Cuyahoga County Division of Children and Family Services (CCDCFS)
Policy Statement

Policy Chapter:	**Information Services**
Policy Number:	**12.05.07**
Policy Name:	**Electronic Communications and Information Technology (IT) Resource Usage**

Original Effective Date:	07/19/1999
Revision Date(s):	04/01/2013, 04/19/2006
Current Revision Date:	04/01/2016
Approved By:	Thomas D. Pristow

PURPOSE: To establish controls and provide guidance in understanding the proper use of County and/or State-provided electronic communications services and information technology (IT) resources to ensure they are appropriately and professionally used for the purposes for which they are acquired.

SCOPE: This policy applies to all Cuyahoga County Division of Children and Family Services staff, contract employees, temporary employees, and other agents of the county and/or state who use and administer such electronic communication services and IT resources.

POLICY

Cuyahoga County and/or the State of Ohio furnishes a variety of electronic communication services and IT resources to employees, contractors, temporary personnel and other agents of the county and/or state in order to conduct the business of the county and/or state. Great care is required to prevent misappropriation of publicly-owned IT resources. This policy provides guidelines for the usage of the electronic communication services and IT resources.

PROCEDURES

A. **Use of county and/or state provided IT resources.** Cuyahoga County and/or State of Ohio provides computers, electronic communication services, software, supplies and other IT resources to employees, contractors, temporary personnel, and other agents of the county and/or state for supporting the work and conducting the affairs of Cuyahoga County and the State of Ohio. Personal use is strictly prohibited.

B. **Users are responsible for electronic communications and transactions made with their USERID and PASSWORD.**

1. Employees should not disclose their password to others. However, in the event the user is unavailable and there is a compelling need to access the user's files, management can request access to the user's account by asking the Information Services staff to reset the user's password.

2. When an employee leaves the work area for the day, s/he must SIGN OFF from all programs and LOG OUT of all network connections. When an employee leaves the work area for the weekend or for two days or more, s/he must SIGN OFF from all programs, LOG OUT of all network connections and SHUT DOWN the COMPUTER/PC.

3. All staff shall be required to check (and open) their email no less than twice per day, unless they are not in the office for the day.

4. Access to, and use of, county and/or state provided electronic communications equipment and services are provided at the discretion of the county and/or state and may be revoked at will.

C. **Unacceptable Personal Use.** Any personal use of IT resources that disrupts or interferes with government business, incurs an undue cost to the Agency and/or State, could potentially embarrass or harm the Agency and/or State, or has the appearance of impropriety is strictly prohibited. Personal use that is strictly prohibited includes, but not limited to, the following:

1. **Unauthorized Installation or Use of Software.** Installing or using software including, but not limited to, instant messaging clients, peer to peer file sharing software, personally owned software, or non-approved USB drives, is strictly prohibited. Installation and use of unlicensed software is strictly prohibited. USB drives must be approved by Information Services and in accordance with State policies and guidelines.

2. **Unauthorized Installation or Use of Hardware.** Installing, attaching, or physically/wirelessly connecting any kind of hardware device to any county and/or state provided IT resource, including computers, laptops, and network services is strictly prohibited without prior approval from the user's Department Manager and Information Services staff. This includes, but not limited to, music devices, cellular devices, portable computers, electronic readers, and personally-owned CD's. Connecting or attempting to connect a wireless device to county and/or state wireless services without proper agency approval is strictly prohibited. USB drives must be approved by Information Services and in accordance with State policies and guidelines.

3. **Restrictions on Internet Use.** Users shall not stream audio and/or video on county and/or state IT supplied resources with the exception of conducting official business that includes, but not limited to Webinar

participation. Users shall not utilize or access Internet file storage areas or programs on county and/or state IT supplied resources.

4. **Violation of Law.** Violating or supporting and encouraging the violation of Local, State, or Federal law is strictly prohibited.

5. **Illegal Copying.** Downloading, duplicating, disseminating, printing or otherwise using copyrighted materials, such as software, texts, music and graphics, in violation of copyright laws is strictly prohibited.

6. **Operating a Business.** Operating a business, directly or indirectly, for personal gain is strictly prohibited.

7. **Accessing Personals Services.** Accessing or participating in any type of personals ads or services, such as or similar to dating services, matchmaking services, companion finding services, pen pal services, escort services, or personal ads is strictly prohibited.

8. **Accessing Sexually Explicit Material.** Downloading, displaying, transmitting, duplicating, storing or printing sexually explicit material is strictly prohibited.

9. **Harassment.** Downloading, displaying, transmitting, duplicating, storing or printing material that is offensive, obscene, threatening or harassing is strictly prohibited.

10. **Gambling or Wagering.** Organizing, wagering on, participating in or observing any type of gambling event or activity is strictly prohibited.

11. **Mass Emailing.** Sending unsolicited emails or facsimiles in bulk or forwarding electronic chain letters in bulk to recipients inside or outside the county and/or state email domains is strictly prohibited.

12. **Solicitation.** Except for agency approved efforts, soliciting for money or support on behalf of charities, religious entities or political causes is strictly prohibited.

13. **Impeding Access.** Impeding the County's and/or State's ability to access, inspect and monitor IT resources is strictly prohibited. A user shall not encrypt or conceal the contents of any file or electronic communications on county and/or state computers without proper authorization. A user shall not set or manipulate a password on any county and/or state computer, program, file or electronic communication with proper authorization.

14. **Misrepresentation.** Concealing or misrepresenting one's name or affiliation to mask unauthorized, fraudulent, irresponsible or offensive behavior in electronic communications is strictly prohibited.

15. **Restriction on the use of Email Address.** Users shall avoid the appearance of impropriety and avoid the appearance of leveraging the stature of the county and/or state in the use of their assigned county and/or state email address. County and/or state email addresses shall not be used for personal communications in public forums such as or similar to listservs, discussion boards, discussion threads, comment forums, or blogs (web logs).

16. **Violation of Systems Security Measures.** Any use of county and/or state provided IT resources that interferes with or compromises the security or operations of any computer system, or compromises public trust, is strictly prohibited.

17. **Confidentiality Procedures.** Using IT resources to violate or attempt to circumvent confidentiality procedures is strictly prohibited.

18. **Accessing or Disseminating Confidential Information.** Accessing or disseminating confidential information or information about another person without authorization is strictly prohibited.

19. **Accessing Systems without Authorization.** Accessing networks, files, or systems or an account of another person without proper authorization is strictly prohibited. Users are individually responsible for safeguarding their passwords.

D. **No Expectation of Privacy.** This policy serves as notice that users shall have no reasonable expectation of privacy in conjunction with their use of county and/or state provided IT resources. Contents of computers may be subject to review, investigation and public disclosure. Access and use of the Internet, including communication by email and the content thereof, is not confidential, except in certain limited cases recognized by state or federal law. The county and/or state reserves the right to view any files and electronic communications on county and/or state computers, monitors, and log all electronic activities, and report finding to appropriate supervisors and authorities.

E. **Penalties.** Violation of this policy may result in disciplinary action or contractual penalties, and may be cause for termination. In addition, users who violate the policy may be subject to a civil action or criminal prosecution as a result of inappropriate use or misuse or IT resources. The Ohio Revised Code (ORC) makes certain misuses of IT resources criminal offenses:

a. ORC Section 2909.04 – knowingly using a computer system, network, or the Internet to disrupt or impair a government operation.

b. ORC Section 2909.05 – causing serious physical harm to property that is owned, leased, or controlled by a government entity.

c. ORC Section 2913.04 – accessing without authorization any computer, computer system, or computer network without consent of the owner.

d. ORC Section 2921.41 – using a public office to commit theft which includes fraud and unauthorized use of government computer systems.

Each employee must acknowledge reading and understanding this policy/procedure statement (and the related Electronic Communications Equipment policy/procedure statement, #12.05.06) by signing and dating the Acknowledgement Form.

1. The Human Resources Department will be responsible for collecting and placing in each employee's Personnel File a copy of the signed/dated Acknowledgement Form.

2. A copy of the Acknowledgment Form is accessible via DCFS agency intranet's Forms/IT Forms section.

SEE ALSO:

Related County and State Policies

This policy is an adaptation of Cuyahoga County Department of Information Technology (DoIT) Policy 2-1-99 and Acceptable Use of Government Office Equipment and the Internet 2005; and an adaptation of the State of Ohio, Office of Information Technology Policy Number ITP-.8, Effective 3/20/2006.

Cuyahoga County Division of Children and Family Services Policies and Procedures Manual

Policy 7.04.01: Sharing and Dissemination of Confidential Client Information
Policy 12.05.06: Electronic Communications Equipment

FORM

Electronic Communications Policy/Electronic Communications Equipment Policy Acknowledgement Form