

ORC:
OAC:
COA:
CFSR:
Board:
Other: _____

Next Review Date: 8/2023
Last Reviewed: 07/2020
Review Responsibility: Executive Council

FCCS PROCEDURE

NO.: 12C.01

SUBJECT: Responsible Use of Technology

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, Aug 31, 2010; Nov 14, 2011; Mar 24, 2014; Sep 6, 2016; Aug. 3, 2020

Responsible for Implementation: All Staff

Franklin County Children Services provides desktop telephones and accessories, personal computers and components, printers and services of Internet access, voice mail and e-mail to staff as work tools. Employee's use of these electronic tools, including Internet traffic and the contents of e-mail and voice mail messages, may be monitored at any time. Employees are responsible for using and maintaining agency-issued technology according to this policy.

Procedures:

Responsible Use

Responsible use includes:

- 1) Accessing only those confidential databases – both internal and external – that contain information that is required for fulfilling job responsibilities. **Accessing SACWIS for reasons other than job responsibilities is a misdemeanor of the fourth degree.**
- 2) Report any malfunctions with electronic equipment or services to a Service Desk Technician at 275-2534.

3) Prohibited actions include:

- a) Receiving, viewing, or sending agency emails on personal devices without the use of Webmail.
- b) When using Webmail, staff are prohibited from downloading attachments to any non-agency issued device.
- c) Connecting personal devices to the FCCS Network or equipment.

- i. Under approved work from home conditions, personal computer monitors via HDMI cords and authorized printers may be connected to agency mobile devices. These exceptions are made based on Information Technology best practices/guidance and Executive Council approval.
 - ii. Personal devices like headsets and earbuds are permissible per policy exception.
- d) Connecting personal devices to FCCS – Trainer/Guest Wireless (non FCCS).
- e) Connecting agency devices to FCCS – Trainer/Guest Wireless (non FCCS).
- f) Allowing anyone other than authorized staff approved for access (i.e., FCCS employees, student interns, and contractors) to use electronic equipment or services.
- g) Trading the equipment with other employees, student interns or contractors.
- h) Moving any equipment such as desktop computers, monitors, and desktop telephones.
- i) Disassembling the equipment for any reason, including attempting to repair it.
- j) Installing additional hardware components such as sound cards and video cards.
- k) Installing additional software, including free applications, screen savers, add-on toolbars and instant messaging applications.
- l) Spilling food or beverages on the equipment.
- m) Using diskettes, flash drives, CDs or DVDs that are not agency issued.
- n) Etching, marking on or adhering non-removable stickers to the equipment.
- o) Keeping equipment after separation from the agency.

4) Public Record Request

- a) Using agency-issued technology responsibly requires respecting Ohio's public records laws, which provide citizens with the right to access many but not all, documents from public agencies. In response to public record requests, the Executive Director will work with staff from the Legal and IT

Departments to determine what information our technology is capable of providing and which information the law dictates we must provide, which information we must protect and which information can be disclosed at our discretion.

- b) On issues where we have discretion, the agency's guiding philosophy will be to share information if it is requested. Agency-issued equipment and services are intended to be used primarily for business purposes; therefore, any staff member who chooses to use the equipment or services for personal reasons is advised that this philosophy extends to all work, whether professional or personal, conducted using agency-issued equipment or services. In addition, any personal use must be limited and must not:
 - i) Interfere with or delay fulfillment of job responsibilities.
 - ii) Cause congestion, damage or disruption of services.
 - iii) Involve solicitation.
 - iv) Be associated with any for-profit outside business activity.
 - v) Involve any chain letters or similar type messages.
 - vi) Involve any material that might compromise our ability to maintain a work environment that is free of discrimination or harassment based on a person's protected status, such as race, religion, creed, color, national origin, sex, marital status, age, handicap, disability, sexual orientation, membership in the uniformed service, political affiliation, Federation membership or legal activity.
 - vii) Be associated with any political activities.

5) Security Requirements for Working away from the Office

- a) To safeguard the confidentiality of our clients' data, staff members who access FCCS webmail and/or SACWIS when away from the office must adhere to the following security requirements:
 - i) Access SACWIS or FCCS webmail only through secured Internet connections.
 - ii) Do not use free, wireless Internet connections such as those available in restaurants, places of business and Franklin County

Children Services Trainer/Guest Wireless (FCCS – Trainer/Guest Wireless).

- iii) If you use wireless Internet connection at home, confirm with your Internet Service Provider that your connection is secure and cannot be accessed by individuals outside your home.
- iv) If you access SACWIS or FCCS webmail through your home computer, you must maintain up-to-date antivirus software.
- v) When using SACWIS away from the office, no reports may be saved to the non-agency computer and no reports may be printed. When using FCCS webmail away from the office, no email that contains client or alleged perpetrator information may be saved to the non-agency computer or printed.
- vi) If you access SACWIS in a setting, including your home, where non-FCCS employees are around, you must position yourself and the computer screen so others cannot view data in SACWIS. If you access FCCS webmail that contains client or alleged perpetrator information, the same requirements apply.
- vii) When you are working from home (or away from the office), you should position yourself in secure environments when confidential conversations with referral sources, clients, etc. are taking place as to prevent the overhearing of confidential information.
- viii) When you are signed on for a SACWIS or FCCS webmail session, do not leave the computer unattended. If you leave the computer, log off of SACWIS or FCCS webmail.
- ix) You may login to the agency network using an agency-issued device or personal device following the IT Guidance when appropriate. Access to SACWIS, FCCS webmail, FCCSTeams, and the intranet are permissible under this policy. Workers must **only** login to the FCCS network via VPN using an agency-issued device over a secure connection.

6) Security Requirements for Storing Files and Data

- a) The storage of proprietary or protected agency information is restricted to agency devices, such as network servers or agency-issued PCs, laptops,

tablet computers, phones and digital cameras. Workers are explicitly prohibited from using personal internet storage and sharing sites for any proprietary or protected agency information, including document files, scanned images, photos, videos, audio, etc.

7) Expectations for Managers

- a) Managers serve as role models regarding the fulfillment of agency policies; therefore, managers are expected to demonstrate strict adherence to the agency's Responsible Use of Technology policy. It would be especially problematic for managers to send any email messages that violate agency policy to their subordinates. For example, supervisors who forward political campaign information of any kind to subordinates are abusing their authority and are setting a poor example for their staff.
- b) Managers have the responsibility to act when they receive inappropriate emails from other agency employees. When managers receive inappropriate emails from someone under their supervision, they are expected to point out the violation of the Responsible Use of Technology policy to the sender and to make clear the expectation that this not happen again. When the email is from someone not under the manager's direct supervision, the responsibility is to notify the employee's supervisor so that he/she will follow up accordingly. In addition, any emails that come to the attention of a manager – whether from a subordinate or other employee – that violate our agency's Discrimination and Harassment policy (Employee Handbook, section 5A) should be sent to the attention of Human Resources.
- c) Staff are responsible for refraining from any actions that may damage agency-issued equipment.

8) Trainer/Guest Wireless

- a) The use of Trainer/Guest Wireless is for contracted trainers and visitors conducting business at FCCS site.
- b) Staff are prohibited from using Trainer/Guest Wireless.

9) Failure to Comply With Responsible Use of Policy

- a) Franklin County Children Services may monitor use of agency-issued electronic equipment and services. Staff who fail to use agency-issued

technology equipment and services responsibly in accordance with this policy may be fined up to the price of the damaged or lost materials, restricted in their use of the services and/or be subject to disciplinary procedures. Any instances of irresponsible use of equipment or services shall be reported to the employee's supervisor for review and possible investigation. Supervisor may contact I.T. when suspected violations occur.