

ORC:
OAC:
CFSR:
Board:
Other: _____

Next Review Date: 1/2024
Last Reviewed: 1/2021
Review Responsibility: Executive Council

FCCS PROCEDURE

NO.: 12C.2

SUBJECT: Responsible Internet Use

Approved by: Executive Council

Effective Date: Sep. 4, 1998

Date(s) of Revision: Oct. 1, 1998; Jan. 1, 2001; Apr. 1, 2003; May 4, 2005; Feb. 27, 2009; Jun. 4, 2009, Mar 15, 2010, Nov 18, 2010; Dec 5, 2011; Sep 6, 2016; Jan 26, 2021

Responsible for Implementation: All Staff

FCCS employees have access to the Internet. This access carries with it certain responsibilities. Please note that these responsibilities are present whenever users are connected to FCCS systems/devices, be it in the office or through the use of connectivity software (e.g. VPN).

Procedures:

Responsible Internet Use

The Internet's capacity for providing global access to massive amounts of uncensored information makes it both a powerful tool and a potential liability to the agency. Inappropriate use of the Internet can expose the agency to the following types of risks:

- 1) Damage to the agency's computers, network or software.
- 2) Breach of confidential information about clients or employees.
- 3) Interference with the use of the Internet for business purposes.

Responsible Internet use includes:

- 1) Abstaining from downloading any software, programs or applications, including sound card software, video card software, screen savers, add-on toolbars and instant messaging.
- 2) Refraining from typing your Agency e-mail address into any website, except those maintained by professional organizations related to the practice of child welfare or those used to complete tasks necessary for fulfilling job responsibilities.
- 3) Avoiding any websites promoting harassing or threatening statements-sites with material that may be hostile or offensive on the basis of age, race, color, religion, national origin, disability, or any cultural identifier, sex, sexual orientation, gender identity or expression, but requesting an unblocking of websites that may be beneficial when working on cases (or research) that involve sexual abuse or inappropriate sexual activity, or the use of those websites is in pursuit of strategies for improving our cultural competencies and cultural competency trainings. At the request of an Associate Director or above the IT Department will unblock websites with sexual content for a limited number of staff for a limited period of time.
- 4) Avoiding websites related to any activities (e.g., gambling, chat rooms, illegal transactions, political campaigns) that are not related to job functions and that would expose the agency to risk or embarrassment.
- 5) Using the Internet primarily as a business tool and limiting any personal use so that it does not interfere with work responsibilities.
- 6) Reporting excessive pop-up screens to ITServiceDesk@fccs.us. Pop-up screens are types of windows that appear in front of a website. They are usually company advertisements. Excessive pop-up screens will seem to endlessly cascade where every pop-up you close seems to open many more.

Access to restricted websites:

FCCS employees have limited access to the internet. This access precludes visiting certain sites deemed unsuitable for agency use. The filtering process is

done by a software package that, at times, may block legitimate sites. This policy allows for enabling access to those legitimate sites.

To request access to a restricted website:

- 1) Send an email to your Director stating your business need, timespan needed (i.e. ongoing or specific timeframe) and the web address link.
- 2) Requestor's Director should forward their approval to ITServiceDesk@fcss.us.
- 3) IT will then contact the internet service provider and process the request.