Department of Children's Services

POLICY

7.2 Acceptable Use, Network Access Rights, and Obligations	
Application: All Employees of the Department of Children's Services and all Individuals who have been provided access to any State of Tennessee network.	
Authority: TCA 10-7-301 -10-7-308;10-7-504; 10-7-512; 4-3-1001, et seq.; 4-3-5501, et seq.; 37-5-105 (3); 37-5-106, 39-14-601	**Standards: COA:** PA-RPM 5.01, 5.02, 5.03, 5.05; PA-PRG 4.01, 4.02, 4.03
Original Effective Date: 7/12/2004 Current Effective Date: 10/29/2024	Supersedes: 5/30/2023 Last Review Date: 10/29/24

Glossary:

- Public Records
  - All documents, papers, letters, maps, books, photographs, microfilms, electronic data processing files and output, films, sound recordings or other material, regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any governmental agency. (T.C.A. 107301(6)).
- State-Issued Electronic Device
  - State cell phones, iPads, laptops, computers, or any other form of electronic communication device.

Policy Statement:

All employees, vendors, contractors, or other entities provided access to any Department of Children's Services network, including the intranet, internet, drives, DCS Electronic Record System, emails, state issued electronic devices, and any other internal networks, will utilize such access with professionalism, following policy ***4.3, Employee Code of Conduct***, and any statewide and/or agency policies, protocols, and rules, as well as all state, federal, and local laws, or regulations.

Purpose:

To outline and define the professional standards and expectations to which all employees, vendors, contractors, or other entities provided access to any Department of Children's Services network will adhere to ensure uninterrupted, secure network access by authorized individuals, proper security of sensitive/confidential client and Department information, and proper usage of state networks.

Procedures:

A. State Issued Electronic Devices, Internet, and Network Access

State employees, vendors/business partners/sub-recipients, local governments, and other governmental agencies may be authorized to access state network resources to perform business functions with or on behalf of the state. Only authorized users will be allowed access to any department network, including hardware/software, internet or intranet access, emails, calendars, video conferencing applications, or any other state platform.

1. Users must be acting within the scope of their employment or contractual obligations with the state and must agree to abide by the terms of this agreement.
2. Occasional personal use of state network resources, for activities such as making calls, sending/receiving emails, etc., may occur, though this practice is highly discouraged.
3. All users should be aware that network usage may be monitored, and there is no right to privacy while using a state network.
4. Transactions resulting from the use of electronic devices and/or network issues are the property of the state and subject to state open records laws.
5. Prohibited uses of network resources include, but are not limited to, the following:
   - **a)** Sending or sharing with unauthorized persons any information that is confidential by law, rule, or regulation.
   - **b)** Sending any information that could reasonably be viewed as malicious, obscene, threatening, intimidating, or similarly inappropriate.
   - **c)** Placing or viewing adult content/material on any state network or electronic device.
   - **d)** Installing software that has not been authorized by the Strategic Technology Solutions (STS) division of Finance and Administration.
   - **e)** Removing or deactivating monitoring software or attempting to circumvent security controls in any way.
   - **f)** Attaching processing devices that have not been authorized by STS.
   - **g)** Using network resources and/or electronic devices to play or download games, music, or videos that are not in support of business functions.
   - **h)** Broadcasting audio, video, or other media formats for non-business purposes.
   - **i)** Using network resources and/or electronic devices to engage in or support unlawful activities as defined by federal, state, and local law.
   - **j)** Utilizing network resources and/or electronic devices for activities that violate the ***Rules of the Tennessee Department of Human Resources***, as well as the Department of Children's Services policy ***4.3, Employee Code of Conduct***.
   - **k)** Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
   - **l)** Leaving one's workstation unattended without engaging password protection.

m) Information regarding computer crimes may be reviewed at ***Tennessee Code Section 39-14-601.***

B. Emails, Texting, Teams, Video Conferencing, and Calendar Access

Emails, texting, Teams, video conferencing, and calendar functions are provided to expedite and improve communications among network users.

Emails or messages created, sent, or received in conjunction with the transaction of official business are public records, in accordance with T.C.A 10-7-301 through 10-7-308 and the Rules of the Public Records Commission. State records are open to public inspection unless they are protected by state or Federal law, rules, or regulations. As a court could interpret state records to include draft letters, working drafts of reports, and what are intended to be casual comments, be aware that anything sent as electronic mail or message could be made available to the public.

Prohibited uses of emails, texting, Teams, video conferencing, and calendar functions include, but are not limited to the following:

1. Accessing non-state provided web email services.
2. Emailing or texting protected/confidential data, as protected by the *Health Insurance Portability and Accountability Act (HIPAA),* located at ***PLAW-104publ191.pdf (congress.gov)***, and DCS policies, rules, and regulations regarding confidentiality, found at ***DCS Policies & Procedures (tn.gov)***, to their personal email accounts or personal devices.
3. Storing personal information, media (videos, photographs, audio recordings, etc.), or any other non-state or work-related data.
4. Instant messaging, texting, or Internet Relay Chat (IRC) that is not occurring via a state/DCS approved internet-based platform, such as Teams or Webex.
5. Sending unsolicited junk email or chain letters (i.e. “spam”) to any users of the network.
6. Any material that contains viruses or any other harmful or damaging programs.
7. Copyrighted materials via email or message that are not within the fair use guidelines or without prior permission from the author or publisher.
8. Communications that violate the ***Rules of the Tennessee Department of Human Resources***, as well as the Department of Children’s Services policy ***4.3, Employee Code of Conduct***.
9. Confidential material to an unauthorized recipient or sending confidential emails or messages without the proper security standards (including encryption, if necessary) being met.

C. Use of Technology in Contacting Families and Providing Services

Video conferencing and other technology may be used with clients under certain circumstances for convenience and safety and must follow the guidelines listed below. It's to be noted that clients may request for services, contacts, and/or meetings to be held in person or by phone, if that is the preference. See ***Protocol for Social Media Usage to Contact Clients*** for guidance in the use of social media.

1. When video conferencing/technology-based contact is initiated by DCS, the DCS employee must use a *HIPAA* compliant platform (such as Teams or Webex).
2. If a HIPAA compliant platform is unavailable, then the DCS employee may use a non-HIPAA compliant platform but may *not* discuss HIPAA protected information on said platform.
3. Facetime may be utilized, if Teams or Webex is unavailable, from a state-issued electronic device for a DCS worker-child visit.
4. Employees must assess the appropriateness of technology-based service delivery and monitor its effectiveness with the family served.
5. When technology-based service delivery is found to be ineffective for a DCS served family, the employee must arrange for in-person service delivery.
6. Employees must ensure the following is completed prior to initiating technology-based service delivery:
   - **a)** Service recipients are advised of the risks and benefits of using technology-based service delivery.
   - **b)** Recipients are informed of the conditions for which in-person service delivery would be referred.
   - **c)** Service recipients are provided with the employee's contact information, location, and credentials.
   - **d)** Instructions and information on how to access the utilized technology-based platform is provided to the service recipient.
   - **e)** The DCS Employee will discuss any privacy and confidentiality limitations associated with technology-based communications and will review and have the service recipient acknowledge the confidentiality statement on Form ***CS-0747 Child and Family Team Meeting Summary (CS-0747)*****.**

D. Storing Electronic Information

1. All business-related electronic information created by users is stored on a network drive. This includes shared drives such as the F, L, or M drives, SharePoint, or an employee's OneDrive. Information should never be stored on an employee's desktop computer drive (commonly referred to as the C: drive). Business-related information can be considered, but not limited, the following:
   - **a)** Child Welfare Data.
   - **b)** Archived Business emails.
   - **c)** Archived Chat messages sent via official State of TN messaging channels.

d) Office 365 files created for business related work.
e) Recorded Meetings required to be retained past the 14-day STS retention period.

2. Users understand that the storage of electronic information on the desktop computer drive (commonly referred to as the C: drive) is highly susceptible to loss.
3. Users understand that the storage of electronic information on the network drive is secure and is backed-up on a nightly basis to avoid disruptions to state government activities resulting from inappropriate storage of electronic information.
4. The user will utilize this default setting for the storage of all electronic information that is vital to the business of the Department of Children's Services.
5. In the event that it is desirable to temporarily store electronic information outside of the network drive location, the user must accept the risk that any electronic information that is lost is most likely not recoverable.
6. DCS Internal Affairs and DCS Internal Audit may utilize removable media (USB/ external hard drives, compact disks, audio tapes, paper, etc.) for the storage of extremely sensitive information. The removable media should have a backup in the event of unrecoverable damage to the original.

Forms:

CS-0747 Child and Family Team Meeting Summary

Collateral Documents:

4.3, Employee Code of Conduct

Protocol for Social Media Usage to Contact Clients