# IREDELL COUNTY
## USE OF INFORMATION TECHNOLOGY RESOURCES POLICY
## Revised January 1, 2012

### 1.1 Scope and Ownership

This policy applies to all Iredell County technology systems (hardware, software, data networks, user accounts, and associated processes/services) owned, leased, or otherwise operated by Iredell County. The scope of the policy also includes all personnel who have access to Iredell County systems (employed by the County or not).

Systems containing Iredell County data which are hosted by third parties outside of the Iredell County network, and the personnel with access to those systems are also subject to this policy.

All technology resources defined in this section, along with all information transmitted by, received from, and stored upon said systems are considered to be possessed by, and/or the property of Iredell County.

### 1.2 Policy violation

When a policy violation occurs, aside from disciplinary action, system access may be revoked in whole or in part if deemed to be in the interest of Iredell County system security and/or availability.

### 1.3 Personal Use

Iredell County systems are intended for business use. Any personal use must comply with the following:

- must not violate applicable laws or regulations
- must not violate contractual agreements or intellectual property rights
- must not violate Iredell County personnel policies
- must not incur security risk to the County
- must not incur any additional cost to the County
- must not interfere with work duties
- must not be used for personal gain
- must not be used for solicitation

### 1.4 Monitoring and Privacy

Iredell County has the right to monitor, audit, and/or inspect any and all aspects of the County's electronic technology resources without advance notice to any users. Failure to monitor in any specific situation does not constitute a waiver of the County's right to monitor.

Personnel within scope of this policy are advised that they have no privacy rights and that there is no reasonable expectation of privacy when using County systems.

#### 1.4.1 Monitoring, Auditing, and Inspection Activities

At the written request of a department director for one of their respective employees, or upon authorization by the County Manager or Human Resources Director, the Chief Information Officer or designee has the authority to monitor and/or inspect any Iredell County system without notice to users.

For security and network maintenance purposes, authorized individuals within Iredell County's Information Technology Department may monitor equipment, systems, data and network traffic at any time.

### 1.4.2 Privacy expectations

Iredell County does not guarantee the confidentiality of user information stored on any network, computer, or communications device belonging to Iredell County.

Iredell County's users should be aware that the data they create on County technology or communications systems remains the property of Iredell County and is not private (unless the data is protected by privacy or confidentiality laws).

Information that is stored on or transmitted to or from County systems may be subject to disclosure pursuant to the North Carolina Public Records Law.

## 1.5 Security

Iredell County system security must be maintained at all times. Users must take all reasonable precautions, including but not limited to: safeguarding passwords, maintaining reasonable physical security around Iredell County equipment, and locking or logging off unattended workstations.

A user who is actively logged on to a Iredell County system is responsible for any activity that occurs whether or not they are present.

### 1.5.1 Administrative Privileges

For security reasons, administrator-level network, server, and PC access, is limited to Information Technology support staff and/or their designees. Administrator privileges will not be extended to users in order for software to operate. Software vendors are responsible for providing software that will operate without administrator privileges.

### 1.5.2 Passwords and User System Access

The Iredell County Information Technology Department is responsible for creation, assignment, and deletion of all user accounts for Iredell County systems. The level of access to the network, servers, applications, and personal computers will be administered by the Information Technology Department based upon the job tasks for the individual user.

Users are responsible for protecting their passwords and access to assigned accounts (network, systems, applications, etc.) at all times.

PASSWORD AND ACCOUNT DO'S

- Passwords must be changed at least every 90 days.
- Create strong passwords (greater than eight characters, mixed case, mix letters numbers and symbols, use long phrases when possible).
- Log off unused systems, and/or utilize password protected screen savers.
- Compromised passwords/accounts must be reported to the Information Technology Department.
- Refer anyone who asks for your password to this policy.

PASSWORD AND ACCOUNT DON'TS

- Do not use weak passwords (simple words, names, personal dates, all alpha, all same case, predictable patterns, e.g. 12345, zyxw, asdf, etc.).
- Do not give your password to anyone verbally, or electronically, for any reason. Your password belongs to you, and only you.
- Do not use personal, non-County system passwords (e.g. home email, home Internet, eBay, etc.) as passwords for County systems.
- When possible, do not reuse the same password for multiple systems.
- Do not store written passwords in any area accessible by others.

- Do not store passwords electronically unless they are encrypted and inaccessible to others.

### 1.5.3 Physical Security

Shared Iredell County systems (network, servers, systems, etc.) will be physically secured by the Information Technology Department.

- Access to the server room, disaster recovery site, network switches, and other key infrastructure is limited by lock with access granted to authorized personnel only.
- Media, such as daily and monthly backups, will be stored in a secure area with access granted to authorized personnel only.

Users are responsible for the physical security of assigned technology resources.

- To the degree possible, technology resources should be protected from theft and/or vandalism, fire and other natural environmental hazards.
- Laptops, cell phones, etc. in vehicles must be stored in the trunk or otherwise out of sight. They may never be left in a vehicle overnight.
- Employees should exercise precautions to make sure that their computer hardware is not exposed to dangers related to their specific use, i.e. accidental beverage spills, improper ventilation of air intakes, etc.

### 1.5.4 Application Security Standards

All software applications which manage sensitive or confidential data, whether acquired from a third party or developed internally must adhere to the following security requirements:

- Must support authentication of individual users.
- Must not store or transmit user credentials in a clear text or easily reversible form.
- Must support application scope restriction based on user levels.
- Must support user tracking for critical transaction activity.

### 1.5.5 Third Party Access to Iredell County Systems

No third party may be allowed access to Iredell County systems without written approval from the Information Technology Department.

### 1.5.6 Reporting Violations

Every department should have procedures in place to monitor compliance with the technology use policies within this document, and to report violations (both by "insiders" such as employees and contractors and "outsiders" such as unauthorized visitors, trespassers and hackers).

It is the responsibility of each technology user to remain diligent in the identification and reporting of technology policy violations. Staff should be aware of their environment and report any suspicious, abnormal or unnatural behavior or events to his or her supervisor and the Information Technology Department.

## 1.6 Prohibited Use

The following is a list of examples of prohibited uses. This is not intended to be a comprehensive and complete list. Other uses not listed here may be deemed as prohibited.

- Any use that violates federal, state, or local law or regulation is expressly prohibited.
- Knowingly or recklessly interfering with the normal operation of computers, peripherals, or networks is prohibited.

- Connecting unauthorized equipment to the network for any purpose is prohibited.
- Running or installing unauthorized software on Iredell County computers is prohibited.
- Copying of any software from Iredell County computers, for other than archiving purposes, is prohibited.
- Using Iredell County network to gain unauthorized access to any computer system is prohibited.
- The use of Iredell County Systems to access, transmit, store, display, or request obscene, pornographic, erotic, profane, racist, sexist, libelous, or other offensive or abusive material (including messages, images, video, or sound) is prohibited.
- The use of Iredell County Systems in such a way as to create an intimidating or hostile work environment is prohibited.
- Iredell County Systems may not be used to solicit for personal gain or for the advancement of a political or religious belief.
- Employees may not use social networking sites on county equipment unless approved by the County Manager.

### 1.7 Remote Access

Remote access to Iredell County systems (access to Iredell County systems from external systems, e.g. via the Internet) consumes technology resources above and beyond those required for local access. The Information Technology Department will review requests and grant remote access based upon business cases and resources available.

Remote access users are subject to all policies herein.

Additional security requirements may be established for remote access systems by the Information Technology Department.

### 1.8 Hardware/Software Standards, Procurement, and Installation

The Iredell County Information Technology Department has the sole responsibility for establishing standards, procuring, maintaining inventory, and installing technology required for County operations. Information Technology is also responsible for engaging and managing relationships with technology vendors.

Employees outside of Information Technology are prohibited from procuring, and installing hardware or software for or on Iredell County systems.

All software installation media must be stored by Information Technology.

### 1.9 Technology Support

The Iredell County Information Technology Department has sole responsibility for technical support to users for all Iredell County systems. Unless Information Technology has specified otherwise for a particular system, users should always contact Information Technology for all technology-related needs.

### 1.10 Electronic Messaging

Electronic messaging includes, but is not limited to email, instant messages, text messages, blog posts, forum posts, wiki posts, images and audio or video recordings. Electronic messaging may not be used in any way which violates County policy.

#### 1.10.1 County Representation

All publicly posted electronic messages must clearly identify the user, with credentials assigned by the County. Message subject and content must be in the interest of the County.

#### 1.10.2 Personal Messaging Accounts

Personal messaging accounts may not be accessed from County systems. Information Technology staff may use personal messaging accounts solely for the purpose of testing Iredell County systems.

#### 1.10.3 Internal Broadcast Messages

Iredell County employees may not send out broadcast (very wide reaching) messages within the county without County Management approval. Only broadcast messages that are County business related or a matter of community interest will be authorized.

#### 1.10.4 Public Record and Retention

Electronic messages may be considered public record and as such are subject to public record retention rules.

Iredell County Information technology is responsible for archiving email.

#### 1.10.5 Social Media

Employees should never use their county e-mail account or password in conjunction with a personal social networking site.

### 1.11 County Internet Content

Public Internet content includes but is not limited to the main County public web site and all content therein, other County-owned web sites which lie outside of the main County web site, and social sites representing the County which are administered by the County.

Iredell County public Internet content is the responsibility of the Iredell County Web Developer. The Web Developer and his/her designee(s) may edit and publish public web content on behalf of the County.

The Web Developer is responsible for establishing and publishing web site standards. All web site content must comply with the Iredell County web site standards (design, layout, etc.) as approved by the Web Developer.

The Web Developer must review web application design and layout for compliance with standards before application publication. As web application content is dynamic in nature, review of said content by the Web Developer is not required.

Each department is solely responsible for the accuracy of the content of their respective web site(s) and/or pages.

Links to other websites are restricted to local, state, or federal government sites. Links to non-profit and personal websites are not allowed. Information on events will be limited to those directly sponsored by Iredell County.

### 1.12 Storage Media Recycling and Disposal

The purpose of this section is to ensure that all digital media is properly recycled or disposed of for reasons pertinent to data security, software license protection, and in compliance with environmental regulation.

If a hard disk, tape, CD, DVD, ZIP disk, diskette, or other storage device can be re-used, users should erase the existing data from the device and continue to use it, or make it available for someone else to use. If the digital media is unusable, or is no longer needed, it should be sent to ITS for destruction.

Un-recycled or unusable media must be completely erased using a disk sanitizer utility. If that is not possible, the media should be physically damaged in a manner to render it unreadable by any device.

### 1.13 Surplus

The Iredell County Information Technology Department has sole responsibility for disposition of surplus technology hardware and software. All unassigned, unallocated, or otherwise unneeded equipment or software must be returned to Information Technology.

### 1.14 County Assets

The use of County assets (computers, Internet access, email, etc.) is intended for purposes relevant to the responsibilities assigned to each employee. Social networking sites are not deemed a requirement for most positions, and certain job titles are not permitted to access these services over the Internet. For employees who are allowed to access these services, a reasonable and limited amount of use of County assets is permitted for social networking services.

# IREDELL COUNTY
## USE OF INFORMATION TECHNOLOGY RESOURCES POLICY
**Revised January 1, 2012**

I hereby acknowledge that I have received, read and understand the Iredell County Use of Information Technology Resources Policy. I agree to comply with all the provisions of this policy. I understand that violation of this policy can result in disciplinary action up to and including termination of employment.

Employee Name (please print)_____

Department_____

Date_____

Signature_____