

**SOUTH CAROLINA DEPARTMENT OF ADMINISTRATION  
INTERNET AND NETWORK SERVICES ACCEPTABLE USE POLICY**

**THE LANGUAGE USED IN THIS DOCUMENT DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE AGENCY. THIS DOCUMENT DOES NOT CREATE ANY CONTRACTUAL RIGHTS OR ENTITLEMENTS. THE AGENCY RESERVES THE RIGHT TO REVISE THE CONTENTS OF THIS DOCUMENT, IN WHOLE OR IN PART. NO PROMISES OR ASSURANCES, WHETHER WRITTEN OR ORAL, WHICH ARE CONTRARY TO OR INCONSISTENT WITH THE TERMS OF THIS PARAGRAPH CREATE ANY CONTRACT OF EMPLOYMENT.**

**I. Policy Statement**

Access to and utilization of personal computers, computer systems, and networks owned or operated by the Department of Administration (Department) impose certain responsibilities and obligations on Department employees (hereinafter termed “users”) and are subject to state government policies and local, state, and federal laws. Acceptable use is always ethical and reflects honesty. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and the individual’s right to freedom from intimidation, harassment, and unwarranted annoyance. Users may be subject to limitations on their access to and the use of the networks as determined by the appropriate supervising authority. If you or anyone you allow to access your account violates this Policy, your access may be restricted or withdrawn.

Where relevant, all Department of Administration policies – including but not limited to those governing harassment, discrimination, ethics, confidentiality, and security – apply to Internet, network, and electronic mail use and content.

By participating in the use of networks and systems provided by the Department, users agree to be subject to and abide by this Policy for their use. Willful violation of the principles and provisions of this policy may result in disciplinary action up to and including termination of employment. Should another user violate this Policy while using your account, both of you may be subject to disciplinary action.

**II. Terms of Permitted Use, Privacy, and Monitoring**

Access to the Internet and the Department’s network is provided as a tool for the Department’s stated business activities. Your computer, associated software, and attached systems are all property of the Department. Use of network services provided by the Department is subject to monitoring for security, network management, or other purposes deemed appropriate by Department management. The Department has software and systems in place that monitor and record all Internet usage. Its security systems are capable of recording each website visit, each chat, newsgroup or electronic mail message, and each file transfer into and out of our

internal networks, and the Department reserves the right to do so at any time. No employee should have any expectation of privacy as to his system, Internet, or electronic mail usage. Employees are therefore advised of this potential monitoring and of the fact that there is no expectation that any system, Internet, or electronic mail usage is private.

The Department may suspend access to its network and the Internet at any time for technical reasons, Policy violations, and other concerns.

### **III. Personal Responsibility**

By accepting your user identification and password and related information, and accessing the Department's network or Internet, you agree to adhere to this Policy. You also agree to report any network or Internet misuse or abuse to your Office or Division Director, or to the Department's Internal Chief Information Officer. Misuse includes Policy violations that harm another employee or another individual's property.

### **IV. Violations**

The following individual personal computer, computer network, and Internet activities are expressly prohibited:

- A. Using, transmitting, receiving, or seeking inappropriate, offensive, vulgar, suggestive, obscene, abusive, harassing, belligerent, threatening, defamatory, or misleading language or materials. The display of any kind of sexually explicit image or document on any computer system is a violation of the Department's sexual harassment policy. Sexually explicit images or documents include those containing nudity or partial nudity. In addition, sexually explicit material may not be archived, stored, distributed, edited, or recorded using the Department's networks or computing resources, except by those employees involved in authorized investigations of potential violations of this Policy. Any such investigation must be authorized by the Executive Director, the Chief of Staff, the General Counsel, the Internal Chief Information Officer, or the designated Division Director, and should be coordinated with the Department's Human Resources Director.
- B. Engaging in immoral, illegal, or unlawful activities, violating the Policies and Procedures of the Department, or encouraging others to do so. Examples include (but are not limited to):
  - a. Accessing, transmitting, receiving, or seeking unauthorized, confidential information
  - b. Conducting unauthorized activities
  - c. Viewing, uploading, printing, copying, filing, transmitting, downloading, or searching for obscene, pornographic, sexually explicit, illegal, or otherwise objectionable, non-business related Web content

- d. Accessing others' folders, files, work, networks, or computers without express permission
  - e. Intercepting communications intended for others
  - f. Downloading or transmitting the Department's confidential information without proper authorization
- C. Using the networks or Internet for recreational, non-public purposes. The following specific activities are expressly prohibited (not meant to constitute an exhaustive list):
  - a. Online gambling
  - b. Stocks, bonds, and securities trading
  - c. Online auction participation
- D. Using the network or Internet for commercial activities
- E. Using the network or Internet for the purpose of supporting candidates for public office in a partisan election; using official authority or influence to interfere with or affect the results of an election or nomination; or directly or indirectly coerce contributions from subordinates in support of a political party or candidate; using the network or Internet for disseminating political campaign material to another employee on his computer
- F. Using the networks, Internet, or other state equipment for personal gain such as selling access to the network, or by performing work for profit with Department resources in a manner not authorized by the Department
- G. Using or installing software not licensed or approved by the Department
- H. Installing or using hardware or peripheral equipment not specifically approved and authorized by the Division Director or the Department's Internal Chief Information Officer, or using approved equipment in a manner inconsistent with the approved purpose for which the equipment was installed. Prohibited equipment examples include any electronic surveillance, audio, or video recording equipment not directly related to functions required by job duties and responsibilities.
- I. Vandalizing or using the network to disrupt network users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of viruses, harmful components, or corrupted data.
- J. Attempting to circumvent or subvert system or network security measures
- K. Intercepting network traffic for any purpose unless engaged in authorized network administrative duties

- L. Encouraging others to view, download, or search for materials, files, information, software, or other offensive, defamatory, misleading, infringing, or illegal content, e.g. forwarding electronic mail with offensive attachments, images, or Internet links
  
- M. Making or using illegal copies of copyrighted software or other mediums, storing such copies on Department systems, or transmitting them over Department networks. Users who violate any copyright declarations are acting outside the course and scope of their employment or other authority and the Department is relieved of any legal responsibility thereof. Users will be personally responsible and liable for such infringing activities.

The following electronic mail activities are expressly prohibited:

- A. Using electronic mail or messaging services to harass, intimidate, or otherwise annoy another person
  
- B. Sending, soliciting, printing, or copying text or images that disparage others based on their race, religion, color, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age
  
- C. Sending, soliciting, printing, or copying jokes (text or images) based on sex, sexual orientation, race, age, religion, national origin, or disability
  
- D. Sending, soliciting, printing, or copying messages that are disparaging or defamatory
  
- E. Sending, soliciting, printing, or copying sexually oriented messages or images
  
- F. Sending, soliciting, printing, or copying messages or images that contain foul, obscene, or adult-oriented language
  
- G. Sending, soliciting, printing, or copying messages or images that are intended to alarm others, embarrass the Department, or negatively impact employee productivity

If an employee finds himself connected incidentally to a website that contains offensive material he must disconnect from the website immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.

If an employee is the recipient of electronic mail that violates any of the provisions pertaining to electronic mail, he must immediately delete and remove the offending message.

## **V. Non-Working Time Limited Personal Use**

Department computer systems and networks are to be used primarily for conducting official state business. It is recognized that employees may occasionally use these systems and networks for limited incidental personal use during non-working time. Such limited personal use may be acceptable as long as other usage policies are followed and the use does not interfere with an employee's work or negatively impact the computer system or network, and does not result in additional public expense. These systems are not available or accessible for public speech or any First Amendment expressive activity or for use by the public; further, the systems are expressly declared not to be a public forum.