instruction or, as time permits, to locate information for patrons. At this time, the Library cannot guarantee that a trained staff member will be available at all times for assistance. Staff can provide information about training sessions along with suggestions of books, magazines and other materials concerning the Internet.

Staff will not use patron media storage devices in staff computers. If a patron asks a staff member to access a patron media storage device for printing or any other service, staff will use a dedicated laptop to access the patron device.

Wireless Internet Access (Granville County Library System)

The Granville County Library System provides free wireless Internet access for users with wireless enabled laptops/notebooks or other wireless devices. This service is not to be used as a permanent connection. As it becomes feasible, printing from wireless connections will be added to the service.

Use of the wireless network is at your own risk and the Granville County Library will not be responsible for any information (i.e. credit card) that is compromised, or for any damage caused to your hardware or software due to electrical surges, security issues or consequences caused by viruses or hacking.

Library staff is not available to troubleshoot problems related to your wireless device or to assist in making changes to your device's network setting and/or hardware configuration.

Access to the wireless network may be limited due to lack of bandwidth during peak hours.

User Responsibilities (Granville County Library System)

By choosing to use this free wireless service you agree to abide by the Library's Internet Policy that prohibits abusive or illegal activity while using this service. This policy can be found in section 2(b) above.

All wireless access users should have up-to-date virus protection on their wireless devices.