

# OCONEE COUNTY INFORMATION TECHNOLOGY POLICY

## Table of Contents

1. Introduction
2. Computer Usage
3. Software Usage
4. Email/Messaging Usage
5. Internet Usage
6. Ownership of Data and Files
7. Security
8. Inappropriate Use of Resources
9. IT Policy Violations

### 1) Introduction

It is the policy of Oconee County to regulate all County computers, phones, and related technology, "Devices" and the manner in which they are used. County Information Technology, "IT," resources are provided to employees for work-related activities and communications, research, and professional development. This policy is designed to maintain the security of the overall network, and to provide guidelines about permitted usage of County IT resources.

### 2) Computer Usage

The following rules govern usage of all Devices:

- a) Only the employees of Oconee County and other persons designated by County Administration or County IT are authorized to use or access County computers.
- b) Employees will only use Devices in the direct performance of their assigned duties unless authorized by their department head.
- c) Employees should not bring personal laptops or other personal computers (excluding personal phones or tablets) to the workplace, unless expressly permitted to do so by County IT.
- d) Employees should not connect any personal devices to County electronic systems unless expressly permitted to do so by County IT.
- e) Employees needing assistance with computer related problems should contact County IT (either by phone, email or submit a work order) for all hardware or software problems and installations.

### 3) Software Usage

The following rules govern software usage, installation, and uninstallation in the County and on County Devices:

- a) No downloaded application software is to be installed on any County equipment by anyone except County IT. Downloaded software may create conflicts with existing software and result in a partial or complete computer failure. All software must be installed or uninstalled by County IT employees and will be subject to review at any time.
- b) Requests for new software or software installation will be made through County IT.
- c) No software or files from the County shall be copied for personal use without permission.
- d) No employees shall use County computers to develop software to be used outside the County.
- e) Any software developed on County Devices while on County property or when engaged as a County Employee is the property of Oconee County.

#### **4) Email/Messaging Usage**

The following rules govern usage of County Email and Messaging:

- a) Brief and occasional personal use of email is acceptable as long as it is not excessive or inappropriate. Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities.
- b) Email/messaging shall not be used to solicit or sell products or services that are unrelated to the County's business
- c) Email/messaging shall not be used to distract, intimidate, or harass coworkers or third parties or disrupt the workplace.
- d) All emails/messages are the property of Oconee County, may be retrieved at any time and are subject to review, including personal emails utilizing County Devices.
- e) Email/messaging should not be used to send chain emails that are unrelated to legitimate County purposes.
- f) Department Heads have the discretion to work with employees to determine the appropriateness of using email/messaging for professional or personal activities.
- g) Emails containing sensitive, Personally Identifiable Information (PII) should be encrypted according to the latest encryption protocols recommended by County IT.
- h) All county employees may be required to have a standardized email signature line, according to the County Administrator or designee.

#### **5) Internet Usage**

The following rules govern Internet usage on all County devices:

- a) All County policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to confidentiality, standards of conduct, and harassment.
- b) Brief and occasional personal use of the Internet is acceptable as long as it is not excessive or inappropriate. Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities.
- c) Internet usage shall not be used to solicit or sell products or services that are unrelated to the County's business
- d) Internet usage shall not be used to distract, intimidate, or harass coworkers or third parties or disrupt the workplace.
- e) Employees should understand that sites visited, number of times visited, and total time connected to each site are maintained and are subject to review.
- f) Employees are only permitted to download work-related files.
- g) All Users with Internet access must have current anti-virus and anti-malware software running at all times.
- h) Oconee County is not responsible for material viewed or downloaded by users from the Internet.
- i) Department Heads have the discretion to work with employees to determine the appropriateness of using the Internet for professional or personal activities.

## **6) Ownership of Data and Files**

The following rules govern ownership of data and files in the County:

- a) The County owns the rights to all data and files in any County Device used in the County.
- b) The County also reserves the right to monitor any and all electronic communication (including email, phone call, text communication, and any and all personal/private/instant messaging systems) and their content when used on County Devices, as well as any and all use of the Internet and of computer equipment used to create, view, or access e-mail and Internet content.
- c) Employees must be aware that email messages sent and received using a County Device are not private and are subject to viewing, downloading, inspection, release, and archiving by County officials at all times. Additionally the Georgia Open Records Act could allow a public disclosure of email messages sent and received using a County Device.
- d) The County has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with policy and state and federal laws.
- e) No employee may access another employee's computer, computer files, or email messages without prior authorization from the employee, their department head, or the County Administrator.
- f) No employee, including system administrators and supervisors, may access email and computer systems files without a legitimate County interest.

## **7) Security**

The following rules govern network security in the County:

- a) Employees of Oconee County that need to access county computers have an individual username and password that allows them to access the system. An employee may not share or offer the use of his or her password so that anyone else may gain access to the system. Unauthorized use of another employee's password is prohibited.
- b) No internet connection shall be installed in County facilities unless first reported and approved by County IT.
- c) All technology projects that involve internet/intranet usage shall first be reported and approved by County IT.
- d) Employees must log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended.

## **8) Inappropriate Use of Resources**

Other inappropriate uses of resources include, but are not limited to:

- a) Deliberately propagating any virus, worm, Trojan horse, cryptolocker, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either County Devices or those of any other individual or entity.
- b) Any types of hacking, invasions of privacy, trespassing or other network compromises.
- c) Causing congestion, disruption, disablement, alteration, or impairment of the County networks or systems.
- d) Attempts to degrade performance of a computer system on the Internet or to deprive authorized personnel of resources or access to any computer system.
- e) Defeating or attempting to defeat security restrictions on county systems and applications.
- f) Using abusive, profane, threatening, or otherwise objectionable language in either public or private messages.
- g) Misrepresenting oneself or the County.

- h) Sending, receiving, or accessing pornographic materials.
- i) Using recreational games.
- j) Video streaming not related to work, professional development, or work-related activities.
- k) Engaging in any unlawful or malicious activities.
- l) Violating the laws and regulations of the United States or the State of Georgia.

**9) IT Policy Violations**

The following describes consequences for violating the rules outlined in this IT Policy:

- a) Violation of this policy, failure to permit an inspection of any device covered by this policy, or failure to report a security breach, shall result in disciplinary action, up to and possibly including termination of employment. In addition, the employee may face both civil and criminal liability from the County or from individuals whose rights are harmed by the violation.
- b) Use of County Devices is a privilege granted by the County and may be revoked at any time for inappropriate conduct.
- c) Employees are individually liable for any and all damages incurred as a result of violating County security policy, copyright, and licensing agreements.

This policy shall take effect on the date it is adopted by the Oconee County Board of Commissioners.

ADOPTED AND APPROVED, This 5th day February, 2019

OCONEE COUNTY BOARD OF COMMISSIONERS

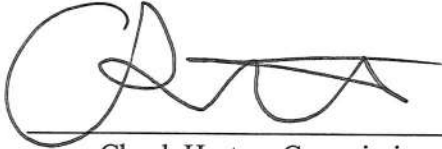
Attest:

  
Kathy Hayes, County Clerk



  
John Daniell, Chairman

  
Mark Thomas, Commissioner, Post 1

  
Chuck Horton, Commissioner, Post 2

  
W.E. Wilkes, Commissioner, Post 3

  
Mark Saxon, Commissioner, Post 4