

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
July 2, 2015 – P.T. 2015.19

Section

20.1	Purpose
20.2	Definitions
20.3	Permissible uses of Electronic Mail, Internet, and Data Distribution Function
20.4	Transmission of Confidential Information
20.5	Prohibited Uses of Electronic Mail
20.6	State Computer Equipment Usage
20.7	Use of Unauthorized Equipment
20.8	Prohibited Uses of the SACWIS and Any Other Search Function
20.9	Statewide Business Related Announcements
20.10	Department Monitoring, Access and Disclosure
20.11	Security and Confidentiality
20.12	Maintenance of Electronic Mail
20.13	Policy Enforcement
20.14	Policy Acknowledgement
Appendix A	Electronic Mail/Internet Usage/SACWIS Search Function and Distribution Certificate of Understanding

20.1 Purpose

The purpose of this Administrative Procedure is to establish the Department’s policy regarding the access, use, maintenance and disclosure of electronic communication, and data distribution, which includes, but is not limited to, electronic mail and Internet usage. Electronic mail or E-mail has become an essential method of communication that is accessible to all Department of Children and Family Services (DCFS) staff. The Department encourages and supports the use of E-mail to facilitate timely and efficient business-related communications; however, there are some basic principles that govern the use of electronic communication and data distribution.

- The Department’s electronic mail and Internet systems should be used only for business-related communications and research.
- Department employees and other authorized users should have no expectation of privacy in anything they access, create, store, send or receive when using the Department’s electronic mail and Internet systems.
- All users of the Department’s electronic mail and Internet systems are required to use these resources in a responsible, professional, ethical and lawful manner.
- E-mail or Internet, used inappropriately, could result in lawsuits, costly litigation and/or employee discipline.
- The sending of E-mail does not absolve the sender from communicating orally with the recipient on critical job-related matters or tasks.

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
July 2, 2015 – P.T. 2015.19

Electronic Data Distribution

- Data distribution standards and methodologies shall be implemented or approved by the Office of Information Technology Services (OITS).
- Data distribution standards and methodologies will be observed at all times to ensure the quality and security during delivery.
- Data movement via physical devices such as flash, removable hard drives, tape, etc. shall meet with OITS approval.

Virtual Private Network (VPN)/Remote Access

- Secured internet access into the DCFS network must be requested from and approved by OITS and the user's business manager/supervisor. Upon approval, OITS will provide client (local computer) software and permission. Approval may be requested by contacting the OITS Help Desk.
- Usage is restricted to DCFS employee's or contracted business partners, to utilize for access to DCFS applications and services only.
- Any and all VPN/remote connectivity constitutes an acceptance of the "acceptable use policies" of DCFS and its information and computing systems. All VPN connections are subject to investigation, monitoring.

20.2 Definitions

CYCIS (Child and Youth Centered Information System) – confidential information of persons served by the Department of Children and Family Services is stored in the CYCIS database.

Electronic Mail System - the State's messaging system that depends on computing equipment to create, send, forward, receive, reply to, transmit, store, hold, copy, view, print, and read electronic mail.

Electronic Mail (E-mail) - any electronic computer document or message created, sent, forwarded, received, replied to, transmitted, stored, copied, downloaded, displayed, viewed, read, or printed via the Internet or Intranet.

FTP – a communications protocol governing the transfer of files from one computer to another over a network.

Internet - a group of independent, self-defined, and self-contained computer communication areas. Internet connections enable access to the Internet (a.k.a. the World Wide Web) when appropriate software has been installed on a workstation.

Intranet - a self-contained computer communication network that is strictly internal to the Department and authorized users.

MARS (Management and Accounting Report System) – confidential information of persons served the Department of Children and Family Services is stored in the MARS database.

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
July 2, 2015 – P.T. 2015.19

Remote Access (RAS) – a dial up method of access to the DCFS network using modems and phone lines.

SACWIS means the (State Automated Child Welfare Information System) - Confidential information of persons served by the Illinois Department of Children and Family Services is stored in the SACWIS database.

SACWIS search function - the mechanism by which authorized SACWIS users may retrieve information maintained in the Department's database regarding child abuse and neglect investigations, child welfare service cases, and related information involving mandated reporters and Department personnel.

“Social Media” means current and future interactive technologies including, but not limited to, text, audio, video, images, podcasts, and other multimedia communications, in virtual communities and online networks.

VPN – a virtual private network that provides a means to access the DCFS network from other networks outside of DCFS.

20.3 Permissible Uses of Electronic Mail, Internet, Department Social Media Accounts, and Data Distribution

a) Authorized Users

Only Department staff, authorized contractual staff, and private agencies using the DCFS network are considered authorized users of the Department’s electronic mail, Internet systems, and other data distribution methods. Department social media accounts may only be used by authorized staff. Each Department social media account will be monitored by an individual site contact person, who will be designated as such by OITS. Each site contact person for a Department Facebook account must sign as **CFS 123-1, Facebook Site Contact Agreement**.

b) Purpose of Use

1) Electronic Mail and Internet

Internet usage, electronic mail, or the use of any Department resources for electronic mail should be related to Department business. This includes union-related business as stipulated in the agreements between the Department of Central Management Services and the applicable collective bargaining entities.

2) SACWIS, CYCIS, MARS, and Other Search Function

The SACWIS, CYCIS, MARS, and other search function shall be limited to use by authorized persons that have need of specific database information for the accomplishment of assigned case management functions.

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
July 2, 2015 – P.T. 2015.19

3) Department and Personal Social Media Accounts

Acceptable uses of the Department's Facebook account by authorized, include, but are not limited to:

- Locating parents and missing children;
- Sending messages to missing children in care in an effort to locate them;
- Sending messages to family members of children in care, provided confidentiality is maintained;
- Monitoring the Facebook page of any youth in care;
- Monitoring the Facebook page of the caregiver or parent of any child in care for anything that may impact the child's safety;
- Determining if parents are violating safety plans or orders of protection;
- Determining if parents are using drugs or alcohol;
- Determining if parents are making online threats toward DCFS or others;
- Determining if parents or children are posting inappropriate messages;
- Determining if alleged perpetrators of sexual abuse or child pornography are having contact with minors; or
- Determining if inappropriate pictures are being posted.

Prohibited uses of Department social media accounts, include, but are not limited to:

- Using the Department's Facebook account for personal purposes;
- "Friending" or otherwise inviting clients to be part of the Department's social media account;
- Posting any information, or contacting anyone through social media, in a way that may be construed as a violation of confidentiality per **Rule and Procedure 431, Confidentiality of Persons Served by the Department**; or
- Posting anything related to the client.

Prohibited uses of employees' personal social media accounts, include, but are not limited to:

- Using a personal account to correspond with clients via messaging or posting to clients' accounts;
- "Friending" or otherwise inviting clients to be part of the employee's personal social media account;
- Posting any information, or contacting anyone through social media, in a way that may be construed as a violation of confidentiality per **Rule and Procedure 431, Confidentiality of Persons Served by the Department**; or
- Posting anything related to the client.

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
July 2, 2015 – P.T. 2015.19

20.4 Transmission of Confidential Information

Confidential information may be transmitted only as authorized under **Rules and Procedures 431, Confidentiality of Personal Information of Persons Served by the Department of Children and Family Services**. Information related to the Comprehensive Medicaid Billing System and Medicaid Community Mental Health Services shall remain confidential and may only be transmitted by authorized persons in accordance with Rules and Procedures 431, Procedures 359, Appendix H, Medicaid Community Mental Health Services Program and Policy Guide 2003.05 (Health Insurance Portability and Accountability Act).

Additionally, any transmission of confidential information via the internet must include the statement:

“PRIVILEGED AND CONFIDENTIALITY NOTICE: This email (and/or the documents accompanying such) may contain privileged/confidential information. Such information is intended only for the use of the individual or entity above. If you are not the named or intended recipient, you are hereby notified that any disclosure, copying, distribution, or the taking of any action in reliance on the contents of such information is strictly prohibited. If you have received this transmission in error, please immediately notify the sender by telephone to arrange for the secure return of the document.”

Note: Section 20.5 lists specific information the department prohibits sending via the internet.

20.5 Prohibited Uses of Electronic Mail or Internet

Displaying or disseminating materials that can be considered by some people to be obscene, racist, sexist, or otherwise offensive may constitute harassment by creating a hostile work environment. Accessing non-business related Internet sites may subject the user to discipline, up to and including discharge. Furthermore, unintended usage or unauthorized access or interference may subject the employee and/or the Department to legal action. Consequently, the Department requires appropriate standards of conduct to be employed when using electronic mail or Internet.

Specific prohibited uses of electronic mail include, but are not limited to:

- Using electronic mail systems for any purpose restricted or prohibited by State and Federal laws or regulations;
- Sending electronic mail that is considered offensive to any individual or group or accessing Internet websites for non-business purposes;
- Including inspirational quotations, religious verses, or other non-business related information in the body, signature block, or beneath the signature block of the e-mail is prohibited. Staff may only use their name, contact information, and appropriate confidentiality notice in their signature block if they choose;

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
July 2, 2015 – P.T. 2015.19

- Transmitting, via the Internet, case-related information such as, but not limited to, case notes, correspondence or documents in violation of Rules and Procedures 431. Personal information of persons served by the Department shall not be transmitted using the Internet, except as approved in writing by the Director or Chief Legal Counsel for purposes of automated E-mail reminders of juvenile court hearings and case reviews. No confidential information shall be contained in an Internet E-mail message, listed in a “chat room,” or otherwise referenced in any Internet communication. Personal information of persons served by the Department may be transmitted via Outlook E-mail to other Illinois state agencies when the disclosure is in accordance with Rules and Procedures 431, and the information is sent through the DCFS Outlook E-mail system by selecting the other Illinois state agency employee’s name from the Outlook Global Address List. Any other method of addressing an E-mail, including typing in the state employee’s full E-mail address, may result in the E-mail being transmitted via the Internet, which is prohibited;
- Transferring or downloading any confidential information onto user-owned personal computers, flash drives or other removable media or email is prohibited;
- Transmitting confidential personnel, employee discipline, or employee evaluation-related information unless necessary as part of the employee’s job duties within the Department;
- Sending copies of documents in violation of copyright laws;
- Unauthorized intercepting and opening of electronic mail except as required in order for authorized employees to diagnose and correct delivery problems or to monitor usage in accordance with this Administrative Procedure, or for authorized investigations pursuant to Rule 430 or other appropriate Department purposes;
- Using electronic mail to harass or intimidate others or to interfere with the ability of others to conduct Department business;
- Accessing or attempting to access websites for non-business purposes that are sexually explicit, demeaning or exploitive of minors, women or minorities or otherwise counter to the purposes of the Department;
- Unauthorized use of an individual’s E-mail account other than for monitoring or investigative purposes consistent with this Administrative Procedure or Rules 430;
- Constructing an electronic mail communication so it appears to be from someone else;
- Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmissions without proper authorization;
- Downloading and installing of unauthorized software;
- Using the E-mail or Internet system to conduct statewide mailings for notifications of births, deaths, illness, parties and social events;
- Using E-mail or Internet for other such non-business related matters;
- Including non-business related graphics within an E-mail message;
- There is a presumption that the use of chat rooms is non-business related; or
- Unauthorized use of Internet access is not limited to business hours. DCFS equipment cannot be used for non-business purposes.

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
July 2, 2015 – P.T. 2015.19

20.6 State Computer Equipment Usage

Desktop computers, laptop computers, printers, and other equipment that is issued to employees should only be used for State business. Misuse of DCFS/State equipment may result in disciplinary action up to and including dismissal.

Unauthorized use of State property is prohibited. Staff should not lend any computer equipment that was issued to them.

Proper care should be taken in the use of State owned equipment. It is prohibited to damage or expose State owned computer equipment to any condition that might cause damage.

Files/data of a personal nature such as music, photos/pictures, and movies should not be loaded, run, printed or viewed on State property. OITS has the right and will remove these files on discovery.

Unauthorized programs/applications that were not authorized and issued by DCFS OITS should not be loaded or run on State equipment. This includes screen savers, add-on graphics/fonts, slideshow applications, or any other application that was not authorized/issued and installed by DCFS OITS. OITS has the right and will remove these files on discovery.

20.7 Use of Unauthorized Equipment

It is prohibited to connect non-State owned computer equipment to the DCFS Network without written authorization from DCFS OITS. This includes personal computers, hubs, switches, printers, scanners, storage devices, and other peripherals.

Add-on equipment such as storage devices, cameras, printers, or other peripherals should not be installed/connected to State property unless authorized and installed by DCFS OITS technicians.

20.8 Prohibited Uses of the SACWIS and Any Other Search Function

Purposes for which the SACWIS search function and any other electronic means may not be used include, but are not limited to the following:

- The SACWIS search function may not be used by persons other than those authorized by the Department.
- The SACWIS search function may not be used to retrieve database information for purposes other than the accomplishment of assigned duties.
- Information obtained via a SACWIS search shall not be transmitted using the Internet or contained in an Internet E-mail message, listed in conversation in a “chat room,” or otherwise referenced in any Internet communication.

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
July 2, 2015 – P.T. 2015.19

20.9 Statewide Business-Related Announcements

Business-related announcements to all Department users, must be directed to the following E-mail address: ANNOUNCEMENTS. Include in the first line of the message the date that you wish the announcement to be sent.

E-mail sent to this address will be reviewed for appropriateness prior to distribution. The submitter will be contacted, if necessary, to discuss any issues with the announcement. Allow a minimum of one business day for distribution. Emergency announcements should be marked URGENT and include in the first line an explanation of the situation creating the emergency. (Note: This will be removed prior to distribution.)

20.10 Department Monitoring, Access and Disclosure

Electronic mail created or stored on Department equipment or Internet usage constitutes a Department record and is subject to the disclosure laws of the State of Illinois. The Department reserves the right to monitor, access and disclose contents of electronic mail or internet usage without the consent of the originator or the recipient of the correspondence.

The SACWIS search and the information developed from the search that is stored on Department equipment constitutes a Department record and is subject to the disclosure laws of the State of Illinois. The Department reserves the right to monitor, access and disclose contents of searches without the consent of the originator of the search.

20.11 Security

Users are advised that electronic mail messages that are transmitted, received, or stored on the Department's electronic mail systems are the property of the Department, and as such, may be considered public records. All Internet sites accessed and attempts to access are subject to monitoring by the Department. The SACWIS search and the information developed from the search that is stored on the Department's electronic systems are the property of the Department, and as such, may also be considered public records.

All Department electronic mail and Internet usage that connects to the Internet, Outlook, or AS400 systems passes through the Department of Central Management Services' (CMS) computer network. Both CMS and DCFS conduct regular back-ups of their electronic mail files. Even though the sender and recipient have discarded or deleted their copies of an electronic mail record, there may be back-up copies, either at DCFS or CMS that can be retrieved as the result of discovery requests in the course of litigation or other official inquiry.

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
July 2, 2015 – P.T. 2015.19

20.12 Maintenance of Electronic Mail

All electronic records will be maintained according to the rules and timeframes set forth by the State Records Commission and the Department. Staff should preserve essential electronic business records through archiving documents on their workstation or through conventional filing and maintenance.

The Department will maintain a back-up copy of deleted E-mail transactions for 30 days, at which time they will be removed from the system. A back-up copy of the E-mail journal will be taken every 30 days of all E-mail transactions occurring in that 30-day period and will be retained for five years.

20.13 Policy Enforcement

Violations of Department E-mail or data distribution policies will subject employees to disciplinary action up to and including discharge.

20.14 Policy Acknowledgement

Users of the Department's electronic mail system and/or SACWIS search function *must* sign a **CFS 123 (Electronic Communication and Distribution Certificate of Understanding)** acknowledging that they have read and understand the conditions and terms of this agreement (See Appendix A). The signed copy is to be maintained in the employee's on-site personnel file for all DCFS and POS users and a copy sent to the Office of Employee Services for inclusion in the employee's personnel file for all DCFS users. Failure to sign a CFS 123 will result in loss of network privileges.

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
July 2, 2015 – P.T. 2015.19

This page intentionally left blank.

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
July 2, 2015 – P.T. 2015.19

APPENDIX A

CFS 123
Rev 2/2011

State of Illinois
Department of Children and Family Services

**ELECTRONIC MAIL COMMUNICATION AND DISTRIBUTION CERTIFICATE OF
UNDERSTANDING**

- 1) I acknowledge that I have read Administrative Procedure #20, Electronic Communication and Distribution, and that I am responsible for abiding by the policies contained, therein.
- 2) I understand that the use of computer equipment, software and the electronic mail system is for State of Illinois business only.
- 3) I understand that unauthorized transmittal of confidential information via the electronic mail system is prohibited.
- 4) I understand that only non-confidential information may be transmitted across the Internet (outside the Department's Outlook E-mail system) and that I may never use specific names of wards (except as approved in writing by the Director or Chief Legal Counsel for purposes of automated E-mail reminders of juvenile court hearings and case reviews), perpetrators, witnesses, or any other persons served by the Department in an Internet E-mail message, listed in conversation in a "chat room," or otherwise referenced in any Internet communication.
- 5) I understand that, in order to maintain confidentiality, the Department prohibits transferring or downloading any confidential information onto personal computers or email.
- 6) I understand that information obtained via a SACWIS search shall not be transmitted using the Internet or contained in an Internet E-mail message, listed in conversation in a "chat room," or otherwise referenced in any Internet communication.
- 7) I understand that electronic mail records are considered Department business records subject to Federal and State freedom of information laws and official State of Illinois record retention rules.
- 8) I understand there is no expectation of privacy in any E-mail, Internet or SACWIS search document I create, store, send, or receive when using the Department's electronic mail and Internet systems.
- 9) I understand that Internet access is limited to only those areas directly related to State business and that I must refrain from accessing, displaying or creating any offensive, malicious or illegal material.

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
July 2, 2015 – P.T. 2015.19

- 10) I understand that downloading from or uploading to the Internet copyrighted material that will then be distributed to other individuals is prohibited.

- 11) I understand that a violation of this policy may result in disciplinary action, up to and including possible discharge, as well as civil and criminal liability that my action may create.

Signature: _____ Date: _____

Printed Name: _____

Work Location: _____