Computer Usage Policy

Mission Statement: The Fontana Regional Library system (Library) provides the public of Jackson, Macon, and Swain counties with excellent service and convenient access to resources for their educational, informational, and recreational needs.

Purpose Statement: This document constitutes a Library-wide policy for the management of computer data networks and the resources they make available, as well as stand-alone computers that are owned and administered by the Library. The policy reflects the ethical principles of the Library and indicates, in general, what privileges and responsibilities are characteristic of the Library computing environment.

General Information: Computers and the Internet enable the Library to provide resources beyond its collection. They allow access to ideas, information and commentary from multiple and global sources. Access to electronic resources is provided free by the Library as part of its mission. The Library will provide access readily and equitably to users, regardless of race, age or socioeconomic status. The Library believes that the benefits to the community from this access far exceed any disadvantages. By its very nature, the Internet is an unregulated medium. As such, while it offers access to a wealth of material that is personally, professionally and culturally enriching to individuals of all ages, it also enables access to some materials that may be offensive, illegal or inaccurate. The Library cannot control access points which often change rapidly and unpredictably. This library fully complies with NC General Statute section §143-805: "Prohibit viewing of pornography on government networks and devices."

INTERNET SAFETY

The Library addresses the following Internet safety issues through its Acceptable Use Agreement, Parental Permission Form, and the use of technology protection measures on library computers:

- Access by minors to inappropriate matter on the Internet and World Wide Web;
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- Unauthorized access, including "hacking," and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and
- Measures designed to restrict minors' access to materials harmful to minors.

Technology Protection Measure: The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors as those terms are defined in Section 1703 of title 17, Children's

Internet Protection, United States Code, and based on the Supreme Court's June 2003 ruling that the filtering language in CIPA was, on its face, constitutional for public libraries. In accordance with the ruling, the library provides adults the ability to have unfiltered Internet access for "bonafide research" or "other lawful purpose" by submitting the library's "Request for Disabled Internet Filtering" form.

Cyber-bullying: It is unlawful for any person to use a computer or computer network to "cyberbully" in accordance with North Carolina statute 14-458.1 article 60 "Cyber-bullying". The term "cyber-bullying" means to do any of the following:

- With the intent to intimidate or torment a minor:
  - Build a fake profile or Web site;
  - Pose as a minor in:
    - An Internet chat room;
    - An electronic mail message; or
    - An instant message; ○ Follow a minor online or into an Internet chat room; or
  - Post or encourage others to post on the Internet private, personal, or sexual information pertaining to a minor.
- With the intent to intimidate or torment a minor or the minor's parent or guardian:
  - Post a real or doctored image of a minor on the Internet;
  - Access, alter, or erase any computer network, computer data, computer program, or computer software, including breaking into a password protected account or stealing or otherwise accessing passwords; or
  - Use a computer system for repeated, continuing, or sustained electronic communications, including electronic mail or other transmissions, to a minor.
- Make any statement, whether true or false, intending to immediately provoke, and that is likely to provoke, any third party to stalk or harass a minor.
- Copy and disseminate, or cause to be made, an unauthorized copy of any data pertaining to a minor for the purpose of intimidating or tormenting that minor (in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network).
- Sign up a minor for a pornographic Internet site with the intent to intimidate or torment the minor.
- Without authorization of the minor or the minor's parent or guardian, sign up a minor for electronic mailing lists or to receive junk electronic messages and instant messages, with the intent to intimidate or torment the minor.

Unfiltered Wireless Internet Access: Unfiltered wireless Internet access ~~is~~ can be provided for patrons who have their own hardware and software in compliance with the Children's Internet Protection Act (CIPA) in that, the Act specifies that a library must have a Technology Protection

Measure in place "with respect to *any* of *its* computers with Internet access [emphasis added]." In this regard, it is understood that CIPA's phrase "its computers" refers to a library's PCs, not patron-owned wireless devices.

CONFIDENTIALITY: The Library will treat data stored on computers as confidential (whether or not that information is protected by the computer operating system). Requests for disclosure of information will be honored only under one of the following conditions:

- When approved by the Regional Director;
- When authorized by the owners of the information;
- When required by local, state or federal law.

Computer users will receive notice of such disclosures when possible. (Viewing of information in the course of normal system maintenance does not constitute disclosure.)
Warning: Users of electronic mail systems should be aware that electronic mail in its present form cannot be secured and is, therefore, extremely vulnerable to unauthorized access and modification.

RESPONSIBILITIES OF USERS: Users of Library computing resources have the following responsibilities:

- Users must sign an Acceptable Use Agreement or an Application for Borrower's Card to use full access Internet stations;
- Users of full access Internet stations must use either their own current library card or their own current guest card issued by an NC Cardinal Library. To obtain a card, please refer to the Fontana Regional Library circulation policy;
- Users of mobile computers must have both a library or guest card issued by an NC Cardinal Library **and** a current government issued photo ID card. The photo ID is held by the library for the duration of the mobile computer(s) session;
- As the Library cannot control the content of material accessible electronically, individual users must accept responsibility for information accessed;
- Users are responsible for payment of printing fees incurred;
- Users should be aware of computer viruses and other destructive computer programs, and take steps to avoid being a victim or unwitting distributor of these processes;
- Computer accounts, passwords, library or guest cards, and other types of authorization that are assigned to individual users should not be shared with others;
- Ultimate responsibility for resolution of problems related to the invasion of the user's privacy or loss of data rests with the user. The Library assumes no liability for loss or damage to the user's data or for any damage or injury arising from invasion of the user's privacy.

Parents' and legal guardian's responsibility: Parents or legal guardians of minor children (under 16 years of age) are encouraged to provide guidance to their own children. Parents or legal guardians are solely responsible for their child's, and only their child's, use of the Library's electronic resources. Parents and legal guardians must grant permission for their minor children to use the Internet by signing the Fontana Regional Library Acceptable Use Agreement or the Application for Borrower's Card.

Legal use: The public and staff may only use computing resources for legal purposes. Examples of unacceptable purposes include, but are not limited to, the following:

- Harassment of others;
- Libeling or slandering others;
- Destruction of or damage to equipment, software, or data belonging to the Library or others;
- Disruption or unauthorized monitoring of electronic communications;
- Unauthorized copying of copyright-protected material;
- Using any computer for illegal or criminal purposes;
- Using any computer as a staging ground to "crack" or "hack" any computer system:
- Viewing pornography, as defined in North Carolina General Statutes section §143-805.

Ethical use: Computing resources should be used in accordance with the ethical standards of the Library. Examples of unacceptable use (some of which may also have legal consequences) include, but are not limited to, the following:

- Violation of computer system security;
- Unauthorized use of computer accounts or access codes;
- Use of computer communications facilities in ways that unnecessarily impede the computing activities of others (such as randomly initiating interactive electronic communications or email exchanges, overuse of interactive network utilities); •Violation of software license agreements;
- Violation of network usage policies and regulations;
- Violation of another user's privacy;
- Disruptive use of computers that might be detrimental to library service.

Library Responsibilities: The Library is responsible to provide reliable computer services in a safe and accessible environment. The Library will make a reasonable effort to:

- Provide staff assistance to users of Library computing resources;
- Accommodate users with special needs;
- Maintain Library computer equipment in good order;

- Resolve outside vendor problems in a timely manner;
- Partner with parents, teachers and other organizations to meet community needs;
- Administer and enforce this policy fairly and impartially.

Library Computers: The Library provides computers for the following activities at all locations:

- Internet Access, including full access and express stations, available with a signed agreement;
- Topic Specific Workstations with access to pre-selected Internet sites and related information on popular subjects;
- Educational and Recreational Games suitable for all ages;
- Microsoft Office applications (i.e., Microsoft Word, etc.) for enhanced productivity;
- Online access to the Library catalog;
- Technology training classes and workshops;
- Computer labs for training seminars, workshops and general computer use.

Patron computers and Wireless Devices: The Library provides unfiltered limited wireless Internet access at all locations, free of charge, for patrons who have the required hardware and software needed for this service:

- Access is on a first connect basis and controlled automatically by the Access Point;
- The owner is responsible for setting up their equipment to access the Library's wireless network;
- The Library does not assume responsibility for the safety of equipment or for configurations, security, or data files resulting from connection to the library's wireless service;
- Library staff may provide assistance in getting connected to the wireless network and other services. Library staff may assist patrons in configuring their own equipment.
- Library staff will not configure patrons' equipment, or accounts. Virus and security protection is the responsibility of the patron.

SANCTIONS. Violators of the Computer Usage Policy may lose Library privileges. Staff will be subject to normal disciplinary procedures as well. Violations of the Policy described above for legal and ethical use of computing resources will be dealt with in a serious and appropriate manner. Illegal acts involving Library computing resources may also be subject to prosecution by local, state or federal authorities.

DISCLAIMER. Since the Internet is a global electronic network, there is no state/county control of its users or content. The Internet and its available resources may contain material of a controversial nature. In accordance with current state and federal laws, library computers that connect to the Internet use a technology protection measure to filter and block access to images that are obscene, pornographic, or harmful to minors.

Internet filtering is used in order to comply with NC General Statute section §143-805, which prohibits viewing pornography on government networks and devices. Filters are not 100% effective and may not filter images that should be blocked, and conversely, may block images that should not be blocked. In the event a site is wrongly blocked, or conversely, not blocked, library users may request a review. Parents of minor children must assume responsibility for their children's use of the Internet through the Library's connection. Parents and children are encouraged to read Child Safety on the Information Highway, reprinted and distributed with permission of the National Center for Missing and Exploited Children.

Library staff cannot control the availability of information links which often change rapidly and unpredictably. Not all sources on the Internet provide accurate, complete or current information. Users need to be adept information consumers, questioning the validity of the information.

The Fontana Regional Library assumes no responsibility for any damages, direct or indirect, arising from the use of its website or other services.

Computer Usage Policy

Knowledge At Your Finger Tips
Fontana Regional Library®

This policy is based on and is consistent with the *Library Bill of Rights*, *Access to Electronic Information, Services, and Networks: An Interpretation of the Library Bill of Rights*, and the *Children's Internet Protection Act*.

Time Limits. Computer use is limited to one hour per session unless no one is waiting, and two sessions per day to maximize availability of Library computers for all users.

Accessing Library Computers. Users can access library computers by signing-in at the Information Desk, PC Reservation Station, or an available computer.

Users of full access Internet stations must use either their own current library card or their own current guest card issued by an NC Cardinal Library.

Users of the Library's mobile computers must have both a library or guest card issued by an NC Cardinal Library and a current government-issued photo ID card. The Library will hold the photo ID for the duration of the mobile computer(s) session. Users may make appointments in person or on the phone for hour-long sessions.

Printing. The Library charges patrons $.25 per side for printing. Patrons should use the Print Preview feature to view before printing any documents.

Saving Files. Save your work on removable media, not the hard drive. Removable media may be available for purchase at the information desk.

Computer Use. Do not use any software program other than those that the Library has installed.

Minors under 16 years of age who use full access Internet must have their parent's or legal guardian's signature granting permission on the Fontana Regional Library Application for Borrower's Card or the Fontana Regional Library Acceptable Use Agreement.

Help. Library staff are available to assist patrons, if requested.

AGREEMENT

I agree to comply with the stated rules of the Computer Usage Policy.

Applicant's Name (please print):_____ Phone #: _____ Guest [ ]

Applicant's Signature: _____ Date: _____ FRL Staff

Initials: _____

Parents are required to provide the following information for Applicants below 16 years old:

❑ I give my child permission to use the Internet at the Library

❑ I do NOT give my child permission to use the Internet

Applicant's birth date (day/month/year): _____

Parent's Signature: _____

ADDENDUM A

Additional Responsibilities for Fontana Regional Library Staff Users

- This information applies to Fontana Regional Library computer systems and refers to hardware, data, software, and communications networks associated with these computers. In particular, this information covers computers ranging from multi-user time sharing systems to single user personal computers, whether stand-alone or connected to the network.

- To be an authorized user of Fontana Regional Library (Fontana Regional Library) computer and network resources, you must be a volunteer, part-time or full-time employee with Fontana Regional Library.

- As an authorized user, you are responsible for the security and use of your computer accounts.

- You accept full responsibility for your accounts and all activity performed on Fontana Regional Library computing resources. You are responsible for preventing unauthorized use of Fontana Regional Library computer account(s) as well as refraining from using someone else's accounts.

- As a user of computers provided by a public agency, you agree to comply with North Carolina General Statute section 143-805, which prohibits viewing of pornography on government networks and devices.

- Fontana Regional Library STAFF workstations are configured differently from PUBLIC workstations. This allows various library-required applications installed on staff workstations to have greater control of system resources with lower levels of security to meet the needs to conduct business. To ensure the Fontana Regional Library computer systems, computer networks, as well as the data they store and process, are operated and maintained in a secure environment and in a responsible manner, the following guidelines are provided for STAFF workstations:

    - Users may not change, copy, delete, read or otherwise access files or software owned by other parties without permission of the custodian of the files or Librarian or IT Officer.
    - Users may not bypass accounting or security mechanisms to circumvent data protection schemes. It is the user's responsibility to report a potential security problem to IT Services immediately and should not be discussed with any other party. It is IT Services' responsibility to notify the appropriate parties and supervisor or Librarian.
    - Users may not attempt to modify software except when intended to be user customized.

- Staff should back up their data on a daily basis, then store the backed up data. FRL provides back-up storage (not working space) on a secure server with limited space. Although the server data is backed-up daily, IT Services cannot guarantee the data can or will be recovered in the event of a power failure, or catastrophic event. The recommended backup for your data should be a storage device, such as a UFD, zip drive, or rewritable CD-ROM and stored in-place, such as a locked drawer.
- All networking equipment connected to the Fontana Regional Library network must first be approved by the Librarian and registered with IT Services. This applies to all networked devices, ranging from multi-user systems to single user personal computers. This includes, but not limited to, networked printers, mini-hubs, routers, switches, and any other network communication devices.
- Any networked devices or services that are detected and verified to degrade the quality of service on the network, if not corrected by the user, will result in termination of network service of that device until the cause of the problem is corrected.
- Using computing resources to interfere with the normal operation of Fontana Regional Library computing systems and connected networks including, but not limited to, downloading or transferring excessively large files, or unfairly monopolizing resources that results in the exclusion of others in such a way that it causes disruption in the operation of the library or exploits network security and/or other vulnerabilities is prohibited.
- Intentionally causing any damage to any equipment is prohibited.

Additional Legal and Ethical Use for Staff Users

- Unauthorized copying, sending, or receiving of copyrighted or trade/service marked materials is strictly prohibited.
- Users shall assume that any software they did not create is copyrighted. They may neither distribute copyrighted proprietary material without the written consent of the copyright holder nor violate copyright or patent laws concerning computer software, documentation or other tangible assets.
- Fontana Regional Library computing resources are prohibited from copying audio and video library material, in whole or part without the written consent of the copyright holder and is signed and dated by the supervisor.
- Staff will not use Fontana Regional Library computing resources for private business purposes unrelated to the mission of the Library.
- Personal use of Library computing resources must be approved by the appropriate Librarian with the following guidelines in effect:

- Personal use will be on an employee's personal time.
- It will not interfere with any work-related activity.
- The person will supply their own expendable materials.
- The use of computer games for personal interest is not permitted on library time.

- Do NOT install software unnecessary to the operation of the library such as:
  - Peer-to-peer (P2P) file sharing software~~. (e.g., FrostWire, gnutella, BearShare, Grokster, Morpheus, Napster, LimeWire, BitTorrent, Skype, etc.).~~ Many forms of malware target P2P users exclusively.
  - Instant messaging software (~~AOL, Yahoo, etc.)~~ and chat software. Many forms of malware are designed to spread using these inherently unsecured channels, which do not have the antivirus protection of a proper email system.
  - Add-on browser toolbars
  - Aftermarket screen savers (especially those that automatically download pictures from the Internet)
  - Weather-monitoring software
  - News-monitoring software
  - Stock market-monitoring software
  - Non-Microsoft media players (e.g., VLC, Winamp)
  - Aftermarket browser toolbars
  - Aftermarket desktop search engines capable of sharing your data with other computers
  - Alternative email clients
  - Web server software
  - Shopping or coupon software (e.g., Claria, formerly named Gator)
  - Password-caching software (stores your user IDs/passwords at a remote location)
  - Online gambling software
  - Remote control or remote access software.

- The Library encourages staff to use email for job-related communication and professional development. Use of email for personal interest is not permitted on library time. Please refer to Addendum B of this policy.
- The role of technology in the 21st century workplace is constantly expanding and includes social media communication tools that facilitate interactive information sharing, interoperability, and collaboration. Social media websites have large, loyal user bases and increasingly important outreach and communication tools for libraries. Examples of social media include Facebook©, ~~Twitter~~ X©, ~~MySpace~~™, YouTube©, Flickr®, WordPress©, LinkedIn®, etc.

- Social networking improves interactivity between the library and the public, and it reaches populations that do not consume traditional media as frequently as others do. However, users should take care to choose the types of social networks that make the most sense for their type of information and that give emphasis to tools that provide more information across multiple outlets to the broadest audience.
- Staff members using social media need to strike a balance between providing access to information and protecting data on the library's internal network. To find that balance we need to assess the risk. Addendum C of this policy is meant to help the staff understand these risks and outline some best practices for social media usage. The library has adopted these tools and encourages the staff to use them productively and intelligently.

ADDENDUM B.

Account Requirements

- As soon as an applicant informs the Library that they will accept a position of employment with Fontana Regional Library, the Librarian should notify IT Services via email with the following information:
  - The person's full legal name
  - Employment position
  - First day of Fontana Regional Library employment
  - Name of the dedicated workstation where this person will normally work

Terms of Use

- If a staff member's job responsibilities change and the use of email is no longer required, the account must be terminated. The Librarian will notify IT Services promptly of any employment changes that render the account holder ineligible.

- The Librarian of a terminated employee will notify IT Services of the separation on or before the employee's termination date so that account access can be revoked appropriately. The Librarian will notify IT Services by email or by telephone at and provide the employee's name.

- Fontana Regional Library staff using Fontana Regional Library email must recognize certain risks associated with doing business electronically, and failure to consider such issues can lead to misuse of email or its improper management and expose Fontana Regional Library to unnecessary legal risk (North Carolina Department of Cultural Resources, "*E-mail as a Public Record in North Carolina: Guidelines for Its Retention and Disposition".* Raleigh: Office of Archives and History, 2002.):
  - Email systems and the media on which messages are stored can be insecure;
  - Email in transmission is no more private than a postcard;
  - Standard customs exist that establish proper language and tone of email messages;
  - Email often is used informally but may be interpreted as formal communication;
  - Email is not a proper method for discussing confidential matters, such as personnel issues, unless encrypted;
  - Email message can be forwarded to individuals not intended to read them.

- Email is Library-owned and a public record when it is used to transact public business. Any information created on equipment owned or operated by Fontana Regional Library, is Library property.

- Users have a responsibility to make sure that all public information disseminated is accurate. Users shall provide in
  association with such information the date at which it was current and an email address allowing the recipient to contact the staff responsible for making the information available in its current form.

- All email messages must contain the name of the sender, email address, job title, and library contact information, commonly referred to as the signature block. When sending or forwarding email users shall identify themselves clearly and accurately. Anonymous or pseudonymous posting is expressly forbidden.

- Users will not misrepresent the policies or positions of their library in email. Staff members will ensure that their emails hall contain the following disclaimer in their signature block:

  "Opinions expressed in this message may not represent the policy of my agency. All email sent to or from the Fontana Regional Library e-mail systems is subject to monitoring and disclosure to third parties, including law enforcement personnel."

- Fontana Regional Library staff should scan any email attachment for viruses. Save the file to your computer's hard drive and scan it for viruses.

- Fontana Regional Library staff should not send or forward any unsolicited commercial advertising and any other type of mass mailing which meets both conditions:
  - Does not pertain to library business and;
  - Results in network spamming, which is strictly forbidden.

- Users shall not stalk others, post, transmit, or originate any unlawful, threatening, abusive, fraudulent, hateful, defamatory, obscene, or pornographic communication, or any communication where the message, or its transmission or distribution, would constitute a criminal offense, give rise to civil liability, or otherwise violate any applicable law.

ADDENDUM C.

North Carolina Department of Cultural Resources

Best Practices for Local Government Social Media Usage in North Carolina

April 2010

1. PURPOSE

The role of technology in the 21st century workplace is constantly expanding and now includes social media communication tools that facilitate interactive information sharing, interoperability, and collaboration. Commonly used social media websites, such as Facebook©, Twitter©, MySpace™, YouTube©, Flickr®, Blogger, and LinkedIn®, have large, loyal user bases and are, thus, increasingly useful outreach and communication tools for government entities from the federal to the local level. Moreover, a social networking presence has become a hallmark of a vibrant and transparent communications strategy. Social networking improves interactivity between a local government and the public, and it reaches populations that do not consume traditional media as frequently as others do. Therefore, local governments should consider using social networking websites to enhance their communications strategies. In doing so, however, local governments should take care to choose the types of social networks that make the most sense for their type of information and that give emphasis to tools that provide more information across multiple outlets to the broadest audience. All government communication tools should be used in ways that maximize transparency, maintain the security of the network, and are appropriately professional. Social media is no exception. Therefore, the application of social media in local government must be done thoughtfully and in a manner that minimizes risk. In addition, social media users should be aware that these types of communications are considered public records and, consequently, must be kept for a certain period of time in compliance with the public records law. These guidelines are intended to ensure that local governments' social networking sites[1] are secure and appropriately used and managed by outlining "best practices" for the use of social media. Thus, the suggestions provided in this document are

designed to protect government employees and ensure consistency across entities when incorporating social media into their mission.

RECOMMENDATIONS

1.1 IMPLEMENTATION

Every government should have a clear communications strategy and should take the time to determine how social media fits into this strategy. The following questions should be considered when determining whether use of social media is appropriate:

- Who is the media meant to reach? Is this my target audience?
- What is the organization attempting to communicate? Can it be effectively communicated using this media?
- Who is responsible for managing the organization's account? Will this person represent the organization appropriately? Has he or she been properly trained in the use of social media?
- What are the organization's responsibilities regarding collection and records retention including preservation of social media content? What does the records retention schedule require for these records?

When a local government decides to use a form of social media that is deemed beneficial to its mission it should first set up boundaries for using the service. It is recommended that an account administrator is assigned to spearhead the use of social media within the workplace. Account administrators and other potential users are encouraged to complete online training for social media in tutorial form on the North Carolina Department of Cultural Resources website, NCDCR Records Management.

Account administrators are encouraged to create internal policies that keep track of social media domain names in use and the associated user identifications and passwords currently active. Should the employee who administers the account be removed as administrator or no longer be employed by the organization, all passwords and account information should be immediately changed to maintain organization control.

1.2 ACCEPTABLE USE

All use of social networking sites by local governments should be consistent with applicable state, federal, and local laws, regulations, and policies including all information technology security policies. This includes any applicable records retention and disposition schedules or policies, procedures, standards, or guidelines promulgated by the Department of Cultural Resources. All

usage should be governed by these policies as well as the recommendations in this document and future internal policies.
Following are specific recommendations for acceptable use of social media sites:

Separate Personal and Professional Accounts:
Employees should be mindful of blurring their personal and professional lives when administering social media sites.

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

Professional Use:
All government-related communication through social media outlets should remain professional in nature and should always be conducted in accordance with the organization's communications policy, practices, and expectations. Employees must not use social networking sites for political purposes, to conduct private commercial transactions, or to engage in private business activities. Employees should be mindful that inappropriate usage of social media can be grounds for disciplinary action. If an account is used for business, the entire account, regardless of any personal views, is subject to these best practices guidelines and the records retention schedule, including the collection and preservation provisions.

Be Clear As To Identity:
When creating social media accounts that require individual identification, government employees should use their actual name, not pseudonyms. However, using actual names can come with some risks. Any employee using his or her name as part of a local government's application of social media should be mindful of the following:

- Do not assume privacy. Only post information that you are comfortable disclosing.
- Use different passwords for different accounts (both social media and existing work accounts). Using the same password for all accounts increases the vulnerability of the accounts being compromised.

Terms of Service:
Employees should be aware of the Terms of Service (TOS) of the particular form of media. Each form of social media has its own unique TOS that regulate how users interact using that particular form of media. Any employee using a form of social media on behalf of a local government agency should consult the most current TOS in order to avoid violations. If the TOS contradict organization policy then a decision should be made about whether use of such media is appropriate.

Content of Posts and Comments:
Employees using social media to communicate on behalf of a local government should be mindful that any statements made are on behalf of the organization; therefore, employees should use discretion before posting or commenting. Once these comments or posts are made they can be seen by anyone and may not be able to be "taken back." Consequently, communication should include no form of profanity, obscenity, or copyright violations. Likewise, confidential or non-public information should not be shared. Employees should always consider whether it is appropriate to post an opinion, commit oneself or one's organization to a course of action, or discuss areas outside of one's expertise. If there is any question or hesitation regarding the content of a potential comment or post, it is better not to post. There should be great care given to screening any social media communication made on behalf of the organization as improper posting and use of social media tools can result in disciplinary action.

Posts and Comments Are Public Records:
Like email, communication via government-related social networking websites is a public record. This means that both the posts of the employee administrator and any feedback by other employees or non-employees, including citizens, will become part of the public record. Because others might not be aware of the public records law, local governments should include the following statement (or some version of it) somewhere on the social networking website:

> *Representatives of [insert specific local government] communicate via this website. Consequently, any communication via this site (whether by a government employee or the general public) may be subject to monitoring and disclosure to third parties.*

1.3 SECURITY

From a security standpoint, local governments should be mindful of how to best prevent fraud or unauthorized access to either the social media site or the government network. In almost every case where an attacker accesses a system without authorization, they do so with the intent to cause harm. The harm intended may be mild or more serious.

Thus, security is an ever-present concern that must be addressed. If participating in social media, local governments should:

- Ensure that employees are made aware of which information to share, with whom they can share it, and what not to share.
- Provide security awareness and training to educate users about the risks of information disclosure when using social media, and make them aware of various attack mechanisms.
- Ensure that employees are aware of the Privacy Act of 1974 requirements and restrictions. Educate users about social networking usage policies and privacy controls to help them better control their own privacy in any profile they use for work-related activities and more effectively protect against inadvertent disclosure of sensitive government information.

1.4 RECORDS MANAGEMENT AND PRESERVATION

Communication through local government-related social media is considered a public record under NC G.S. 132 and will be managed as such.

- All comments or posts made to local government account walls or pages are public, not private.
- Account administrators who receive messages through the private message service offered by some social media sites should encourage users to contact them at a public email address maintained by their organization. For private messages that account administrators do receive, they should be treated as constituent emails and therefore, as public records. Account administrators or other authorized staff members should reply using their government email account.

- Local governments should set all privacy settings to public.

Local governments must assume responsibility for public records and comply with the retention period set forth in their approved retention and disposition schedule. Local governments must assign their own schedule of collection and disposal for social networking Web sites according to the administrative value of the record and permanently retain records with historical value. Refer to Web Site Guidelines policies on the North Carolina Government Records website, North Carolina Department of Cultural Resources Records Management.

CONCLUSION

Social media is an effective and efficient way for local governments to communicate with and participate in the larger community. It will continue to shape and support the way they communicate and collaborate with constituents as they strive to provide an accountable and

transparent government. As local governments use social media they need to strike a balance between providing access to information and securing their government's core network. This document is meant to help local governments understand these risks and outline some best practices for social media usage.

Library Bill of Rights

The American Library Association affirms that all libraries are forums for information and ideas, and that the following basic policies should guide their services.

I. Books and other library resources should be provided for the interest, information, and enlightenment of all people o because of the origin, background, or views of those contributing to their creation.

II. Libraries should provide materials and information presenting all points of view on current and historical issues. Materials should not be proscribed or removed because of partisan or doctrinal disapproval.

III. Libraries should challenge censorship in the fulfillment of their responsibility to provide information and enlightenment.

IV. Libraries should cooperate with all persons and groups concerned with resisting abridgment of free expression and free access to ideas.

V. A person's right to use a library should not be denied or abridged because of origin, age, background, or views.

VI. Libraries which make exhibit spaces and meeting rooms available to the public they serve should make such facilities available on an equitable basis, regardless of the beliefs or affiliations of individuals or groups requesting their use.

Adopted June 18, 1948.
Amended February 2, 1961, and January 23, 1980, inclusion of "age" reaffirmed January 23, 1996, by the ALA Council.

Knowledge At Your Finger Tips
Fontana Regional Library®

Library Bill of Rights

Access to Electronic Information, Services, and Networks: an Interpretation of the LIBRARY BILL OF RIGHTS

Introduction: The world is in the midst of an electronic communications revolution. Based on its constitutional, ethical, and historical heritage, American librarianship is uniquely positioned to address the broad range of information issues being raised in this revolution. In particular, librarians address intellectual freedom from a strong ethical base and an abiding commitment to the preservation of the individual's rights.

Freedom of expression is an inalienable human right and the foundation for self-government. Freedom of expression encompasses the freedom of speech and the corollary right to receive information. These rights extend to minors as well as adults. Libraries and librarians exist to facilitate the exercise of these rights by selecting, producing, providing access to, identifying, retrieving, organizing, providing instruction in the use of, and preserving recorded expression regardless of the format or technology.

The American Library Association expresses these basic principles of librarianship in its *Code of Ethics* and in the *Library Bill of Rights* and its Interpretations. These serve to guide librarians and library governing bodies in addressing issues of intellectual freedom that arise when the library provides access to electronic information, services, and networks.

Issues arising from the still-developing technology of computer-mediated information generation, distribution, and retrieval need to be approached and regularly reviewed from a context of constitutional principles and ALA policies so that fundamental and traditional tenets of librarianship are not swept away.

Electronic information flows across boundaries and barriers despite attempts by individuals, governments, and private entities to channel or control it. Even so, many people, for reasons of technology, infrastructure, or socio-economic status do not have access to electronic information. In making decisions about how to offer access to electronic information, each library should consider its mission, goals, objectives, cooperative agreements, and the needs of the entire community it serves.

The Rights of Users: All library system and network policies, procedures or regulations relating to electronic resources and services should be scrutinized for potential violation of user rights. User policies should be developed according to the policies and guidelines established by the American Library Association, including Guidelines for the Development and Implementation of Policies, Regulations and Procedures Affecting Access to Library Materials, Services and Facilities.