

**EOCF Policies
Confidentiality of Information**

Policy Number: A-401 Old Policy Number: ADM008	Effective Date: 3/26/2003 Revised: 2/15/2005	Page # 1 of 4
Executive Director Approval Date: 3/26/2003	Policy Council Approval Date: 3/26/2003	Governing Board Approval Date: 3/25/2003
Proposed Effective Date:	Notes:	Draft Number: N/A

COMPONENT: Administration

POLICY STATEMENT: EOCF maintains confidentiality of child, family, and personnel files in "hard" and electronic format. Only appropriate staff determined by their job assignment will have access to child, family, and personnel files. Child, family, and personnel files are kept in locked desks or file cabinets.

PERFORMANCE OBJECTIVE: To inform all personnel of the procedure for maintaining confidentiality.

PROCEDURES/GUIDANCE:

Child and family files:

1. Child files (hard copies) will be kept in locked file cabinets and only be accessible to the staff assigned to the child and the child's parent or legal guardian.
2. New child enrollment applications and information on wait lists will be maintained in locked cabinets. Staff working in the Outreach, Recruitment and Enrollment components will maintain confidentiality of information.
3. Information in child files will only be discussed with parents or legal guardians.
4. Child and family information, such as names, phone numbers and addresses, will not be given to anyone other than appropriate program employees, for official use, without permission.
5. Parents must give written permission to the appropriate staff before information will be shared outside of EOCF. Information will only be shared with EOCF staff on a need to know basis, during routine monitoring by supervisors or MDT staff, or federal and state review teams. The only exceptions will be in the case of reporting child abuse and neglect, or if information is subpoenaed by a court of law.
6. Each staff member assigned to the child and family will be responsible for maintaining confidentiality of child and family files at each center.

7. Any breach of confidentiality will be grounds for disciplinary action up to and including termination.
8. At the end of each program year, all files will be brought to and secured at Suite 214, ORE component area.
9. Child and family files will be destroyed after five years.
10. A roster of children and families served, including name, address, telephone number and child's Social Security number, will be maintained for historical purposes and longitudinal studies. This information will be secured at Suite 214, ORE component area.
11. A parent roster, for use by parents for program parent activities, will contain the names, address and phone numbers of only those parents who have given written permission.
12. Information on children and families will be kept confidential, but not limited to:
 - Files of children and families
 - Records including health, social service or educational data on children
 - Rosters and file boxes containing any information on children
 - Salary and income information on program families
13. Staff such as supervisors and resource team members who regularly access files for review sign off on a "File Access Log."
14. Staff may copy information from the child files **only** for a parent who has legal or physical custody of the child, or the person who is the legal guardian of the child.
15. Verbal discussion of confidential information among staff will **only** be done to conduct the delivery of services to children and families.

Electronic records of children and families:

1. Child and family information entered into EOCF's database system, currently ChildPlus, may be directly accessed by staff by permission of the Executive Director, Deputy Director, Director of Child and Family Services (P-3 and 3-5) and Database Analyst.
2. Staff, such as directors, managers and supervisors, may have indirect access to ChildPlus information through data reports.
3. Staff who are given permission will be issued a user identifier code and password.

Personnel files:

1. The Human Resources Manager will maintain personnel files in a locked room in locked cabinets.
2. Records will be available to the Executive and Deputy Director, Human Resources Manager, directors, managers, and Board of Directors. In the case of internal recruiting, transfers or job promotions, the hiring supervisor may have access.
3. Staff may review their own personnel file in the personnel office, currently located in Suite 207.
4. Employee information, such as address and phone number, will not be given to anyone other than appropriate program employees for official use without permission.
5. Information to be kept confidential includes, but not limited to:
 - Personnel files
 - Health and medical files
 - Salary and income information
6. Personnel files will be kept for seven years after an employee leaves.
7. Supervisors must assure that all confidential information is securely locked when they are out of their offices.

Electronic records of personnel files:

1. Staff information will be maintained by Human Resources in a database, currently MS Access. Only Human Resources staff, Executive Director, and Deputy Director will have access to the database. An offsite backup to the database may be maintained in a secure location at the discretion of Human Resources, Deputy Director or Executive Director.
2. Information released from the database will be limited to those staff who need the information to perform their jobs. Staff must consent before any personal information is released to other staff or external agencies. Any information released will be used for official purposes only.
3. Reports that do not contain personal information may be released to outside organizations such as grantor or partner agencies.

Email Confidentiality Procedure:

The purpose of this procedure is to inform all staff on email transactions to ensure maximum protection of confidential information. EOCF attempts to provide secure and reliable email services. Users of EOCF's email system are expected to follow sound professional practices in providing for security of electronic email records, data, application programs, and system programs under their jurisdiction. Since such professional practices and protections are not foolproof, the security and confidentiality of electronic mail cannot be guaranteed. Furthermore, operators of email services have no control over security of email that has been downloaded to a user's computer. As a

deterrent to potential intruders and to prevent misuse of email, email users should at minimum, follow the guidance provided.

1. Always use other means of communicating confidential information if the situation permits such as, hand delivery, phone conversation, or agency mail in confidential envelopes. You can inform the recipient by email the nature of the information being sent without using a name of a client.
2. All computers that store confidential information must have password protection.
3. Computer users must log out when leaving a computer unattended.
4. Whenever possible, alert the recipient of a confidential email that it is coming.
5. All email communication containing confidential information is to be labeled "confidential". Information is considered confidential whenever it contains a client name.
6. When applicable, use only client initials rather than a name.
7. Delete all confidential emails written within 72 hours of sending or receiving them. Delete them from the "deleted Items" file in Outlook as well as the "Sent" and "In Box".

**EOCF
Confidentiality of Information
Employee Agreement
(Policy #A-401)**

To be returned to Human Resources for filing in Employee file.

I, _____, have read EOCF's
(print name)

Confidentiality of Information Policy (Policy #A-401) as revised in February 2005. I assume responsibility and liability for violations of a child and family's or co-worker's rights to confidentiality resulting in my failure to implement this guidance.

Employee's Signature

Date

HS Performance standards referenced: 1304.51(f-g), 1304(h)(1)
ECEAP Performance standards referenced: 1.100
Washington State Child Care Licensing Requirements