



SOUTH CAROLINA REVENUE AND FISCAL AFFAIRS OFFICE

Information Security Program ACCEPTABLE USE POLICY

Revision History

Date	Authored by	Title	Ver.	Notes
14-Jul-2014	Information Security	Acceptable Use Policy	1.0	Initial draft

INTRODUCTION

SOUTH CAROLINA REVENUE AND FISCAL AFFAIRS 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.

Acceptable Use Policy

I. Policy Statement

Access to and utilization of personal computers, computer systems, and networks owned or operated by the Revenue and Fiscal Affairs Office (RFA) impose certain responsibilities and obligations on RFA employees, contractors, or third-party representatives (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, or subject to disciplinary action as outlined in this policy, 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 If you or anyone you allow to access your account violates this Policy, your access may be restricted or withdrawn.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 Revenue and Fiscal Affairs Office 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 RFA, 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 RFA’s network is provided as a tool for the RFA’s stated business activities. Your computer, associated software, and attached systems are all property of the RFA. Use of network services provided by the RFA is subject to monitoring for security, network management, content, or other

purposes deemed appropriate by RFA management. The RFA 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 RFA 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 RFA 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 RFA'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 Agency Director, or to the RFA's Internal Chief Information Officer.

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 RFA'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 RFA'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, or his designee, and should be coordinated with the RFA's Human Resources Director.
- B. Engaging in immoral, illegal, or unlawful activities, violating the Policies and Procedures of the RFA, or encouraging others to do so. Examples include (but are not limited to):
 - a. Accessing, transferring, transmitting, receiving, or seeking unauthorized, confidential information
 - b. Conducting unauthorized activities
 - c. Viewing, uploading, printing, copying, filing, transmitting, downloading, or searching for unauthorized personally identifying information or 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, transferring, or transmitting the RFA's confidential information without proper and prior 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. Online gaming
 - e. Unauthorized Peer-to-peer activities
- D. Using the network or Internet for commercial or political purposes
- E. Using the network, Internet, or other state equipment for personal gain such as selling access to the network, or by performing work for profit with RFA resources in a manner not authorized by the RFA
- F. Using or installing software not licensed or approved by the RFA
- G. Installing or using hardware or peripheral equipment not specifically approved and authorized by the Executive Director or the RFA'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 but are not limited to unauthorized networking devices, non-business provided and unencrypted external storage devices, any electronic surveillance, audio, or video recording equipment not directly related to functions required by job duties and responsibilities.
- H. 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.
- I. Attempting to circumvent or subvert system or network security measures
- J. Intercepting network traffic for any purpose unless engaged in authorized network administrative duties
- K. 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
- L. Making or using illegal copies of copyrighted software or other mediums, storing such copies on RFA systems, or transmitting them over RFA networks. Users who violate any copyright declarations are acting outside the course and scope of their employment or other authority and the RFA is relieved of any legal responsibility thereof. Users will be personally responsible and liable for such infringing activities.
- M. 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, receiving, 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, receiving, soliciting, printing, or copying jokes (text or images) based on sex, sexual orientation, race, age, religion, national origin, or disability
- d. Sending, receiving, soliciting, printing, or copying messages that are disparaging or defamatory
- e. Sending, receiving, soliciting, printing, or copying sexually oriented messages or images
- f. Sending, receiving, soliciting, printing, or copying messages or images that contain foul, obscene, or adult-oriented language
- g. Sending, receiving, soliciting, printing, or copying messages or images that are intended to alarm others, embarrass the RFA, 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.
