Record Keeping and Security of Child Records

Security

Information contained in child and family records for Head Start, Early Head Start, and ECEAP (both written and electronic) must be secured in a confidential manner at all times. Confidential information must never be left unlocked in an unattended room and should be locked away when not in use. This includes all forms of external drives and removable media.

Child and family information is collected and retained in both paper and electronic files which supports staff at the classroom level in their work with children and families.

It is each person's responsibility to ensure that the data they are working on is not read or handled by anyone who has no need to do so. In the event that confidential data is lost or even suspected to be lost, the direct supervisor must be notified immediately.

Files, whether paper or electronic, must contain all current information and be available for:

- Comprehensive Service Reviews (CSR) and mini CSR's
- Home Visits/Center Conferences
- IEP Meetings
- Behavior Plan Meetings
- Record Reviews (program and outside reviewers)
- TS Gold Checkpoints
- Child or family legal and/or crisis issues
- Monitoring purposes

Sensitive Records

When documenting sensitive issues that might cause problems for a parent or family, specifically CPS & DV (domestic violence), please document and file accordingly:

Documentation is kept in the child's file at the center. Copy of documentation is brought to the OESD's Early Learning Department to be filed in the child's Administrative File.

Access of Families to Their Files

Unless legal documents state otherwise, both biological parents and legal guardians have the right to access their child's file. Information on the family, such as Home Visit Plan, Family Partnership Agreement, etc. is accessed only by the parents(s) or guardian who was involved, e.g., the parent who participated in the Home Visit.

Other Access to Child Files

CPS workers, court-appointed Guardian Ad Litems, and attorneys with subpoenas may have access to the child's file. They must sign the "Action Log" form located in the file and will document the reason for their access. Center staff and support staff at the center will have regular access to the child files and are not required to sign the "Action Log" form.| Administrative Assistants will have regular access to files that come into the OESD and are not required to sign the "Action Log" form. Teaching staff from ECEAP or Head Start Partnership sites from School District classrooms (i.e., Green Mountain's Developmental Preschool) with enrolled ECEAP or Head Start children are considered authorized staff with regular access. All other program staff will sign and identify the reason for accessing the file.

Security of Paper Records

All child files must be kept in a locked cupboard or file cabinet. Working documents related to child and family information must also be secured in a locking drawer, etc. when not in use.

Transportation of Child and Family Files

All child and family files must be secured during transit when being transported out of the classroom or the OESD. Common reasons for transporting all or part of a file include Home Visits, transferring the file to another classroom or Home Visitor when the child and family have moved, transferring enrollment, USDA information, or other confidential information to the OESD. This list is not exhaustive and there may be other valid reasons for the removal of the file from the classroom to another location.

Security of Electronic Child and Family Files

Computers are available to staff to expedite the documentation of services to children and families. It is each person's responsibility to ensure the physical security of the media they use, including storage of files on PCs and other removable media, by locking it in a file cabinet or drawer.

Each staff member is assigned a unique user name and password that they will use to log on to a computer. Staff must log on and off using their own user name and password. If they access a computer that has been left open by a previous user, it is their responsibility to "log off" that user and "log on" with their own name and password. Sharing of user names and passwords is strictly prohibited. Passwords must not be written down or disclosed to other individuals.

When a computer is re-assigned from one location to another, technology staff will ensure that data no longer resides on the computer and that accounts are disabled.

When a computer is prepared for surplus sale, technology will use third party software to securely wipe personal data that is on the computer.

Confidential information concerning children and their families will be removed from the computer at the end of the program year or earlier if applicable. Information relevant to specific children and/or families must be printed and placed in the child's file. Removal of confidential information is accomplished by deleting the file into the "trash" icon on the desktop and emptying of deleted items from the "trash." Confidential information on external storage devices must be erased before re-use.

Resource: Family Privacy Act and Family Educational Rights and Privacy Act.