Confidentiality Policy for Staff

As both a family agency and a school, families with children receiving services from VCLC are entitled to privacy and staff is required to respect the confidentiality of their information. Confidentiality is a concept that ensures privacy and protection against disclosure of personal information. The way privacy and confidentiality is respected is an important factor in establishing trust between our staff and our families. Respect for confidentiality is required by FERPA, the Federal Family Education Rights and Privacy Act and a mandated responsibility as an employee of Variety Child Learning Center.

In order to work and plan together effectively, colleagues sometimes share sensitive information with staff with “a need to know.” This material needs to be handled respectfully in a way that is relevant to planning and problem solving. Any information shared with your team members needs to remain within your team.

- VCLC policy, in keeping with applicable regulations, is that the confidentiality of client records and parental access to such records is permitted only as directed in FERPA, as currently amended.
- Identifiable data, other information or records pertaining to individual students may not be disclosed by any employee of the school to any person other than the parent of the student except as directed in Part 99 of Title 34 of Federal Regulations.
- Access to confidential written material or records is restricted, according to FERPA, to professional staff specifically involved in that child’s care. Whenever a staff member uses a child’s file, they must sign the Access to Records form in the front of the child’s folder and the Access to Records form in the Master Log.
- Staff must be aware of being overheard and not discuss confidential information in hallways and around the building or outside of school premises. Discussing a child’s situation, outside of school, even without disclosing the name is a very serious violation of school policy.
- Sensitivity and restraint must be used when responding to parents who speak or ask questions about other children or families.
- No member of VCLC staff shall take confidential information from the central student files except when it is needed to provide services to the student. All confidential records must be kept in locked files. Staff log notes, and any identifying information that must be transported for IFSP/IEP meetings need to be transported in a closed envelope.
- Records/any papers that have personally identifiable information must be disposed of by using a shredding machine.
- Staff members may not take photos of the children for their personal use. Employees are not permitted to post information about a family or photos online, in blogs, websites or social networking sites, including but not limited to, Facebook, My Space or chat rooms whether the information is positive or negative. This information is part of respect for confidentiality and a mandated responsibility as an employee of VCLC.
- When information about a child/family is contained in records that include information about multiple children, only information pertaining to that child/family can be released. Personally identifiable information about others must be protected. Only information appropriate to a request should be released. Extraneous or sensitive information about the child and family should be protected, through deletion of identifiable information about others.

Independent Contractors

VCLC independent contractors are responsible for following VCLC Confidentiality Policy (updated April 2010). Independent contractors must maintain their original treatment logs and reports in a locked file at home. This information is subject to audit upon request by authorized parties.
 Variety Child Learning Center (VCLC) maintains a password protected network of computers and communication systems to support the conduct of operations. These systems include PCs, software, telephone, voicemail and electronic mail systems, all centralized computer equipment, networks and access to the internet. Although limited personal use of our system is allowed, subject to the restrictions outlined below, no use of these systems should ever conflict with the primary purpose for which they have been provided or applicable laws and regulations. Each user is personally responsible to ensure that these guidelines are followed.

Technology

All data in our computer and communication systems (including documents, and other electronic files, email and recorded voicemail messages) is the property of VCLC. VCLC may inspect and monitor such data at any time. VCLC may also monitor usage of the internet by employees, including reviewing a list of sites accessed by an individual. No individual should have any expectation of privacy for messages or other data recorded in the system, including documents, e-mails or messages marked "private," which may be inaccessible to most users but remain available to us. The deletion of a document or message may not prevent our access to the item or completely eliminate the item from the system. Likewise, no individual should have any expectation of privacy in terms of their usage of the internet. In addition, VCLC may restrict access to certain sites that it deems are not necessary for our purposes.

VCLC’s Computer Network System is protected by a CISCO MX 100 Security Appliance, firewall devices, Trend Micro Enterprise Products which include Office Scan virus software for the clients, CISCO Web Filtering for internet use and Scan Mail for Microsoft Exchange email use. The network is monitored, maintained and updated on a regular basis. All security patches are downloaded and installed on individual work stations as they are received. The network is backed up daily, weekly and monthly.

Network security is in place. Administration established a hierarchy of accessibility to user-areas, with supervisors having access to their employees’ user-areas. Employees do not have access to their supervisor’s user area.

Each VCLC employee who has the need for a computer is given a user-name and creates a password of at least eight characters (a combination of letters and numbers). Employees must sign in to access their user area. Software applications that contain child, family and/or staff information are password protected. Administration decides the level of access staff have to various software applications.

General Email Policy and Procedures

VCLC’s email system is in place as a tool for communication to perform tasks related to VCLC’s mission. VCLC’s email system is hosted on a secure VCLC Email Server (Microsoft Exchange) which is inside the VCLC network and protected by network security systems. Any outside the network access to VCLC’s email system is secured by a HTTPS (Hypertext Transfer Protocol Secure) connection which provides encryption and secure identification. An account for each employee with a need to use email is set up. The employee selects a password of at least eight characters (a combination of letters and numbers).

VCLC requires all employees to use their VCLC email account for work-related communications. If employees are using email to submit progress notes, quarterly, six-month, annual review reports as well as evaluations, they are required to use their secure VCLC email account. Supervisors are not to accept any reports transmitted from a personal account.

All emails sent by an employee must include the following statement:

This transmission may contain privileged and confidential information. It is intended only for the use of the person(s) named above. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution or duplication of this communication is strictly prohibited. If you are not the intended recipient, please contact the sender and destroy all copies of the original message.
FERPA specifies that email communications with parents and others authorized by the parent are considered “education records” and should be maintained in the same manner as other children’s records. In accordance with New York State Department of Health Early Intervention Email Policy, VCLC’s Compliance Manual, VCLC’s Personnel Manual and VCLC’s best practice policies and procedures, families are informed about the use and the risks of using email when communicating information about their child. Parents are asked to sign a written consent which identifies the email address to which the communication is to be sent and the parties who may correspond with the parent via email, and who may receive or be copied on such emails. A copy of this consent is kept in the child’s records. Employees must use their VCLC email account, not their personal email account.

In order not to impair the systems capabilities but to also increase its efficiency, the following policies and procedures are being conveyed.

Confidentiality
VCLC’s confidentiality policy applies to all computerized information including information on the email system. Employees must not permit others to have unauthorized access to the email system.

Data Security
Refrain from using the email system as a medium to transfer our confidential, copyrighted, or licensed material to unauthorized recipients. Emails containing such material must be cleared through a supervisor.

Employees may not send email containing VCLC information to their personal email accounts or to friends or family email accounts. Sending such information outside our system violates our confidentiality policy.

Employees are prohibited from posting any VCLC information on financial bulletin boards, social networking sites including but not limited to Face Book, My Space or chat rooms whether the information is positive or negative.

Employee Blogs
VCLC recognizes that many employees may maintain web logs or "blogs" in their free time. While VCLC does not prohibit maintaining such blogs, employees are prohibited from posting entries or comments to their personal blogs, or to other blogs on the Internet, during working hours and using VCLC equipment. In addition, employees are expected to comply with our policies against harassment and maintaining confidential information when posting information or comments on blogs.

Faxing Information
VCLC maintains fax machines to support the conduct of operations. Although limited personal use of the system is allowed, no use of these systems should ever conflict with the primary purpose for which they have been provided or applicable laws and regulations. Each user is personally responsible to ensure that these guidelines are followed. The recipient of a fax must be called to ensure that the authorized person is the direct recipient of the fax. Each fax must include the following statement:

This transmission may contain privileged and confidential information. It is intended only for the use of the person(s) named above. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution or duplication of this communication is strictly prohibited. If you are not the intended recipient, please contact the sender and destroy all copies of the original message.

Scanning Documents
Each user of a fax or copy machine is personally responsible to ensure that these guidelines are followed. When scanning a document to email or fax to another party, the employee should send the scanned document to his/her VCLC email address. A cover sheet should be generated that includes the following statement:

This transmission may contain privileged and confidential information. It is intended only for the use of the person(s) named above. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution or duplication of this communication is strictly prohibited. If you are not the intended recipient, please contact the sender and destroy all copies of the original message.
The scanned document can then be emailed or faxed. If the document is faxed, the sender should contact the receiver to let them know that a fax is being sent.

Article 27-F of the New York State Public Health Law

Article 27-F strictly protects the confidentiality of information about the people who have HIV-Infection, or who have considered or undergone HIV testing. In accordance with this law, providers are obligated to maintain the confidentiality of this information if learned during the course of providing services so as to ensure that the person is not discriminated against as a result of his/her HIV positive status. As such, the identity of any child with HIV infection cannot be disclosed to anyone without specific consent to the release of such protected information by the parent or legal guardian. This information may not be disclosed verbally or contained in any written records (e.g., evaluation, progress reports, etc.)

The consent for the disclosure of this confidential information can only be made by completion of the Authorization for Release of Confidential HIV Related Information form. This form must be fully completed by the parent or legal guardian and must include the following information:

- to whom disclosure can be authorized
- the reason consent for disclosure is given
- the time period during which such consent will remain in effect
- the signature of the parent or legal guardian of the child
- the date signed.

When consent for disclosure is given, information regarding the child will be forwarded to the specific individual identified on the consent form. In addition, a copy of the Re-disclosure of Confidential Information notifying the individuals that confidential information has been disclosed to them, must also be provided. Any unauthorized further disclosure (verbal or written) is in violation of New York State law and may result in a fine, jail sentence or both. It is important to note that general authorization for release of medical or other child-specific information is not sufficient authorization for the release of confidential HIV information.

Revised 4/30/10; 8/31/15, 10/29/19