



# Catoosa County Government

800 LaFayette ST, Ringgold, GA 30736  
Phone: 706-965-2500 Fax: 706-935-3112

## ACCEPTABLE TECHNOLOGY USAGE POLICY

This Acceptable Usage Policy covers the security and use of all Catoosa County Government information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all Catoosa County Government employees, contractors and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to Catoosa County Government business activities worldwide, and to all information handled by Catoosa County Government relating to other organizations with whom it deals. It also covers all IT and information communications facilities operated by Catoosa County Government or on its behalf.

### Computer Access Control – Individual's Responsibility

Access to the Catoosa County Government IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Catoosa County Government IT systems.

### Password Requirements

#### User ID and Password

- Username and password combinations provide access to assets.
- A temporary initial password may be assigned, however once the temporary password has been used it will be changed.
- All password(s) resets require the validation of user identity.

#### Password and Session Configurations

**Password configurations, when system limitations are not present, shall be set up to include the following:**

- Limited consecutive unsuccessful login attempts that is less than or equal to five (5).
- Minimum number of characters necessary for password(s) that is greater than or equal to eight (8).
- Alpha and numeric password enforcers.
- Periodic forced password changes that is less than or equal to one hundred-eighty (180) days.
- Disallowance of reused password(s) that is less than or equal to five (5).
- Screensavers shall be used to lock a user's session after a period of twenty (20) minutes of idle time.
- Remote administrative console, Telnet sessions and/or SSH sessions reset after thirty (30) minutes of idle activity.

#### Password

**When system limitations are not present, strong password(s) shall have the following characteristics:**

- Contain at least eight (8) characters. Contain both upper and lower-case characters.
- Contain at least one (1) number to include the numbers 0-9.
- Are not based on personal information, names of family, etc.
- Are never written down or stored online.

**Additionally, it is recommended that password(s):**

- Have deliberate misspellings.

- Are not words in any language, slang, dialect, jargon, etc.
- Are never shared.

**Poor or weak password(s) have the following characteristics:**

- Contains some part of the user's name.
- Contains less than eight (8) characters.
- Are words found in a dictionary, i.e. English or Foreign.
- Are words found in proper names, i.e. Sports Teams, etc.
- Are common usage words as family name, pet, friend, co-worker, etc.

**Individuals must not:**

- Allow anyone else to use their user ID/token and password on any Catoosa County Government IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access Catoosa County Government IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorized changes to Catoosa County Government IT systems or information.
- Attempt to access data that they are not authorized to use or access.
- Exceed the limits of their authorization or specific business need to interrogate the system or data.
- Connect any non-Catoosa County Government authorized device to the Catoosa County Government network or IT systems.
- Store Catoosa County Government data on any non-authorized Catoosa County Government equipment.
- Give or transfer Catoosa County Government data or software to any person or organization. outside Catoosa County Government without the authority of Catoosa County Government. Department Heads and Supervisors must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

**Internet and email Conditions of Use**

Use of Catoosa County Government internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Catoosa County Government in any way, is not in breach of any term and condition of employment and does not place the individual or Catoosa County Government in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.

**Internet Access Level**

All employees will be assigned an access usage level by their Constitutional Officer/Department Head when hired.

Following are the Filtering Tier Levels and Blocked Categories:

<b><u>Content Filter Tier</u></b>	<b><u>Blocked Categories</u></b>
<b>Banned County-Wide</b> (Blacklisted Sites)	Pornography, Tasteless, Sexuality, Proxy/Anonymizer, Adware, Alcohol & Drugs, Dating, Gambling, Hate & Discrimination, Lingerie, Nudity, Weapons, Adult Themes, Games. ( <u>Exception</u> : It may be necessary for certain law enforcement personnel to access blacklisted websites as part of criminal investigations and evidence collection. Access to blacklisted websites will be strictly controlled by the Catoosa County Sheriff.)
<b>No Access</b>	Blocks employees from accessing <u>any websites</u> except those that are required for performing work related tasks (i.e. <a href="http://www.catoosa.com">www.catoosa.com</a> and Catoosa email (Gmail)).
<b>Limited Access</b>	Provides access to required work-related websites, and other specific websites determined by the Department Head/Constitutional Officer as required and essential for the employee to do their job. Examples would be chat and social, classifieds, file sharing & point to point, forums & message boards, instant messaging, photo and video sharing, visual search engines, webmail. Specific websites will be verified by the Department Head / Constitutional Officer, and access will be limited to those websites.
<b>Full Access</b>	Access to all internet sites except those blocked by the county-wide filter. Department Head / Constitutional Officer must attest to why an employee has a work-related need to be granted full access.

**Individuals must not:**

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which Catoosa County Government considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness. For example, distributing chain letters or spam.
- Place any information on the Internet that relates to Catoosa County Government, alter any information about it, or express any opinion about Catoosa County Government, unless specifically authorized to do so.
- Send unprotected sensitive or confidential information externally.
- Forward Catoosa County Government mail to personal (non-Catoosa County Government) email accounts. For example, a personal Hotmail account.
- Make official comments through the internet, or email on behalf of Catoosa County Government unless authorized to do so.
- Download copyrighted material such as music, media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe upon any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without the prior approval of the IT Department.
- Connect Catoosa County Government devices to the internet using non-standard connections.

### **Clear Desk and Clear Screen Policy**

In order to reduce the risk of unauthorized access or loss of information, Catoosa County Government enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

### **Working Off-site**

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with Catoosa County Government remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car (exceptions for law enforcement map apply).
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

### **Mobile Storage Devices**

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Catoosa County Government authorized mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

### **Software**

Employees must use only software that is authorized by Catoosa County Government on Catoosa County Government computers. Authorized software must be used in accordance with the software supplier's licensing agreements. All software on Catoosa County Government computers must be approved and installed by the Catoosa County Government IT department.

### **Individuals must not:**

- Store personal files such as music, video, photographs or games on Catoosa County Government IT equipment.

### **Viruses**

The IT department has implemented centralized, automated virus detection and virus software updates within the Catoosa County Government. All PCs have antivirus software installed to detect and remove any virus automatically.

### **Individuals must not:**

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved Catoosa County Government anti-virus software and procedures.

### **Telephony (Voice) Equipment Conditions of Use**

Use of Catoosa County Government voice equipment is intended for business use. Individuals must not use Catoosa County Government voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications

#### **Individuals must not:**

- Use Catoosa County Government voice for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators, unless it is for business use.

#### **Actions upon Termination of Contract**

All Catoosa County Government equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Catoosa County Government at termination of employment.

All Catoosa County Government data or intellectual property developed or gained during the period of employment remains the property of Catoosa County Government and must not be retained beyond termination or reused for any other purpose.

#### **Monitoring and Filtering**

All data that is created and stored on Catoosa County Government computers is the property of Catoosa County Government and there is no official provision for individual data privacy. However, wherever possible, Catoosa County Government will avoid opening personal emails.

IT system monitoring will take place where appropriate, and investigations will be conducted when reasonable suspicion exists of a breach of this or any other policy. Catoosa County Government has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

**It is your responsibility to report suspected breaches of security policy without delay to your Department Head, the IT department, or the County Manager. All breaches of information security policies will be investigated. If an investigation reveals employee misconduct, the County Manger will work alongside the Constitutional Officer and/or Department Heads to determine what actions will be taken.**

---

**Employee Acknowledgement**

I understand this technology usage policy is intended to protect the integrity and content of the Catoosa County Government IT Systems used to provide government services to the Citizens of Catoosa County. I further understand, that as a County IT user, I must abide by the outlined policies and procedures. The protection and security of Catoosa County Government IT Systems and the information contained therein is vitally important.

---

EMPLOYEE SIGNATURE

---

DATE

---

PRINTED NAME

---

DEPARTMENT

---

DIRECTOR