

**SOUTH CAROLINA
DEPARTMENT OF HEALTH AND HUMAN SERVICES**

THE LANGUAGE USED IN THIS POLICY DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE DEPARTMENT. THIS DOCUMENT DOES NOT CREATE ANY CONTRACTUAL RIGHTS OR ENTITLEMENTS. THE DEPARTMENT RESERVES THE RIGHT TO REVISE THE CONTENT 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.

HR 015.00 **Internet and Social Media Usage Policy**

EFFECTIVE: November 16, 2011

APPLIES TO: All South Carolina Department of Health and Human Services (the Department) Workforce Members

POLICY

The Department of Health and Human Services (the Department) permits the use of the Internet, including Social Media Sites, for legitimate business purposes that enhance the Department's mission, vision, values and goals. This policy applies only to work-related electronic systems and issues and is not meant to infringe upon employees' personal interaction or commentary online and should not be construed as interfering with employees' protected rights or the right to engage in activities protected by any federal, state or local law or regulation. This policy supplements all other Department policies whether they are directly or indirectly related to the use of the Internet and/or Social Media Sites.

PURPOSE

The purpose of this policy is to set forth the minimum guidelines governing the appropriate use of the Internet, including Social Media Sites. Commonly used Social Media Sites include, but are not limited to, Facebook®, Twitter®, Flickr®, MySpace™, LinkedIn® Wiki and YouTube®, as well as personal blogs and Internet pages.

**SOUTH CAROLINA
DEPARTMENT OF HEALTH AND HUMAN SERVICES**

15.01 Internet Usage

- A. Employees of the Department are expected to use the Department's computers, networks and Internet responsibly, productively and for legitimate business purposes. Brief and occasional personal use of the electronic mail system or the Internet (for example, communicating with children's schools or daycare) may be acceptable if the use does not interfere with employee performance or normal workplace operations, is not excessive, is not inappropriate and does not disrupt the operations of the Department's network or otherwise violate this policy.
- B. "Excessive" use is defined as any use that interferes with normal job functions, the ability to perform daily job activities or misuse of working time.
- C. "Inappropriate" use includes, but is not limited to:
1. Using abusive, profane, threatening, racist, sexist or otherwise objectionable language in either public or private messages;
 2. Using ethnic slurs, personal insults, obscenity or engaging in any conduct not in compliance with laws governing defamation, slander, discrimination and/or harassment;
 3. Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") unrelated to legitimate Department business;
 4. Excessive use of blogs or Social Media Sites;
 5. Accessing networks, servers, drives, folders or files to which the employee has not been granted access or authorization from a Department official authorized to make such a grant;
 6. Making or distributing unauthorized copies of Department files or other Department data;
 7. Purposely or negligently disclosing confidential or Protected Health Information (PHI) of other employees, clients or other constituents of the Department without documented written consent. This is also considered unlawful conduct and may result in a HIPAA incident to be investigated and sanctioned accordingly;

**SOUTH CAROLINA
DEPARTMENT OF HEALTH AND HUMAN SERVICES**

8. Misrepresenting oneself or the Department;
 9. Engaging in unlawful or malicious activities;
 10. Deliberately propagating any virus, worm, Trojan horse, trap-door program code or other code or file designed to disrupt, disable, impair or otherwise harm either the Department's networks or systems;
 11. Sending, receiving or accessing pornographic, obscene, sexually suggestive or graphic materials of any kind;
 12. Causing congestion, disruption, disablement, alteration or impairment of Department networks or systems;
 13. Using recreational games; and/or
 14. Defeating or attempting to defeat security restrictions on Department systems and applications.
- D. Using the Department's electronic mail system, Internet access and computer systems to access, create, view, transmit or receive racist, sexist, threatening or otherwise objectionable or illegal material, defined as any visual, textual or auditory entity, file or data, is strictly prohibited. Such behavior violates the Department's Anti-Discrimination/Anti-Harassment Policy and Procedures and is subject to disciplinary action, up to and including immediate termination.
- E. In accordance with the Department's Information Technology Use and Security Policy Section 4.1, the Department reserves the right to monitor the use of Department equipment by employees and others, and employees should have no expectation of privacy with regard to any information contained on Department computers, devices or networks.
- F. The Department's electronic systems must not be used to harm others or to violate state and federal laws and regulations in any way. Use of Department resources for illegal activity may lead to disciplinary action, up to and including termination and criminal prosecution.
- G. To the extent required by law, the Department will comply with requests from law enforcement and regulatory agencies for logs, diaries, archives or files on individual Internet activities, e-mail use and/or computer use.

**SOUTH CAROLINA
DEPARTMENT OF HEALTH AND HUMAN SERVICES**

15.02 Social Media Usage

- A. In the course of performing Department functions, employees must comply with the following guidelines when using Social Media Sites, whether accessed through the Department's electronic systems or personal electronic systems:
1. Information published by Department employees through Social Media Sites must comply with the Department's Privacy and Security Policies.
 2. Department employees must be aware that any information published on Social Media Sites may be interpreted as expressing the official position of the Department; therefore, the information published must be in compliance with the requirements and guidelines provided in this policy.
 3. Content published on Social Media Sites must be in compliance with requirements of the South Carolina Freedom of Information Act.
- B. Employees are prohibited from using Social Media Sites to make statements that are intended to injure or harm the Department, its programs, its employees or its customers. This includes making statements that may be unlawful, such as threatening a Department employee or customer.
- C. Employees should be aware that postings made to Social Media Sites and other on-line forums outside of work can blur the distinction between their professional and personal identities. Under the law, a public employee's free speech rights and interests in addressing matters of public concern are balanced against the Department's interest in efficient operation of government. Employees who use Social Media Sites outside of work should be aware that they are responsible for the content of any postings and should follow these guidelines:
1. An employee posting content about a subject associated with the Department should consider using a disclaimer such as, "The views expressed herein are my own and do not necessarily represent the opinion or views of my employer."
 2. Employees should have no expectation of privacy regarding postings made to public spaces such as blogs and Social Media Sites, regardless of password protections, ability to designate personal privacy settings or

**SOUTH CAROLINA
DEPARTMENT OF HEALTH AND HUMAN SERVICES**

other security measures.

- D. Employees must not use Department email to establish a personal social media presence.
- E. Employees must not conduct Department business over personal social media channels.
- F. Employees may not use Department logos and trademarks on Social Media Sites without the express written consent of executive management.
- G. Any media or press contact made to an employee about social media content posted using the Department’s electronic systems must be referred immediately to the Department’s Public Information Officer.
- H. Any Incident or Breach as defined in this policy related to the use of Social Media Sites must be reported immediately to the Public Information Officer, the Office of General Counsel and the Department’s Office of Human Resources. If the Incident or Breach involves PHI, it must also be reported to the Privacy/Security Incident Investigator in accordance with the Department’s Privacy/Security Incident Reporting and Response Policy.
- I. Violations of this policy may result in disciplinary action, up to and including immediate termination.

15.03 Definitions

- A. Breach – Unauthorized access of personal or proprietary information from the use of Social Media Sites; also, the unwitting download of viruses and other harmful software onto the Department’s computer network.
- B. Incident – Any posting of content on Social Media Sites that potentially or actually creates a breach of the confidentiality of information belonging to Department networks, employees, clients or members of the public as set forth in Department policy or otherwise violates Department policy.
- C. Social Media Sites – Websites that facilitate user-participation, networking and collaboration through the submission of user-generated content. A “social media identity” is a specific user identity or account that has been registered on a third

**SOUTH CAROLINA
DEPARTMENT OF HEALTH AND HUMAN SERVICES**

party social media site. Social media includes, but is not limited to: blogs, wikis, microblogging sites such as Twitter©; social networking sites such as Facebook© and LinkedIn® and video sharing sites such as YouTube©.

- D. Workforce Member – For the purpose of this policy and HIPAA, workforce member is defined as employees, volunteers, trainees and other persons whose conduct, in the performance of work for the Department, is under the direct control of the Department, whether or not they are paid by the Department.