



STATE OF WASHINGTON
DEPARTMENT OF CHILDREN, YOUTH, AND FAMILIES
1500 Jefferson Street, SE • P.O. Box 40975 • Olympia WA 98504-0975

December 31, 2020

To: Debbie Dolgash, Webmaster
From: Rules and Policies Administrator
Subject: Operation Manual Policies to Sunset Phase 3
Approval Date: December 31, 2020

Operations Manual Policy Number & Title	Reason for the Policy Sunset
2227. Quality Initiative	No longer needed.
3300. Advisory Committees	Title only
4320. Limited English Proficiency (LEP)	Replaced with DCYF Administrative 6.02 Access to Services for Clients who are Limited English Proficient (LEP) policy
4330. Serving Persons with Disabilities	Using the DSHS 7.02 Equal Access to Services for Individuals with Disabilities until the DCYF Administrative 6.04 Access to Services for Individuals with Disabilities is finalized
6130. Quality Assurance and Continuous Quality Improvement	No longer needed.
7310. Electronic Files	Replaced with DCYF Administrative 12.01 Information Technology (IT) Security and 12.04 Acceptable Use of IT Resources and the Internet policies
7320. Computer Hardware, Software, and Related Equipment	Replaced with DCYF Administrative 12.03 Agency Approved Software Use and 12.04 Acceptable Use of IT Resources and the Internet policies
7322. Standards	Replaced with DCYF Administrative 12.03 Agency Approved Software Use and 12.04 Acceptable Use of IT Resources and the Internet policies
7323. Procedures	Replaced with DCYF Administrative 12.01 IT Security, 12.02 IT Purchases and Asset Management and 12.04 Acceptable Use of IT Resources and the Internet policies
7340. Telephones	Replaced with DCYF Administrative 12.05 Management of Telecommunication Resources policy
7341. Standards	Replaced with DCYF Administrative 12.05 Management of Telecommunication Resources policy
7420. Policy	Replaced with DCYF Administrative 1.06.04 Control of Capital Assets and 12.02 IT Purchases and Asset Management policies
7430. Procedures	Title only

7431. Purchasing Items Meeting Definition	Replaced with DCYF Administrative 12.02 IT Purchases and Asset Management policy
7432. Receipt And Payment	Replaced with DCYF Administrative 12.02 IT Purchases and Asset Management policy
8323. Staff Training	Replaced with DCYF Administrative 11.04 Developing and Training Employees policy
13200. Initiating a Case Record and Record Establishment	Replaced with Child Welfare Practices and Procedures 6605. Records Management policy
13201. Initiating A Case Record	Replaced with Child Welfare Practices and Procedures 6605. Records Management policy
13210. Record Establishment	Replaced with Child Welfare Practices and Procedures 6605. Records Management policy
13300. Constructing a DCFS Case Record	Replaced with Child Welfare Practices and Procedures 6605. Records Management policy
13600. Restricted Records	Replaced with Child Welfare Practices and Procedures 6605. Records Management policy
13601. Creation of Restricted Records	Replaced with Child Welfare Practices and Procedures 6605. Records Management policy
13604. Access to Restricted Records	Replaced with Child Welfare Practices and Procedures 6800. Background Checks
13605. Designated Access	Replaced with Child Welfare Practices and Procedures 6605. Records Management policy
13609. Who May Restrict a File	Replaced with Child Welfare Practices and Procedures 6605. Records Management policy
13700. Record Accuracy, Privacy, and Disclosure	Replaced with DCYF Administrative 13.05 Public Records Requests and Disclosure policy
13720. Public Records Request	Replaced with DCYF Administrative 13.05 Public Records Requests and Disclosure policy
13721. Public Disclosure Coordinator Responsibilities	Replaced with DCYF Administrative 13.05 Public Records Requests and Disclosure policy
13722. Public Records Request-Responsibilities of all CA Staff	Replaced with DCYF Administrative 13.05 Public Records Requests and Disclosure policy
13726. Disclosure of Client's Representative	Replaced with DCYF Administrative 13.05 Public Records Requests and Disclosure policy
13790. Disclosure for Program and Other Purposes	Replaced with DCYF Administrative 13.05 Public Records Requests and Disclosure policy
13797. Purpose	Replaced with DCYF Administrative 13.05 Public Records Requests and Disclosure and

	Child Welfare Practices and Procedures 6605. Records Management policies
137110. Practice Considerations	Replaced with DCYF Administrative 13.05 Public Records Requests and Disclosure policy
13907. Storage and Retrieval of Case Records	Replaced with Child Welfare Practices and Procedures 6605. Records Management policy
13908. Destruction of Records	Replaced with Child Welfare Practices and Procedures 6605. Records Management policy
14112. Posters and Brochures	No longer needed.
152063. Procedure	No longer needed.
15207. Patch Notification Response Procedures (PNRP)	Replaced with the DCYF Administrative 12.01 IT Security policy
152071. Purpose	Replaced with the DCYF Administrative 12.01 IT Security policy
152072. Applicability	Replaced with the DCYF Administrative 12.01 IT Security policy
152073. Definitions	Replaced with the DCYF Administrative 12.01 IT Security policy
152074. Resources Requirements	Replaced with the DCYF Administrative 12.01 IT Security policy
152075. Procedures for Patch Application	Replaced with the DCYF Administrative 12.01 IT Security policy
15209. Network Emergency Response Procedures (NERP)	Title only
152091. Purpose	No longer needed
152092. Scope	No longer needed
152093. Definitions	No longer needed
152094. Resources Requirements	No longer needed
152095. Upgrade/Change Procedures	Replaced with the DCYF Administrative 12.01 IT Security policy
15210. Shared Emergency Administration (SEA) Account Policy	Title only
152101. Purpose	No longer needed
152102. Applicability	No longer needed
152103. Definitions	No longer needed
152104. Resources Requirements	No longer needed
152105. Procedures	No longer needed
15211. CA Information System Disaster Recovery Procedures	Title only
15212. Securing Unattended Computer Terminals (06/16/06)	Title only
152121. Purpose	Replaced with the DCYF Administrative 12.01 IT Security and 12.04 Acceptable Use of IT Resources and the Internet policies
152122. Applicability	Replaced with the DCYF Administrative 12.01 IT Security and 12.04 Acceptable Use of IT Resources and the Internet policies

152123. Standard	Replaced with the DCYF Administrative 12.01 IT Security and 12.04 Acceptable Use of IT Resources and the Internet policies
------------------	--

Policy Text

2227. Quality Initiative

1. Executive Order 97-03 requires each agency to implement a quality improvement program. The continuous quality improvement approach has demonstrated improved performance in a wide range of public and private organizations. Successful quality efforts require effective leadership, strategic planning, customer focus, employee involvement, continuous improvement, and self-assessment of results.
2. Each agency is required to implement a program to improve the quality, efficiency, and effectiveness of the public service it provides. Improvement in quality is to be accomplished through:
 1. Business process redesign, employee involvement (including involvement of recognized collective bargaining representatives), and other quality improvement techniques.
 2. Provision of training to employees to enable them to successfully implement and complete their efforts in quality improvement.
 3. Designation of a person in each agency to be responsible for improvement of the quality of the systems and work processes within the agency.
 4. Establishment of a Quality Steering Committee composed of appropriate senior management, mid-management, front line staff, and support staff organizations.
3. The CA Quality Improvement Manager provides statewide coordination and technical assistance to support the Quality Initiative. The position is responsible for:
 1. Planning, coordinating, and implementing activities to further the Quality Initiative.
 2. Preparing the CA's annual quality improvement plan and revising as needed.
 3. Providing training regarding continuous quality improvement (CQI) theory and practice for all organizational levels of CA.
 4. Assisting quality improvement teams to use the continuous improvement strategy, including statistical process control.
 5. Developing mechanisms to report on the status of implementation of the Quality Initiative and progress made by quality improvement teams.
 6. Facilitating identification of priority areas for process improvement.
 7. Designing, administering, and analyzing customer, client, and employee surveys.

3300. Advisory Committees

4320. Limited English Proficiency (LEP)

Approval By: Jennifer Strus, Asst. Secretary
 Effective Date: June 1, 1989
 Revised Date: May 1, 2014
 Sunset Review: June 2018

Purpose Statement

To provide Limited English Proficiency (LEP) clients access to CA programs and services in a timely manner and at no cost. LEP means persons are limited in their ability to read, write or

speak English or have a limited ability to speak or read English well enough to understand and communicate effectively.

Laws

[Title VI of the Civil Rights Act of 1964](#)

[RCW 74.04.025](#)

[Chapter 49.60 RCW](#)

[Chapter 388-271 WAC](#)

Policy

1. Provide each Limited English Proficient (LEP) client verbal and written information in his or her own language through certified or qualified interpreters and translators at every phase of service delivery, at no cost and without significant delay as outlined in DSHS Administrative Policy 7.21 Access to Services for LEP Clients.
2. Post [multilingual signs](#) in CA office reception areas, that explain LEP services are available at no cost to the client and without significant delay.
3. Obtain interpreter services for LEP clients whenever there is difficulty in communication, even if the client has not requested interpreter assistance.
4. Use only DSHS certified/qualified interpreters or certified/authorized bilingual staff for in-person communications when serving LEP families. Informal interpretation through family, friends, or office staff members who are not certified is not appropriate. Children, family members, family friends, neighbors, etc., should not serve as interpreters.
5. LEP clients have the right to secure, at their own expense, their own interpreter or have an adult family member or adult friend serve as their interpreter. This does not waive the CA worker's responsibility to arrange for a certified/qualified interpreter to assist CA staff in communicating in-person with the client.
6. Do not allow an interpreter unsupervised access to clients (i.e., do not leave an interpreter alone with clients).
7. Use only DSHS contracted translation companies or DSHS certified bilingual staff for translation work.

Procedures

1. Establish with the client the primary language in which the client prefers to communicate.
2. Arrange interpreter and translation language services for LEP clients as needed. If the assigned CA worker is a certified/authorized bilingual employee, document in a case note.
3. Mark the client as LEP in FamLink (on the "Basic Person Management Page"). Record each client's primary language in FamLink and the case file, and mark "LEP" on the outside of each LEP client's file/binder.
4. Document the use of all LEP services (e.g., use of interpreters or when clients are given translated documents or publications) in FamLink or by documenting on [DCYF 15-245 LEP Client Service Record](#).
5. File copies of all translated client specific documents (e.g. Court Report) in the case file with the corresponding English document or upload translated document(s) into FamLink.

Forms and Tools

[DCYF 15-245 LEP Client Service Record](#)

Resources

The following resources are located on the CA Intranet.

Interpreter Services

- How to get an in-person interpreter (not for court)
- On-Demand telephone Interpreter Services
- Court interpreters
- List of Interpreter Referral Agencies on the WA State Department of Enterprise Services Interpreter Contract
- Guidelines for hiring a non-certified/qualified interpreter
- Guidelines for working with spoken language interpreters
- Court interpreter payment guidelines

Translation Services

- How to get documents translated
- DSHS Forms in other languages
- DSHS Publications in other languages

4330. Serving Persons with Disabilities

1. CA staff will provide equal access to its services and programs to persons who are deaf, deaf-blind, and hard of hearing in accordance with DSHS Administrative Policy 7.20.
2. CA provides equal access to its services and programs to persons with disabilities. The Administration will provide reasonable accommodations to all clients with disabilities and take steps to furnish appropriate auxiliary aids and services whenever necessary to make services accessible to persons with disabilities.
3. Primary consideration will be given to the preferences of the individual with the disability in determining what type of auxiliary aid or service is necessary. These auxiliary aids or services include, but are not limited to:
 1. Telecommunications devices for the deaf (TDD). These devices are connected to telephone lines and enable persons who are deaf or hard of hearing to communicate through printed messages. Each local office must be equipped with a TDD or teletypewriter (TTY).
 2. Washington State Telecommunications Relay Service, a statewide 800 service, which relays messages from TDD users to telephones. Telebraille is also available through the relay service.
 3. American Sign Language (ASL), the native language of the deaf community in the United States. ASL is a visual-gestured language with vocabulary and grammar, which is different from English.
 4. Sign language interpreters. Whenever available, the services of an interpreter who is certified by the Registry of Interpreters for the Deaf (RID) and/or the National Association of the Deaf (NAD) is to be secured. If a certified interpreter is not available, a non-certified interpreter deemed qualified by the client may be used. A certified interpreter must be used for all medical and legal appointments.
 5. Lip-reading or note writing.
 6. Qualified readers who read standard print materials to visually impaired or blind persons.
 7. Extra large print versions of materials.

8. ASCII (American Standard Code for Information Interchange) text files for voice synthesizers and computer screen magnification.
9. Braille transcriptions.

6130. Quality Assurance and Continuous Quality Improvement

Approval

By: Jennifer Strus, Asst. Secretary

Effective Date: February 15, 1998

Revised Date: May 1, 2014

Sunset Review: June 2018

Purpose Statement

Children's Administration (CA) seeks to continuously improve the quality, efficiency, and effectiveness of culturally competent services provided to children and families. CA accomplishes this through quality assurance and continuous quality improvement efforts that include:

1. Providing tools, expertise, resources, and training to support the pursuit of innovative improvement initiatives.
2. Recognizing and respecting diversity.
3. Focusing on improved client outcomes while fostering innovation.

Laws

[RCW 43.88.090](#)

[Executive Order 97-03](#)

[Executive Order 13-04](#)

Policy

1. The HQ Quality Assurance/Quality Improvement (QA/CQI) manager has primary responsibility for quality assurance, including reviews that measure compliance with performance standards and oversight of continuous quality improvement efforts.
2. Program Managers, Supervisors, Area Administrators, Regional Administrators, the Division of Licensed Resources (DLR) Administrator and the CA Headquarters Management Team use data to inform practice improvements through information driven decision making.
3. Performance benchmarks are established in the areas of child safety, permanency, and child and family well-being.
4. Quality Assurance (QA) and Continuous Quality Improvement (CQI) efforts engage staff (internal stakeholders) from all program areas and levels of authority as well as community and tribal advisory groups (external stakeholders).
5. Training on the use of performance measure data and continuous quality improvement methods is available to all staff.

Procedures

1. Gather data to inform practice improvements from multiple sources, including but not limited to:
 1. FamLink
 2. Case reviews (central and targeted case reviews)
 3. External sources (e.g., Office of the Family and Children's Ombuds, federal child welfare reports, Administrative Office of the Courts)
 4. Surveys (staff, caregivers, etc.)
2. Establish performance benchmarks and report agency performance regarding those benchmarks. Benchmarks support CA and DSHS strategic goals.
3. Convene
 1. A statewide CQI Advisory Committee to meet regularly to provide oversight and consultation for QA/CQI activities. The HQ QA/CQI manager will convene and facilitate these meetings.
 2. Local office QA/CQI committees to regularly identify and set goals for areas needing improvement. Goals may support CA and DSHS strategic goals or practice improvements identified by local offices QA/CQI committees. Regional and DLR Administrators will convene the local office QA/CQI committees and assign responsibility for those committees.
4. CA Headquarters and regional QA/CQI staff will
 1. Provide training on the use of performance measure data and continuous quality improvement methods.
 2. Monitor achievement towards CA goals and strategies through tracking benchmarks, program expectations and performance measures.
 3. Support staff in quality data collection and reporting.
 4. Provide technical assistance for QA/CQI processes.

Forms and Tools

DSHS 10-495 Case Review Feedback Summary
DSHS 10-497 CQI Action Plan

Resources

Lean In Washington

7310. Electronic Files

1. Following the procedures outlined in this section and in the DSHS Information Technology Security Manual does not guarantee that staff's messages and files will be protected. If a user fails to maintain their password security or leaves their terminal unattended while logged into the system, their messages and files are vulnerable. Also, staff need to be aware that messages that are sent can be forwarded to others, printed where others may read them, or sent to the wrong user.
2. Electronic message systems, including voice mail, FAX, e-mail, the FamLink bulletin board, and the CA Intranet server, may be used only for state business purposes. Use of state resources for private gain or benefit is specifically prohibited by RCW 42.52.160. Records created through these systems are legally the property of the state. In the use of computer technology, staff are to comply with the provisions of DSHS Administrative Policy 15.10; chapter 15000, section 15205, of this manual; and the DSHS Information Technology Security Manual, a copy of which is available in each region through its

Computer Information Consultant (CIC). However, WAC 292-110-010 provides for the occasional use of state resources when:

1. There is no actual cost to the state; or
2. The cost to the state is de minimis; i. e., so small as to be insignificant or negligible.
3. The following points apply to CA staff:
 1. A manager, in the supervisory line of the employee, with reasonable justification, has access to data within CA's systems to carry out required business functions.
 2. State-provided electronic message systems may not be used to transmit or store information that promotes:
 1. Discrimination on the basis of age, race, color, gender, creed, marital status, national origin, disability, or sexual orientation;
 2. Harassment;
 3. Copyright infringement;
 4. An employee's personal political beliefs or personal business interests; or
 5. Any activity prohibited by federal, state, or local law or regulation.
 3. Transmission of e-mail messages containing confidential or privacy-protected data (e. g., confidential client or employee data) shall:
 1. Be marked private;
 2. Not be proxied or forwarded, except in "need to know" situations.
 4. Supervisors shall not disclose to third parties the contents of electronic files under an employee's control, except under unusual circumstances; for example:
 1. Compliance with applicable public disclosure laws, discovery rules, or pertinent law; or
 2. When disclosed as part of an official department, state, or external investigation.
 5. Staff shall not disclose confidential passwords used to gain access to local, wide area, and FamLink. If the password is compromised, staff shall change it immediately.
 6. In order to assure confidentiality of client information, staff will use CA network equipment to print or transfer client information or photos.

7320. Computer Hardware, Software, and Related Equipment

7322. Standards

1. Protection-Staff to whom computers and printers are permanently or temporarily assigned shall:
 1. Ensure protection of data processing equipment from theft or damage.
 2. Protect division software from theft or unauthorized, accidental, or malicious use, modification, or destruction.
 3. Protect division confidential documents from theft or unauthorized disclosure.
 4. If an employee, through personal negligence, causes damage to state equipment, CA may require the employee to pay for repair or replacement of the damaged equipment.
2. Appropriate Use-Staff shall use department computers, peripheral equipment, and software only for official state purposes.

7323. Procedure

1. General Protection

1. Regional Administrators, Regional Managers, and Directors shall ensure that portable fire extinguishers -- preferably a Halon type -- suitable for treating electrical fires are located near data processing equipment in their areas of responsibility.
 2. Users of computers shall:
 1. Protect diskettes from excess cold, heat, direct sunlight, electromagnetic sources such as telephones and static electricity, and from ball point pens and pencils.
 2. Remove all diskettes from the computer when they are no longer in use.
 3. Computer users shall utilize surge control devices to protect all computer and peripheral equipment.
 4. Staff shall not plug coffee pots, hot plates, or other high current devices into a surge protector serving computer equipment.
 5. Staff shall secure computer hardware and software when not in use. See chapter 15000, section 15212.
 6. User staff shall secure lap-top computers in file cabinets or closets at the end of each work day.
 7. When in travel status, staff shall not ship computers or printers as general luggage through the airlines.
2. Security of Data
 1. Staff shall store confidential documents or data in accordance with chapter 15000, section 15203.
 2. Staff shall not leave documents or diskettes containing confidential information unattended in areas readily accessible to persons without authorization to see such documentation.
 3. Computer users shall save important documents and those for which there may future need in FamLink or on their F Directory, as applicable, to assure automatic back-up of files.
 4. When an employee ends employment in a location, supervisory personnel shall review all files on hard drive, main frame, and floppy diskettes controlled by the employee to determine which files to delete or retain.
 3. Software Use
 1. Computer users shall not use programs obtained through shareware or from a bulletin board until they have been certified as free of computer virus by the user's Computer Information Consultant (CIC) or other authorized staff.
 2. Staff shall install and/or use only software purchased, distributed, or approved by the department.
 4. Prohibited Activities-Staff are prohibited from the following activities:
 1. Unauthorized copying or use of software.
 2. Unauthorized entry into restricted data bases.
 3. Use of state computer resources for private business purposes.
 4. Loan of computer hardware or software to unauthorized individuals.
 5. Use of recreational computer games during work periods for other than supervisor-approved training purposes.
 6. Use of privately owned personal computer hardware during business hours except as part of a pre-approved telecommuting project.
 5. Accountability and Tracking of Laptop Computers: CA Directors and Regional Administrators are responsible for the accountability and tracking procedures. To assure accurate tracking and accounting for laptop computers, laptop computers must either be assigned to specific staff or signed out to staff following the procedures below.
 1. For managing laptop inventory:

1. Each CA office will designate one specific employee, plus one backup employee, to be responsible for tracking laptop computers.
 2. Any lost, stolen, or missing equipment must be reported immediately to the designated staff, who will immediately report to the Regional Business Manager or headquarters property manager for reporting in the Tracks inventory system.
 3. Designated staff for the office must send a lost, stolen, or missing equipment report to the Regional Administrator or applicable Director on a monthly basis.
2. Laptop Computers Signed Out by Staff
 1. All laptop computers will be kept in a locked cabinet or area unless checked out by staff.
 2. The designated staff responsible for tracking will ensure that each laptop has a sign-out log, which will be kept with the laptop in the locked area. When the equipment is signed out, the log sheet will remain in the locked area.
 3. Staff checking out the laptop will do so only through the designated staff. The designated staff will completely fill out the log sheet immediately upon a staff person checking out or returning the equipment.
 4. The staff person who signed out the equipment is responsible for the computer until it is returned to the designated staff and properly logged in and returned to the locked area.
 3. Laptop Computers Permanently Assigned to Specific Staff
 1. The designated staff person will maintain a current list recording the name of the staff person assigned the equipment, the date assigned, and the equipment's make, model, and State Tag Number.
 2. The staff person assigned to the equipment is responsible for it.
 3. If staff assigned to the equipment allows other staff to use it, the staff person assigned remains responsible for the equipment.

7340. Telephones

7341. Standards

1. Telephones provided to employees are state property, with usage paid by the state. Therefore, employees must use them only for official department business.
2. Each Regional Administrator, Regional Manager, or Director, as applicable, must ensure that a different SCAN authorization number is assigned to each individual staff member who may place long distance telephone calls.
3. CA staff conducting state business must place long distance telephone calls using the SCAN or SCAN-PLUS system. They must not place personal or private business long distance calls through the system. The sole exception would be when an employee is detained on state business beyond normal work hours and is expected elsewhere.
4. To use the SCAN or SCAN-PLUS system, volunteers must receive authorization in advance from the DCFS Regional Administrator or designee or DLR Regional Manager and use their own individual access code.

7420. Policy

1. The Director, Management Services Division, for CA headquarters, or the applicable Division of Children and Family Services (DCFS) Regional Administrator or Division of Licensed Resources (DLR) Regional Manager must:

1. Appoint an Asset Inventory Coordinator (AIC) to be responsible for the inventory control activities listed in the DSHS Asset Management Manual and TRACKS, the DSHS inventory system;
 2. Appoint an Asset Inventory Representative (AIR) to be responsible for the oversight of inventory at the regional and local levels;
 3. Ensure annual completion of a physical fixed asset inventory and reconciliation and that each inventory is documented by a signed "Certificate(s) of completion";
 4. Ensure that staff with no direct responsibility for assets subject to the inventory count performs physical inventories;
 5. Ensure the AIC is informed of any changes in the physical locations of the division or region's organizational units or their mailing addresses; and
 6. Attest to the completion of all biennial inventories by co-signing a "Certification of Completion" with the AIC.
2. The AIC must:
1. Facilitate exchange of information between CA and the DSHS Asset Management Section;
 2. Return the quarterly TRACKS confirmation packet of location code information and other inventory data updates to Asset Management within 15 working days of issue;
 3. Provide guidance to the AIR's on implementing division or regional and TRACKS procedures;
 4. Conduct inventory training necessitated by staff turnover;
 5. Coordinate the annual and biennial physical inventories with the AIR's and Asset Management;
 6. Compile the CA Physical Inventories and attach a "Certificate of Completion," co-signed with the division director or regional administrator and send to Asset Management.
 7. Notify Asset Management in writing of any changes in the AIR's, locations, phone numbers, organization, and security levels for access to TRACKS; and
 8. Perform inventory control tasks, including timely computer input and reconciliation, according to the guidelines in the Asset Management Manual.
3. The AIR must:
1. Account for the receipt, tagging, maintenance, and disposition of inventory according to the guidelines in the Asset Management Manual;
 2. Notify the AIC immediately of any changes in fixed assets, inventory staff, or the organization that might affect TRACKS; and
 3. Confirm the completion and reconciliation of the annual inventory by the signature of the regional administrator.
4. The Headquarters Local Area Network (LAN) Administrator and the regional Information Technology Application Specialist/Information Technology System Specialist (ITAS /ITSS) or designee must:
1. Share with regional staff the responsibility of inventory control functions associated with the coordination of new equipment, transfers, equipment loans, surplussing and the disposal of computers and related equipment;
 2. Send the updated information to the AIC/AIR/RBM and update TRACKS; and
 3. Assist in the annual physical inventories of all IT equipment.

7430. Procedures

7431. Purchasing Items Meeting Definition

1. CA staff must complete all purchases in compliance with the DSHS purchasing guidelines published annually by Purchased Service Contracts.
2. In addition to following other applicable DSHS guidelines, CA staff must request all IT purchases with the assistance of IT staff as follows:
 1. IT staff provide technical consultation during the entire purchasing processes for office automation hardware and software. This would include the following:
 1. Research products prior to the completion of an Information Technology Purchase Request (ITPR) to ensure compatibility with current systems and future upgrades.
 2. Provide recommendations to regional staff regarding products that would help resolve automation issues.
 3. Assist the Fiscal staff in locating vendors that will provide the right product at a competitive price with adequate post-purchase service.
 4. Ensure existing resources are exhausted prior to purchasing additional ones.
 2. Assigned staff must forward the completed Purchase Request with appropriate signatures to the CA Office Chief with proper justification and include the inventory location on the Purchase request to ensure accurate issuance of state tags on applicable equipment.
 3. The CA IT Office Chief will approve or disapprove the purchase. If disapproved, the IT Office Chief will send the ITPR back to the originator. If approved, the IT Office Chief will forward the ITPR to Purchase Services Contracts, where staff will complete the purchasing process and forward to the originator of the ITPR, a copy of the Field Order/Purchase Order (FO/PO). The Purchase Services Contracts staff will return the FO/PO with state tags, if applicable, for the item being

7432. Receipt and Payment

1. Upon receipt of the equipment and signing by the appropriate staff, the receiving copy of the PO will go to the staff responsible for payment.
2. Staff responsible for payment will send a copy of the received PO and invoice to the AIC/AIR.

8323. Staff Training

Approval: Jennifer Strus, Assistant Secretary

Effective Date: February 15, 1998

Revised Date: October 31, 2014

Sunset Review: October 31, 2018

Purpose

As a critical element in the delivery of quality culturally competent child welfare services, CA is committed to Children's Administration (CA) staff receive the training necessary to be successful in their current job, and throughout their professional career.

Laws

[RCW 74.14B.010](#)

Policy

1. **Mandatory Training**

1. **All New Staff must:** Successfully complete the DSHS New Employee Orientation required by DSHS Administrative Policy No. 18-34 located on the DSHS Intranet. Training topics include:
 1. Domestic Violence & the Workplace
 2. Blood Borne Pathogens & HIV/AIDS
 3. Diversity
 4. Harassment Prevention
 5. HIPAA
 6. Ethics Test
 7. IT Security Awareness
2. **New/Present Social Service Specialists must:**
 1. Successfully complete Regional Core Training (RCT) during the first two months of beginning employment with CA.
 2. Be assigned no more than 10 total cases or no more than 6 intakes as primary or secondary worker until proficient in the RCT competencies and curriculum.
 3. Attend all RCT sessions (some exceptions may be made if the staff can demonstrate their knowledge **and** skills in the specific area as determined by the Supervisor, Area Administrator (AA) in consultation with the Alliance) and approved by the Deputy or Regional Administrator.
 4. Successfully complete In-Service trainings in prospective program areas or related topics, e.g., domestic violence, child mental health, etc., within the first year of CA employment or within one year of position transfer.
 5. Participate in specialized training which meets [RCW 74.14B.010](#) requirements when responsible for interviewing and assessing child sexual abuse.
 6. Attend additional statewide and regional training when required.
3. **Non Social Service Specialists** are not required to attend RCT but will be required to participate in training relevant to their current area of practice.
4. **New/Present Supervisors must:**
 1. Successfully complete entry-level supervisory or managerial trainings as required by DSHS Administrative Policy No. 18-34 and [WAC 357-34-055](#).
 2. Successfully complete Supervisor Core Training within the first six months of becoming a new supervisor or when requested by the Regional Administrator.
 3. Successfully complete In-Service training within the first two years of becoming a new supervisor, transferring to a new supervisory position or earlier if requested by the Regional Administrator.
5. **Foster Parents** - Please see Foster Parent Training Information on the CA Intranet.

2. **Voluntary Training**

1. CA staff will be provided continuing education training opportunities annually to advance their knowledge and skill mastery.
2. Child Welfare Training and Advancement Program (CWTAP) (IV-E) graduate students (not currently employed by CA) may register for RCT within six months of completion of MSW degree requirements. Exceptions may be made for students within nine months of graduation, if they are unable to attend RCT.

CWTAP students are responsible for their travel, per diem, and lodging costs while attending RCT.

3. Tribal social workers are eligible to participate in RCT and other CA trainings.

3. Documentation

1. Training requirements will be recorded by the current Human Resources tracking system.
2. Each region will coordinate with the Alliance to update employee training information. A list of completed trainings is available to CA staff in the tracking system and whether or not a worker did or did not complete training may be used in the personnel evaluation process.

Procedures

1. Mandatory Training

1. New CA (non Social Service Specialists) Staff must:
Contact your supervisor or Human Resources Division to register for the DSHS New Employee Orientation.
2. New/Present Social Service Specialists must:
 1. Complete DSHS New Employee Orientation which is included in RCT.
 2. Begin RCT on the first day of employment and complete RCT by demonstrating proficiency in the knowledge and skills contained in the competencies and curriculum. (CA Supervisors will register new hires with the Alliance when staff is first hired). To demonstrate previous child welfare experience, existing knowledge and skills in a specific RCT session you may:
 1. Submit a completed Prior Learning Assessment (PLA) to your supervisor. If the supervisor agrees, he/she will:
 2. Consult with the Alliance and send the request to the Area Administrator. If the AA agrees, the AA will:
 3. Send the request to his/her Deputy or Regional Administrator for approval. If there is disagreement regarding the approval, the RA will make the final decision.
 3. Complete the following In-Service training within the first year of hire:
 1. Program Specific Training; Intake, CPS Investigations or Family Assessment Response (FAR), Division of Licensed Resources (DLR)/CPS, Family Voluntary Services (FVS), Family Reconciliation Services (FRS), Child and Family Welfare Services (CFWS), Interstate Compact on the Placement of Children (ICPC), Adoption, and Licensing and Unified Home Study.
 2. Indian Child Welfare
 3. Basics of Substance Abuse
 4. Permanency Planning
 5. Engagement and Partnership with Caregivers
 6. Child Development Well-Being; Education, Health, and Adolescence.
 7. Risk and Safety Assessment
 8. Worker Safety
 9. Racial Disproportionality and Disparities
 4. Complete the following In-Service training within the second year of hire:
 1. Mental Health and Child Abuse and Neglect
 2. Domestic Violence and Child Abuse and Neglect [RCW 74.14B.010](#)

3. Diversity - Building Bridges
4. Indian Child Welfare Cross Cultural Skills
5. Advanced Substance Abuse and Child Abuse and Neglect
6. Collaboration/Customer Service
7. Supervisors
8. Contact your Supervisor or Human Resources Division to complete the following trainings as required by DSHS Administrative Policy 18-34 and [WAC 357-34-055](#)
9. Contact the Alliance to complete the In-Service training at Alliance@dshs.wa.gov.

2. Voluntary Training

1. Social Service Specialists contact the Alliance Learning Development Coordinator to register for Focused Continuing Education trainings when approved by his/her supervisor.
2. CWTAP and Tribal staff contact the Alliance Learning Development Coordinator to register for RCT, In-Service and Focused Continuing Education Trainings.

Forms and Tools

Regional Core Training Program Description

Prior Learning Assessment Form

Resources

Prior Learning Assessment

[Alliance For Child Welfare Excellence](#)

13200. Initiating a Case Record and Record Establishment

13201. Initiating A Case Record

1. All Children's Administration (CA) cases are:
 1. assigned a unique case number, generated by FamLink, and
 2. are "family based cases" with the exception of legally free, and adoption support cases.
2. CA has three types of cases:
 1. Family Case - The intake supervisor (Field or Central Intake) reviews each intake, determine if information is on an existing case in FamLink and either links or creates a new case.
 2. Legally Free Case - When a child becomes legally free, the child is deactivated from the family case for the reason of "legally free". FamLink automatically creates a new Legally Free case for that specific child. A legally free case has only one participant and is created without a new intake.
 3. Adoption Support Case - After adoption finalization, an adoption support case is created through the Legally Free Case, from the options menu in FamLink. The legally free case should be closed as soon as all work is completed on it. This closed case becomes a restricted case in FamLink. The adoption support case becomes a "sealed" case, meaning it will only show in search results to those with secured adoption support security.

3. If an adopted child is an alleged victim of abuse or neglect in their adoptive home or if non-adoption support services are requested, a new intake must be created in FamLink and a new family case should be created under the adoptive parents (separate from the adoption support case).

13210. Record Establishment

Case records are created in the local offices for the following screened-in intakes:

1. Child Protective Services (CPS)
2. Family Voluntary Services (FVS)
3. Family Reconciliation Services (FRS)
4. Child and Family Welfare Services (CFWS)
5. Adoptions
6. Child Day Care Services
7. Foster Home/Private Agency Licensing
8. Intra and Interstate Home studies
9. Federal Funding

13300. Constructing a DCFS Case Record

All DCFS paper records are to be constructed with the following sections as described in procedures below. The DCFS physical record contains separate sections placed in a binder in the following order: *All information in the binder is to be filed in chronological order.*

1. Family Assessment Information
2. Case Activities
3. Placement and Legal
4. Privileged Communication
5. Child Health and Safety
6. Family Background
7. Indian Child Welfare
8. Service Reports and Correspondence
9. Correspondence
10. Reports, Staffings, Visits
11. Payment
12. Other
13. Audio Recording
14. Federal Revenue

13600. Restricted Records

1. Electronic and paper files require restricted access for the following categories of personnel and their families: Children's Administration (CA) staff; Economic Services Administration (ESA) Division Early Learning (DEL); personnel covered by the Public Assistance Bargaining Agreement; High Profile Cases; and other defined circumstances.
2. All information related to persons covered under this policy must be immediately secured both physically (in a locked file) and electronically.

13601. Creation of Restricted Records

1. Restricted records will be created for:
 1. CA & DEL employee or their family members that are listed as a subject, victim, or client in a CPS, Risk Only or Non CPS intake; or in facility intakes/cases.
Note: Definition of "family" for CA personnel means members of the household of any employee. Other relatives may be designated if the employee, social worker or client makes a written request and receives approval from the DCFS/DLR Deputy Administrator, DCFS/DLR Area Administrator or the HQ Appointing Authority.
 2. Any employee represented by the Washington Federation of State Employees or their family members are listed as a subject, victim or client in a CPS, Risk Only or Non CPS intake; or in facility intakes/cases.
 3. All other DSHS employees listed as a subject in a CPS or Risk Only intake.
 4. Legally Free Child's Case Record: Upon the Final Adoption Decree and archiving of a legally free child's case record, the child's pre-adoption record must be made Administrative restricted.
 5. High Profile Cases as designated by an Appointing Authority.

13604. Access to Restricted Records

1. Children's Administration (CA) staff must not access any person, case or intake information without a need to know. "Need to know" means that the information is necessary in the discharge of an employee's professional responsibilities (see Administrative Policies No. 18.64; No. 05.01; 15.10)
2. Employees assigned to a case have access to restricted records associated with that case.
3. The following persons have been identified as the "designated Security Group" and have access to all restricted records in FamLink:
 1. Assistant Secretary
 2. FOD, P&PI, & Practice Model Division Directors
 3. Regional Administrators & Deputy Regional Administrators
 4. HQ Risk Management (Deputy FOD Director, Supervisor Constituent Relations, & Practice Consultants)
 5. DLR HQ Program Managers
 6. Legislative Liaison
 7. Ombudsman Office
 8. CATS Service Desk
 9. Foster Care Medical Team Supervisor & Lead Worker (HRSA)
 10. HQ IV-E (One Lead)
 11. HQ Payment Specialist (One Lead)
 12. HQ ICPC Supervisor
 13. HQ Adoption Support Program Manager
 14. Foster Care Public Health Nurse Program Coordinator & PH Assistant
 15. Area Administrators
 16. Administrative Secretaries
 17. Regional Safety (CPS) Program Managers or Fatality Review Program Managers
 18. Intake Supervisors

13605. Designated Access

Anyone in the designated Security Group listed above in 13604, may designate an individual access to an **open** record. Once supervisors or area administrators have been given access to a restricted record they may designate further access through secondary case assignments.

13609. Who May Restrict A File

Files meeting the criteria for restriction may be restricted in FamLink by a supervisor or above.

13700. Record Accuracy, Privacy, and Disclosure

This section addresses maintenance of accurate records, personal privacy, and disclosure and nondisclosure of CA records, including licensing records.

These topics are inter-related, with accuracy of information being a significant element.

13720. Public Records Request

1. The Public Records Act, chapter 42.56 RCW, governs access to and disclosure of public records. CA is required to make identifiable public records promptly available for inspection and copying upon request by any person, unless nondisclosure is required or authorized by law.
2. Administrative Policy 5.02 governs all DSHS responses to Public Records Act requests. All CA staff must follow Administrative Policy 5.02. The CA Operations Manual is intended to supplement this policy with additional internal operation procedures.

13721. Public Disclosure Coordinator Responsibilities

1. All CA Public Disclosure Coordinator must follow Administrative Policy 5.02, Public Records Requests. If Administrative Policy 5.02 and the CA Operations Manual contradict one another, the Public Disclosure Coordinator must follow Administrative Policy 5.02.
2. The Public Disclosure Manager, in the Finance and Operations Support Division (FOSD) is the designated Public Disclosure Officer for Children's Administration. The Public Disclosure function for CA is centralized under the Public Disclosure Manager, with regional offices as well as a headquarters unit.
3. Regional Public Disclosure Coordinators will respond to routine public disclosure requests. However, regional Public Disclosure Coordinators must not respond to the following requests and must immediately route such requests to a headquarters Public Disclosure Coordinator for response.
 1. Requests for reports collected at the state office; for example, statewide Health and Safety Report, FamLink reports generated at the state office level.
 2. Requests for information from more than one region where consistency of information is necessary.
 3. Requests from employees.
 4. Especially sensitive issues are best handled at Headquarters:
 1. Requests from the media, including, newspapers, television, and radio;
 2. Requests from attorneys, which may involve potential lawsuits;
 3. Requests from legislators;
 4. Requests involving "hot" cases or those generating controversy in the community; and
 5. Other cases which may be of a hostile nature or where there is need for headquarters staff and Media Relations to be aware of the request.
 5. When there is a question about whether the preparation should be done at the regional or headquarters level, the regional Public Disclosure Coordinator will consult with a headquarters Public Disclosure Coordinator. or the Public Disclosure Manager

4. Public Disclosure Coordinators must consult with an assigned AAG and/or the DSHS Public Records and Privacy Officer when an issue regarding the release of information is not clear.
5. If the person requesting disclosure disagrees with the decision of a Public Disclosure Coordinator, the person may petition for review of the decision denying disclosure.
 1. If the petition is for the review of a decision made by a regional Public Disclosure Coordinator, it must be sent to a headquarters Public Disclosure Coordinator for review.
 2. If the petition is for the review of a decision made by a CA headquarters Public Disclosure Coordinator, it must be sent to the Public Disclosure Manager or their designee for review.

13722. Public Records Request - Responsibilities of all CA Staff

CA staff must comply with the provisions of WAC Chapter 388-01 and DSHS Administrative Policy No. 5.02 - Public Records Requests. These responsibilities include, but are not limited to:

1. A public records request may be made to any staff and does not need to be made in writing or on a specific form. If a CA staff receives a public records request, or believes they may have received a public records request, they must forward that request immediately to a CA Public Disclosure Coordinator. Not doing so may result in fines to the agency under the Public Records Act, RCW 42.56.
2. When a Public Disclosure Coordinator requests records staff are required to provide all records, whether disclosable or not, to the Public Disclosure Coordinator. It is the responsibility of the Public Disclosure Coordinator to determine what may be disclosed.
 1. Failure to provide all responsive records may result in fines to the agency under the Public Records Act, RCW 42.56.
3. If a public records request is made at a time when such record exists but is scheduled for destruction, the department must retain possession of the record and may not destroy or erase the record until the request is resolved. WAC 388-01-060; RCW 42.56.100.

13726. Disclosure to Client's Representative

When a representative designated by a client requests the client's record, the request must be accompanied by a written release signed by the client. The representative may be an attorney, legal guardian or lay representative. The written release must include the following:

1. The identity of the person(s) or organization(s) to whom disclosure is to be made;
2. An identification of the record, or portion thereof, to be disclosed; and
3. A statement of when the authorization for disclosure expires.

13790. Disclosure for Program and Other Purposes

1. For purposes directly related to the administration of department programs, information shall be disclosed between offices of the department, unless prohibited by 45 CFR 205.50 or other law.
2. For purposes directly connected with the administration of department programs, information may be disclosed by the department to outside agencies, unless disclosure is prohibited by law. Agencies or individuals receiving such information are subject to the same standards of disclosure as are required of the department.

3. To the extent not otherwise prohibited or authorized by law, inquiries from agencies outside the department will be honored only if written and only if the client's authorization is included in the request. WAC 388-01-070

13797. Purpose

1. These forms were developed to meet the various federal and state statutory and regulatory requirements on a Department-wide basis, as confirmed by the review of program Assistant Attorney Generals (AAG).
2. The two forms provide uniformity and are valid Department-wide. CA will use the forms in place of any existing forms. Staff are to accept these forms as valid and not ask a client to complete a different DSHS form if one of these two has been properly executed.
 1. The Consent Form 14-012 allows programs to share information about mutual clients to coordinate service delivery.
 2. The Authorization Form 17-063 permits DSHS to release client records and information to a third party, including an attorney, legislator, or relative.

13200. Initiating a Case Record and Record Establishment

13201. Initiating A Case Record

1. All Children's Administration (CA) cases are:
 1. assigned a unique case number, generated by FamLink, and
 2. are "family based cases" with the exception of legally free, and adoption support cases.
2. CA has three types of cases:
 1. Family Case - The intake supervisor (Field or Central Intake) reviews each intake, determine if information is on an existing case in FamLink and either links or creates a new case.
 2. Legally Free Case - When a child becomes legally free, the child is deactivated from the family case for the reason of "legally free". FamLink automatically creates a new Legally Free case for that specific child. A legally free case has only one participant and is created without a new intake.
 3. Adoption Support Case - After adoption finalization, an adoption support case is created through the Legally Free Case, from the options menu in FamLink. The legally free case should be closed as soon as all work is completed on it. This closed case becomes a restricted case in FamLink. The adoption support case becomes a "sealed" case, meaning it will only show in search results to those with secured adoption support security.
3. If an adopted child is an alleged victim of abuse or neglect in their adoptive home or if non-adoption support services are requested, a new intake must be created in FamLink and a new family case should be created under the adoptive parents (separate from the adoption support case).

13210. Record Establishment

Case records are created in the local offices for the following screened-in intakes:

1. Child Protective Services (CPS)
2. Family Voluntary Services (FVS)
3. Family Reconciliation Services (FRS)
4. Child and Family Welfare Services (CFWS)

5. Adoptions
6. Child Day Care Services
7. Foster Home/Private Agency Licensing
8. Intra and Interstate Home studies
9. Federal Funding

13300. Constructing a DCFS Case Record

All DCFS paper records are to be constructed with the following sections as described in procedures below. The DCFS physical record contains separate sections placed in a binder in the following order: *All information in the binder is to be filed in chronological order.*

1. Family Assessment Information
2. Case Activities
3. Placement and Legal
4. Privileged Communication
5. Child Health and Safety
6. Family Background
7. Indian Child Welfare
8. Service Reports and Correspondence
9. Correspondence
10. Reports, Staffings, Visits
11. Payment
12. Other
13. Audio Recording
14. Federal Revenue

13600. Restricted Records

1. Electronic and paper files require restricted access for the following categories of personnel and their families: Children's Administration (CA) staff; Economic Services Administration (ESA) Division Early Learning (DEL); personnel covered by the Public Assistance Bargaining Agreement; High Profile Cases; and other defined circumstances.
2. All information related to persons covered under this policy must be immediately secured both physically (in a locked file) and electronically.

13601. Creation of Restricted Records

1. Restricted records will be created for:
 1. CA & DEL employee or their family members that are listed as a subject, victim, or client in a CPS, Risk Only or Non CPS intake; or in facility intakes/cases.
Note: Definition of "family" for CA personnel means members of the household of any employee. Other relatives may be designated if the employee, social worker or client makes a written request and receives approval from the DCFS/DLR Deputy Administrator, DCFS/DLR Area Administrator or the HQ Appointing Authority.
 2. Any employee represented by the Washington Federation of State Employees or their family members are listed as a subject, victim or client in a CPS, Risk Only or Non CPS intake; or in facility intakes/cases.
 3. All other DSHS employees listed as a subject in a CPS or Risk Only intake.

4. Legally Free Child's Case Record: Upon the Final Adoption Decree and archiving of a legally free child's case record, the child's pre-adoption record must be made Administrative restricted.
5. High Profile Cases as designated by an Appointing Authority.

13604. Access to Restricted Records

1. Children's Administration (CA) staff must not access any person, case or intake information without a need to know. "Need to know" means that the information is necessary in the discharge of an employee's professional responsibilities (see Administrative Policies No. 18.64; No. 05.01; 15.10)
2. Employees assigned to a case have access to restricted records associated with that case.
3. The following persons have been identified as the "designated Security Group" and have access to all restricted records in FamLink:
 1. Assistant Secretary
 2. FOD, P&PI, & Practice Model Division Directors
 3. Regional Administrators & Deputy Regional Administrators
 4. HQ Risk Management (Deputy FOD Director, Supervisor Constituent Relations, & Practice Consultants)
 5. DLR HQ Program Managers
 6. Legislative Liaison
 7. Ombudsman Office
 8. CATS Service Desk
 9. Foster Care Medical Team Supervisor & Lead Worker (HRSA)
 10. HQ IV-E (One Lead)
 11. HQ Payment Specialist (One Lead)
 12. HQ ICPC Supervisor
 13. HQ Adoption Support Program Manager
 14. Foster Care Public Health Nurse Program Coordinator & PH Assistant
 15. Area Administrators
 16. Administrative Secretaries
 17. Regional Safety (CPS) Program Managers or Fatality Review Program Managers
 18. Intake Supervisors

13605. Designated Access

Anyone in the designated Security Group listed above in 13604, may designate an individual access to an **open** record. Once supervisors or area administrators have been given access to a restricted record they may designate further access through secondary case assignments.

13609. Who May Restrict A File

Files meeting the criteria for restriction may be restricted in FamLink by a supervisor or above.

13700. Record Accuracy, Privacy, and Disclosure

This section addresses maintenance of accurate records, personal privacy, and disclosure and nondisclosure of CA records, including licensing records.

These topics are inter-related, with accuracy of information being a significant element.

13720. Public Records Request

1. The Public Records Act, chapter 42.56 RCW, governs access to and disclosure of public records. CA is required to make identifiable public records promptly available for inspection and copying upon request by any person, unless nondisclosure is required or authorized by law.
2. Administrative Policy 5.02 governs all DSHS responses to Public Records Act requests. All CA staff must follow Administrative Policy 5.02. The CA Operations Manual is intended to supplement this policy with additional internal operation procedures.

13721. Public Disclosure Coordinator Responsibilities

1. All CA Public Disclosure Coordinator must follow Administrative Policy 5.02, Public Records Requests. If Administrative Policy 5.02 and the CA Operations Manual contradict one another, the Public Disclosure Coordinator must follow Administrative Policy 5.02.
2. The Public Disclosure Manager, in the Finance and Operations Support Division (FOSD) is the designated Public Disclosure Officer for Children's Administration. The Public Disclosure function for CA is centralized under the Public Disclosure Manager, with regional offices as well as a headquarters unit.
3. Regional Public Disclosure Coordinators will respond to routine public disclosure requests. However, regional Public Disclosure Coordinators must not respond to the following requests and must immediately route such requests to a headquarters Public Disclosure Coordinator for response.
 1. Requests for reports collected at the state office; for example, statewide Health and Safety Report, FamLink reports generated at the state office level.
 2. Requests for information from more than one region where consistency of information is necessary.
 3. Requests from employees.
 4. Especially sensitive issues are best handled at Headquarters:
 1. Requests from the media, including, newspapers, television, and radio;
 2. Requests from attorneys, which may involve potential lawsuits;
 3. Requests from legislators;
 4. Requests involving "hot" cases or those generating controversy in the community; and
 5. Other cases which may be of a hostile nature or where there is need for headquarters staff and Media Relations to be aware of the request.
 5. When there is a question about whether the preparation should be done at the regional or headquarters level, the regional Public Disclosure Coordinator will consult with a headquarters Public Disclosure Coordinator. or the Public Disclosure Manager
4. Public Disclosure Coordinators must consult with an assigned AAG and/or the DSHS Public Records and Privacy Officer when an issue regarding the release of information is not clear.
5. If the person requesting disclosure disagrees with the decision of a Public Disclosure Coordinator, the person may petition for review of the decision denying disclosure.
 1. If the petition is for the review of a decision made by a regional Public Disclosure Coordinator, it must be sent to a headquarters Public Disclosure Coordinator for review.
 2. If the petition is for the review of a decision made by a CA headquarters Public Disclosure Coordinator, it must be sent to the Public Disclosure Manager or their designee for review.

13722. Public Records Request - Responsibilities of all CA Staff

CA staff must comply with the provisions of WAC Chapter 388-01 and DSHS Administrative Policy No. 5.02 - Public Records Requests. These responsibilities include, but are not limited to:

1. A public records request may be made to any staff and does not need to be made in writing or on a specific form. If a CA staff receives a public records request, or believes they may have received a public records request, they must forward that request immediately to a CA Public Disclosure Coordinator. Not doing so may result in fines to the agency under the Public Records Act, RCW 42.56.
2. When a Public Disclosure Coordinator requests records staff are required to provide all records, whether disclosable or not, to the Public Disclosure Coordinator. It is the responsibility of the Public Disclosure Coordinator to determine what may be disclosed.
 1. Failure to provide all responsive records may result in fines to the agency under the Public Records Act, RCW 42.56.
3. If a public records request is made at a time when such record exists but is scheduled for destruction, the department must retain possession of the record and may not destroy or erase the record until the request is resolved. WAC 388-01-060; RCW 42.56.100.

13726. Disclosure to Client's Representative

When a representative designated by a client requests the client's record, the request must be accompanied by a written release signed by the client. The representative may be an attorney, legal guardian or lay representative. The written release must include the following:

1. The identity of the person(s) or organization(s) to whom disclosure is to be made;
2. An identification of the record, or portion thereof, to be disclosed; and
3. A statement of when the authorization for disclosure expires.

13790. Disclosure for Program and Other Purposes

1. For purposes directly related to the administration of department programs, information shall be disclosed between offices of the department, unless prohibited by 45 CFR 205.50 or other law.
2. For purposes directly connected with the administration of department programs, information may be disclosed by the department to outside agencies, unless disclosure is prohibited by law. Agencies or individuals receiving such information are subject to the same standards of disclosure as are required of the department.
3. To the extent not otherwise prohibited or authorized by law, inquiries from agencies outside the department will be honored only if written and only if the client's authorization is included in the request. WAC 388-01-070

13797. Purpose

1. These forms were developed to meet the various federal and state statutory and regulatory requirements on a Department-wide basis, as confirmed by the review of program Assistant Attorney Generals (AAG).
2. The two forms provide uniformity and are valid Department-wide. CA will use the forms in place of any existing forms. Staff are to accept these forms as valid and not ask a client to complete a different DSHS form if one of these two has been properly executed.

1. The Consent Form 14-012 allows programs to share information about mutual clients to coordinate service delivery.
2. The Authorization Form 17-063 permits DSHS to release client records and information to a third party, including an attorney, legislator, or relative.

137110. Practice Considerations

1. The social worker provides, subject to the constraints outlined above, a copy of all case file information, relevant to a court proceeding, to a child's parent(s), guardian, legal custodian, or legal counsel. Information which the department reasonably expects to introduce to support the petition is considered relevant. The social worker will provide a copy, free of charge, within 20 days of a written request or prior to the Shelter Care Hearing, whichever is sooner.
2. Clients with proper identification have the right to look at their records if they request to do so. They also may challenge the accuracy, completeness, or relevance of statements. Sources of CPS complaints remain anonymous, and their names must be purged from the record prior to the client's review.
3. The social worker offers language interpreter services to clients who are unable to read the case record information.
4. All material presented at a dispute hearing is open to examination of the client and his/her representatives, even though such material would ordinarily be considered confidential.
5. Staff subpoenaed to appear in court shall not take the social service record unless it is also subpoenaed, at which point the social worker consults with the assigned Assistant Attorney General.
6. No individual shall make available outside the department a partial or complete list of service recipient names or address. Social Service Payment System (SSPS) reports containing client identifiers are confidential.
7. For adoption records, after the petition for adoption is filed, information, except medical reports, in the child's record may be released only by written order of a Superior Court.
8. With respect to the service records of children and youth who are under the jurisdiction of the court, the requirements outlined in the Case Services Policy Manual, Chapter 2000, section 2150, are to be followed. RCW 13.50.100
9. If a juvenile, his/her parents, or their attorney makes a written request asking the department about the existence and content of custody, or care records, the Area Manager completes the following steps.
 1. Makes written response to the inquiry within 10 working days after its receipt. The department provides to the juvenile, the parents, or attorney making the inquiry information regarding the location, nature, and content of any records in the department's possession. A juvenile, the parents, or the attorney, wishing to challenge the information contained in the department records, must notify the department in writing, providing:
 1. The name of the juvenile.
 2. A statement of those portions of the record alleged to be inaccurate.
 3. If retention of the record is being challenged, a statement as to why the record should be destroyed.
 2. Reviews the notification of challenge and responds in writing within 30 calendar days. The response will indicate the corrections which have been or will be made or shall state the basis for denial of any requested corrections. If appropriate, the response will also include a statement indicating whether the records have been destroyed or transferred to another juvenile justice or child care agency.

3. Notifies the juvenile, the parents, or their attorney that, if they dispute the department's response, they may seek an administrative review of the decision as provided in the Administrative Procedure Act.
10. CA staff removing records to an alternative work site must maintain security and confidentiality of information contained in records. To maintain security and confidentiality, information contained in FamLink or mobile devices will be printed on CA network equipment

13907. Storage and Retrieval of Case Records

1. Office Request Coordinator- Is the person(s) designated by the office as authorized to request records or obtain information from records stored at RRC.
2. Records Coordinator - Is the person(s) designated at HQ and in each local office to have responsibility and authority for the retention and destruction of all files.
3. Instructions for record storage, retrieval and destruction using the Records Retention Center bar code system can be found at the [Records Retention Center](#).
4. Non-essential volumes of an open case that are too large for the worker's cube can be sent to Records Retention Center for storage. The master files clerk must ensure that the case destruction date matches that of the other volumes when the case is closed. **If non-essential volumes are sent to the Records Retention Center, care must be taken to ensure that they are not prematurely destroyed.**

13908. Destruction of Records

1. Destruction lists sent from the Records and Retention Center are to be reviewed every month by the master files clerk/supervisor and final approval for destruction sent to the Records and Retention Center.
2. Final destruction requires that any related electronic records in FamLink be purged.

14112. Posters and Brochures

1. The following posters must be displayed in each CA client reception area:
 1. Multilingual Interpreter Services, DSHS 24-019(X).
 2. Non-Discrimination posters in English, Cambodian, Chinese, Laotian, Spanish, and Vietnamese, DSHS 24-007.
2. Non-Discrimination Policy brochures in English, Cambodian, Chinese, Laotian, Spanish, and Vietnamese, DSHS 22-171(X) must be available for clients in each reception area.
3. Supplementary client information and brochures are available from the DSHS Forms and Publications Warehouse in a variety of languages.
 1. Each CA office is to maintain a supply of bilingual information for clients that is reflective of the languages spoken in the local service area.
 2. Following is the Translation Color-Coded System used by the department:
 1. SPANISH - Goldenrod
 2. VIETNAMESE - Yellow
 3. CAMBODIAN - Light Bluerod
 4. VIETNAMESE - Yellow
 5. LAOTIAN - Lime Green
 6. HMONG - Tan
 7. CHINESE - Orange
4. The Equal Employment Opportunity is the Law poster is to be displayed in the employee work area of each office.

152063. Procedure

1. Children's Administration staff shall use the form IBM Mainframe Security Access Form for Children's Administration to identify and authorize needed security. The individual(s) creating system user ID's need to have this information two weeks before a new employee begins work in order to have security in place before the employee's first day on the job.
2. This form must be included in entrance and exit interviews, filled out by the Human Resource Consultant Assistant (HRCA) or the supervisor of the new employee, and emailed to ISSD Data Security one week prior to the employee's first day and no more than one week after their last day of employment.
 1. Creating a user new to the Administration
 1. At least two weeks before the employee's first day, a user ID needs to be created within the CAMIS system. This ID will be generated from ISSD Data Security. This will generate the seven character alphanumeric log-in ID that will be used with the other systems. The job classification/title and office information for the user is to be entered at the time this ID is created.
 2. If the user is hired into a new position, using the ID generated in CAMIS, a new user profile will need to be created in the DSHS Domain by a Children's Administration Service Desk person and a user directory created. Within this profile, the local ITSS will add the groups needed for them to access necessary information and printing capabilities. This will give the user access to the Local Area Networks (LAN) and the mainframe where CAMIS resides.
 3. If the user is in an existing position that has been vacated, any files not relating to this position should be removed from the file server by the region's or headquarters' ITSS or exiting employee's supervisor. Any files that are related to the position should be transferred to the new employee by the region's or headquarters or exiting employee's supervisor. Also using the ID generated in CAMIS, a new user ID will need to be created in the Exchange e-mail system by the Children's Administration Service Desk.
 4. If the user has another ID created by another agency, that ID must be used only if that ID is available in the CAMIS system.
 5. e. If the user needs security for specific CAMIS applications, the supervisor submits via memo the request for security training to the Children's Administration Service Desk.
 2. Moving a User Within the Administration From One Position to Another
 1. Since the user should already have a CAMIS user ID and NT domain ID, Children's Administration Headquarters Help Desk staff needs to update the CAMIS and NT ID's by changing the office information. The NT ID information will be updated by the local/regional ITSS.
 2. An e-mail ID may need to be created if the user is moving to an office with a different e-mail domain.
 3. Deleting a User From the Respective Systems
 1. CAMIS -- When a user leaves Children's Administration, the HRCA notifies the Children's Administration Help Desk and the local/regional ITSS within one week of the employee's departure.
 2. The Children's Administration Service Desk will update the CAMIS account information by putting a date in the Inactive Data field. This will

trigger the events to remove access security and ensure the security integrity of the CAMIS system.

3. The local/regional ITSS will transfer any mission critical files from the existing employee to the employee's supervisor (if necessary) and then delete the user's profile from the e-mail system and file server.
4. If the person is remaining with the administration, the employee's CAMIS ID remains active.
5. DSHS Domain -- When a user is leaving Children's Administration permanently, the DSHS domain ID is to be deleted. If the user is leaving the administration temporarily, the DSHS domain ID is to be disabled until the user returns.
6. E-mail -- The Exchange administrator also deletes the e-mail ID at this time.
7. Other Systems - When a user no longer needs access to other Information Services, the HRCA or supervisor notifies the Children's Administration Service Desk, who will remove the user's access to those systems.

15207. Patch Notification Response Procedures (PNRP)

152071. Purpose

1. The purpose of this document is to outline the necessary resources, steps and methodology needed to successfully classify and respond to virus definition file updates and software patch upgrade notifications from vendors.

152072. Applicability

1. The standard applies to all automation systems supported by the Children's Administration Technical Services (CATS) Division and all CATS Staff.

152073. Definitions

1. Patch: A temporary addition to a piece of code, usually as a quick-and-dirty remedy to an existing bug or misfeature.
2. Network: Refers to all automation resources maintained by the Division and includes hardware, software and infrastructure.
3. Patch Tracking Log: Electronic log used to track all actions taken in response to a Patch notification.
4. Virus Definition File: An electronic file that includes the information necessary for Antivirus Software to detect and repair viruses.
5. Maintenance Rollup Package: Refers to a collection of enhancements that are pushed out to PCs at regular intervals. These are generally non-critical and do not require immediate action.
6. CA Patch Notification Distribution List: E-mail distribution list that contains the names of all CATS staff that require notifications during patch procedures.

152074. Resources Requirements

1. CA Patch Notification Distribution List
2. Patch Tracking Log

152075. Procedures for Patch Application

1. Upon receipt of notification of a Patch, the Technical Support Services Manager or designee and Senior Technical Analyst must determine the level of impact on the CA Network. There are 3 Impact Levels it can fall under; No Impact, Minor Impact, Critical Impact.
 1. No Impact means our systems are not vulnerable or fit the scope of the patch (i.e. we do not use that software or function) and it cannot be exploited on our network.
 2. Minor Impact means we may fit the scope but the patch does not fix vulnerability, or the fix is for non-critical functionality improvements (i.e. enhancements to software).
 3. Critical Impact means we fit the scope of the patch and not applying it could result in a negative impact on our network and systems resulting in loss of productivity.
2. Upon determination of impact level, the Technical Support Services Manager or designee and Senior Technical Analyst will take the following actions. All actions must be entered into the Patch Tracking Log.
 1. No Impact. If the patch falls in this category, make notation in Patch Tracking Log and communicate info to CA Patch Notification Distribution List.
 2. Minor Impact. If the patch falls in this category, communicate that info to the CA Patch Notification Distribution List and add it to the regular Maintenance Rollup Package.
 3. Critical Impact. If the patch falls in this category, the Senior Technical Analyst or designee will communicate that info to the CA Patch Notification Distribution List and invoke the Expedited Patch Application Plan (EPAP).

15209. Network Emergency Response Procedures (NERP)

152091. Purpose

1. The purpose of this document is to outline the resources, steps and methodology necessary to successfully resolve a network-wide emergency.

152092. Scope

The standard applies to all automation systems supported by the Children's Administration Technical Services (CATS) Division and all CATS staff.

152093. Definitions

1. Event - an unplanned, non-specific issue that causes limited or a complete lack of computer and/or network functionality including viruses, natural disasters, fires, flooding, etc.
2. Remote Device - any laptop, notebook or tablet pc that can be removed from the network and used by Children's Administration staff
3. Shared Emergency Administrative (ESA) Account - an account created prior to an event and given full administrative privileges on every machine in the Children's Administration network.

152094. Resources Requirements

1. Complete CATS telephone, pager and personal number lists updated on a quarterly basis.
2. Standard communication device for CATS Staff that incorporates paging, cell phone and walkie-talkie or direct connect type capabilities not dependent on telephone land lines.
3. List of local office non-CATS, ISSD and DIS staff that could assist in an emergency.
4. SEA account.
5. Listing of remote computers and their users or custodians.

152095. Upgrade/Change Procedures

1. All communication during an Event will occur in the following manner:
 1. The communication "tree" will mimic the chain of command for both upward and downward communication.
 2. Communications will occur at regular intervals during the event or as needed. The intervals will be determined by the CATS Director, Technical Support Services Manager or designee at the time of the Event based on its severity.
2. If any CATS staff suspects we are under the influence of an Event, that person will immediately contact the Technical Support Services Manager or designee with a description of the event, its symptoms and possible solutions.
3. If an Event is verified by the Technical Support Services Manager or designee, all appropriate staff will be notified by any means available. An interim stop-gap solution will be provided with the communication to prevent further damage to the network or loss of productivity.
4. The Technical Support Services Manager or designee will identify a NERP team. The NERP team will develop, document and prepare a solution for distribution as soon as possible.
 1. Depending on the severity of the event and the solution necessary, the Technical Support Services Manager or designee may summon the assistance of Non-CATS office support staff (see attached NERP Contacts list).
 2. If necessary, the SEA Account could be implemented. Please see the Shared Emergency Administration (ESA) Account Implementation Plan.
5. CATS and/or Office Support group will proceed to apply the fixes to equipment according to the priority identified by each office or as directed by their immediate supervisors. In the event that a priority list is not available from the office, the default priority will be as follows:
 1. Intake
 2. Social Workers
 3. Clerical
 4. Supervisors
 5. Management
6. Once the response is underway, the Technical Support Services Manager or designee will provide the Regional Management with a summary of the event, the plan to repair damage and an estimated time of completion.
7. If the solution involves computer software upgrades, once the local network has been protected, each CATS staff member will need to contact their office's remote users to ensure that a re-infestation does not occur via remote, non-wired or "checkout" equipment. If CATS staff is unable to reach a user who has a "remote" device they will revoke network rights for that device until such time an authorized staff member can physically test the device and ensure its safety on the Children's Administration network.
8. Upon completion of the response, CATS Management should conduct a review to determine the cause of the Event and how to improve processes and procedures to prevent such an emergency and/or improve the response in the future.

15210. Shared Emergency Administration (SEA) Account Policy

152101. Purpose

1. The purpose of this document is to outline the administration of a Shared Emergency Administration (SEA) account. This account is to give Non-Technical Staff, office site assistants or other designated office workers full administrative privileges to Children's Administration desktop computers at the Local Administrative Level in response to an Event that requires software, patches or other solutions be applied to each computer locally and can't be distributed electronically.

152102. Applicability

1. The standard applies to all automation systems supported by the Children's Administration Technical Services (CATS) Division and all CATS staff.

152103. Definitions

1. Local Administrative Level- refers to permission specific to one piece of equipment and not across the whole network and/or domain.
2. Event - Non-specific issue that causes limited or a complete lack of computer and/or network functionality.
3. Non-Technical Staff - Refers to a staff member in each office who has been identified as a resource for CATS to use as needed to resolve technical issues.
4. Remote Tools - Any utility or software program that allows administration of a resource from other than its own counsel. (i.e. SMS, Remote Desktop, etc.)

152104. Resource Requirements

1. Complete list of non-technical staff as designated by the local CATS staff
2. SEA account and password established and installed on equipment

152105. Procedures

1. Upon determining that the event is of a nature that requires assistance from non-technical staff, the Technical Support Services Manager, Area Technical Manager or a designated CATS staff member will distribute the SEA account login name and password (via fax or other method) through the local ITSS to the non-technical staff.
2. Once the event has been resolved, the Technical Support Services Manager or his designee will change the password for the SEA account via Remote Tools and/or manually on all affected CA equipment preventing in order to prevent its continued and unauthorized use. This new SEA account password will be shared only with the Technical Support Services Manager, Area Technical Managers and Senior Technical Analyst.

15211. CA Information System Disaster Recovery Procedures

15212. Securing Unattended Computer Terminals (06/16/06)

152121. Purpose

1. To ensure our adherence to DSHS Administrative Policy 05-01 and to provide a policy for CA regarding the securing of computer terminals that provides access to confidential and mission critical data.
2. Confidential information includes all personal information (e.g., name, birth date, SSN, etc.) and case data (e.g., case number, type, allegations, etc.) relating to CA clients.
3. This policy is necessary to ensure that the administration is in compliance with the Washington State Department of Social and Health Services (DSHS) Information Technology Security Policy Manual (ITSPM), Chapter 3, Classifying and Protecting Data and IT Resources.

152122. Applicability

1. This policy applies to all CA employees, whether working in CA offices, in private homes, or when connecting to the CA network remotely via wired or wireless access, whenever using electronic equipment to access client confidential information.

152123. Standard

1. Due to the critical and confidential nature of the data used by the Administration, it is necessary that all data files and information that are confidential or mission critical in nature are secure when staff leave their terminals unattended.
2. Employees must log off from CAMIS if they do not intend to use CAMIS for documentation or review of data for any period in excess of 90 minutes. CAMIS will automatically log off any user who has remained "idle" in the system for longer than 90 minutes. The automatic log off is necessary to assure data security, to allow active workers freedom to access the system, and to keep the system cost efficient. System users creating or updating CAMIS records, reviewing existing records, and/or performing searches in the system will not be involuntarily logged off if they perform any of these activities at least once every 90 minutes.
3. Employees who use computers that access the Local Area Network (LAN) must either log off or lock their workstations by using the built-in lock feature within the operating system when they leave their terminals unattended. Additionally, an auto-locking feature will be implemented on all CA computer equipment so that following ten (10) minutes of user inactivity the computer will automatically lock with a password.
4. For instructions on how to log off of the system or lock the computer with a password, staff should contact their local Systems Support Specialist or the CA Service Desk via email or telephone.
5. Computer terminals within CA will not be set up to automatically enter the user ID and password into either the LAN or CAMIS system via a macro or program.