WASHINGTON STATE
Department of
Children, Youth, and Families

Administrative Policy

Chapter 12 Information Technology
12.04 Acceptable Use of Information Technology Resources and the Internet

Original Date: August 26, 2020
Revision Date:
Sunset Review Date: August 31, 2024
Approved by: Frank Ordway, Chief of Staff

Purpose

The purpose of this policy is to outline rules for the appropriate use of the Department of Children, Youth, and Families' (DCYF) information technology (IT) resources.

Scope

This policy applies to DCYF employees, volunteers, interns, and work study students who access DCYF IT resources.

Laws

Chapter 9A.80.010 RCW	Official Misconduct
Chapter 42.52 RCW	Ethics in Public Service
Chapter 42.56 RCW	Public Records Act
Chapter 43.105 RCW	Consolidated Technology Services Agency
RCW 43.105.215	Security standards and policies-State agencies' information technology security programs.

Policy

1. DCYF must follow state laws, Office of the Chief Information Officer (OCIO) requirements, and DCYF Administrative 12.01 IT Security policy when using state-issued IT resources.
2. DCYF may search, access, collect, or distribute public records without notice to employees, volunteers, interns, and work study students per chapter 42.56 RCW and the DCYF Administrative 13.05 Public Records Requests and Disclosure policy.
3. Employee, volunteers, interns, and work study student's must:
    a. Comply with the following when creating records on state-issued devices:
        i. DCYF Administrative 13.05 Public Records Requests and Disclosure policy
        ii. Chapter 42.56 RCW
        iii. Discovery
        iv. Record retention schedules
    b. Use state-issued IT resources, e.g., software, agency applications, IT services, the intranet or internet for business purposes only, unless allowed by WAC 292-110-010 or the DCYF Administrative 11.21 Ethics and Employee Conduct policy for limited personal use.

c. Follow the DCYF Administrative 12.01 IT Security policy and the IT Security Manual.
d. Not connect personal devices, e.g., mobile devices, tablets, laptops, etc., to the DCYF guest Wi-Fi. DCYF guest Wi-Fi may only be accessed by contractors, vendors, and business partners.
e. Use the agency-approved virtual private network (VPN) solution when accessing DCYF IT resources remotely.
f. Use agency-approved secure email when sending emails containing confidential and sensitive information to individuals outside of DCYF.
g. Protect mobile IT resources from theft or damage. Mobile devices must be secured and not left unattended in the view of the public.
h. Notify contracted service providers of their requirement to use DCYF IT resources for business purposes only and as required by their contract.

Procedures

1. Using State-Issued IT Resources
    a. Employees, volunteers, interns, and work study students using state-issued IT resources must:
        i. Complete the following trainings in the WA State Learning Center as required in the Mandatory Trainings by all State Employees:
            A. DCYF Information Security Awareness
            B. WA-State Ethics in State Government
        ii. Password protect all computers and mobile devices when not in use.
        iii. Store DCYF records only on state-issued devices per the DCYF Administrative 13.06 Records Management and Retention Procedures policy.
    b. Employees, volunteers, interns, and work study students needing and requesting remote access to DCYF networks must:
        i. Complete the:
            A. IT Remote Access Request and Agreement DCYF 17-443 form.
            B. Nondisclosure of Confidential Information DCYF 03-374 form.
            C. Mobile Work/Telework Agreement DCYF 03-500 form.
        ii. Submit the completed form to their supervisor.
    c. Supervisors with workers requesting remote access to DCYF networks must:
        i. Verify the following are completed at the time of request:
            A. Trainings in the procedures section 1.a.i, as required.
            B. Review and approve forms in the procedures section 1.b.i.A-C.
        ii. Comply with the DCYF Administrative 11.10 Modern and Mobile Workplace policy.
        iii. Send the completed and approved IT Remote Access Request and Agreement DCYF 17-443 forms to the service desk.
    d. IT employees that receive approved IT Remote Access Request and Agreement DCYF 17-443 forms must:
        i. Process the requests.
        ii. Provide the IT resources to the requesters.
2. Permitted Business Use of IT Resources, Including the Internet and Intranet
Employees, volunteers, interns, and work study students:

a. Completing their work duties must only use state-issued IT resources, including but not limited to:
    i. Laptops, tablets, mobile devices, desk phones, computers, etc.
    ii. Copy machines and printers
    iii. Fax services
    iv. Agency-installed software and applications
    v. Video conferencing equipment
b. Accessing or using Wi-Fi connections on IT resources:
    i. Must only connect to DCYF Employee Wi-Fi in DCYF offices and hotspots from their agency issued resources.
    ii. Must only use DCYF email systems, accounts, or websites needed to perform business functions. Accessing websites for reasons other than business is prohibited.
    iii. May access public Wi-Fi, e.g., Starbucks, McDonalds, libraries, or in employees' homes, using the approved VPN, but must not access personal Wi-Fi provided by a client or caregiver.

3. Emails Containing Sensitive and Confidential Information
   Employees, volunteers, interns, and work study students sending emails to individuals outside of DCYF containing confidential information classified as category 3 or 4, must:
    a. Enter "[secure]" as the first word in the subject line, followed by additional non-identifying text.
    b. Not include any confidential information in the subject line.
4. Prohibited Use of IT Resources
   Employees, volunteers, interns, and work study students must not use IT resources, e.g., mobile devices, software, hardware, agency applications, services, and the internet or intranet:
    a. For activities that are prohibited by federal, state, or local laws, or DCYF policies.
    b. For personal:
        i. Benefit or gain, or benefit or gain for other individuals outside of DCYF per RCW 42.52.160.
        ii. Business interests or to support outside employment.
        iii. Use, to order or sell items on the internet, except as specifically approved for DCYF business purposes.
        iv. Use when participating in online games, social media, gambling, contests, etc.
        v. Solicitation of money for religious or political causes, or for events not related to DCYF or the Combined Fund Drive (CFD) events.
    c. To access, create, post, send, or print:
        i. Anything that promotes or contains:
            A. Discrimination as described in RCW 49.60.030.
            B. Harassment or threats.
            C. Copyright infringement or violations of software licensing agreements.
            D. Personal religious beliefs.
            E. Political campaigns, initiatives, or personal political beliefs.
        ii. The following unless it is for official DCYF business, e.g., investigations, and approved in writing by their supervisors:
            A. Threatening or harassing material
            B. Pornographic material

d. To connect personal devices to DCYF-issued smartphone hotspots.
e. To gain unauthorized access to another computer.
f. To upload or email files or programs that can cause harm to DCYF hardware or networks.

Definitions

Clients are individuals who are the beneficiaries of services or benefits from DCYF. This term includes but is not limited to, consumers, recipients, applicants, parents, youth, and children involved with DCYF. Clients include individuals who previously were the beneficiaries of services or benefits and persons applying for benefits or services.

Confidential Information is information that is protected by state or federal laws, including information about DCYF clients, employees, volunteers, interns, work study students, vendors, or contractors that is not available to the public without legal authority. This includes client records. Information is categorized into the following four areas:

- Category 1: Is public information that can be released to the public. It does not need protection from unauthorized disclosure, but does need protection from unauthorized changes that may mislead the public.
- Category 2: Is sensitive information that is not specifically protected by law, but is limited to official use only, and protected against unauthorized access. This data is available through public disclosure requests.
- Category 3: Is confidential information that is specifically protected by law and not available through public disclosure requests. It includes:
    - Personal information about clients, regardless of how the information is obtained. RCW 42.56.590 and RCW 19.255.010.
    - Information concerning employee payroll and personnel records per RCW 42.56.250.
    - Lists of individuals for commercial purposes as defined in RCW 42.56.070(8).
    - Information about the infrastructure and security of computer and telecommunication networks as defined in RCW 42.56.420.
- Category 4: Is confidential information that requires special handling, including but not limited to:
    - Protected Health Information (PHI), per DCYF Administrative13.04 Protecting Privacy and Confidential Information policy.
    - Information that identifies a person as being or ever having been a client of an alcohol or substance abuse treatment, or mental health program.
    - Federal wage data.
    - Location of an abused spouse.
    - Data that would compromise the agency's constituents.

Discovery is the procedure where each party in a legal action obtains records from the other party. It is DCYF's ongoing obligation to provide all records in our possession to the other legal parties, this includes but is not limited to: electronically stored information (ESI), video or audio recordings, photographs, handwritten notes, and memos.

Electronic Messaging Systems are systems that perform the creation, storage, exchange, and management of texts, images, voice, telex, faxes, e-mails, paging, and electronic data interchange (EDI) over a communications network.

Employees are individuals to whom DCYF pays salaries, wages, or benefits for work performed for DCYF.

Hotspots are internet connections via wireless local area networks.

Information Technology (IT) Resources are all the servers, networks, hardware, software, internet, applications, technical knowledge, expertise, and other IT goods and services held, owned or used by DCYF.

Internet is an unsecured publicly assessable network.

Interns are individuals who work for DCYF with or without pay or benefits. This is typically short term and allows individuals to gain valuable skills and abilities.

Mobile Device Management (MDM) is the security software used by information technology (IT) to encrypt, monitor, manage, and secure employees' mobile devices.

Mobile Devices are all handheld devices with a mobile device management (MDM) used to access DCYF data. This includes tablets, smartphones, and other similar devices.

Volunteers are individuals who of their own free choice, perform any assigned or authorized duties for DCYF. Volunteers receive no wages, and are registered and accepted as a volunteer by DCYF to engage in authorized volunteer services.

Work Study Students are college students participating in programs that enables them to work for DCYF while enrolled in school.

Forms

IT Remote Access Request and Agreement DCYF 17-443
Mobile Work/Telework Agreement DCYF 03-500
Nondisclosure of Confidential Information DCYF 03-374

Resources

Chapter 357-34 WAC Employee Training and Development
DCYF Administrative 1.02.04 Combined Fund Drive Program policy
DCYF Administrative 11.04 Developing and Training Employees policy
DCYF Administrative 11.10 Modern and Mobile Workplace Policy
DCYF Administrative 11.21 Ethics and Employee Conduct policy
DCYF Administrative 12.01 IT Security policy
DCYF Administrative 13.05 Public Records Requests and Disclosure policy
DCYF Administrative 13.06 Records Management and Retention Procedures policy
IT Security Manual
Mandatory Trainings by all State Employees
OCIO 141.10 Data Security policy
OCIO 191 Mobile Device Usage policy
RCW 49.60.030 Freedom from Discrimination-Declaration of Civil Rights
Secure Email Frequently Asked Questions
WAC 292-110-010 Use of state resources