Communities Connected *for* Kids

Series	Compliance	
Policy Name	**Front Desk & Confidential Environment**	
Policy Number	**1510**	
Origination Date	2/18/2020	**Revised:**
Regulation	**Chapter 119, F.S.**	

Background/Purpose

It is the intent of Communities Connected for Kids to maintain a safe and secure environment that protects all employees and visitors while ensuring transparency and public access to public records. All reasonable steps are taken to avoid situations in which safety and security may be compromised. It is also the intent of Communities Connected for Kids to utilize universal precautions that support a confidential environment that adheres to HIPAA Laws and maintains the privacy and security of confidential client information.

A. Front Door Entry

1. The receptionist will evaluate the business purpose of a visitor prior to providing admittance to the inner office lobby. Receptionist or staff providing front desk coverage will:
   - Greet visitor using the intercom system or from behind the protective glass.
   - Notify the person being visited and/or confirm the meeting is taking place via the agency meeting calendar.
   - Once confirmed, grant visitor entry into the office building. All visitors are to be accompanied by a staff member.
   - Have the visitor sign in and wait for their agency contact to meet them in the inner lobby. Receptionist may request ID, especially in situations where the visitor does not have an appointment.
   - For larger meetings, the receptionist or another staff member facilitating or participating in the meeting will escort the visitor to the specified meeting place if they are a first time visitor or otherwise unfamiliar with the office layout. Foster parents, relatives or children must be accompanied at all times.

2. To support effective communication, employees are asked to provide the receptionist with information regarding expected visitors before their arrival. In the event there is limited desk coverage, employees with anticipated visitors are expected to request their visitor to notify them upon arrival, and meet them to escort them to the meeting space.

3. All employees using a badge to enter secure areas are expected to ensure that the door closes behind them, in order to not provide inadvertent access to any unknown visitor. If there is an unknown visitor requesting access, the employee should request that they remain in the outer lobby until they can be greeted, and receptionist or designee can implement the protocol outlined above. All secured areas should be kept locked at all times.

Communities Connected *for* Kids

B. Escalation of Emergent threats

1. Any employee who encounters a situation in which they believe safety or security may be compromised should immediately notify, directly or with the assistance of another employee, a member of the senior management team, or if circumstances dictate, law enforcement.

2. An employee who observes a colleague encountering a potential emergent situation must either contact someone in senior management or intervene if the situation is safe to do so.

3. All efforts will be made to safely communicate to other employees, visitors and to the office that an emergent threat may be occurring.

4. Upon notification of an emergent threat, employees are expected to remain away from the area, alert other employees that may be returning to the area, and await further direction

5. In the event a situation arises to a serious threat, not only should 911 be called but all employees will be advised to either lock themselves in their office or to exit the building immediately. As much information will be given to employees via email or whatever means possible.

6. The highest ranking manager on the premises will assume incident command until such time as the issue is resolved, or until they are relieved by a superior or by law enforcement.

C. Confidentiality and public records

1. Both inside the office environment and externally, employees are expected to practice universal precautions in verbal and written communications. Universal precautions assume that open areas of the office are not secure, and therefore require discretion in the discussion of or written presence of confidential information (items left on copiers, etc.). Employees are encouraged to use secure print and HIPPA and PHI guidelines are to be used at all times.

2. As a component of our obligation to protect confidential information, video- and/or audiotaping devices are prohibited from use in CCKids' offices and service centers, unless authorized by the CEO, or Director of Community Relations.

3. As an agency funded by the Department of Children and Families, we operate in compliance with Florida statutes governing access to public records. FS 119.07 permits access to any public record to be inspected and copied by any person desiring to do so, at any reasonable time, under reasonable conditions and under supervision of the custodian of the public records.

4. Should a member of the public make a public records request, the CCKid's employee who receives the request, whether verbal or written, must ensure the request is facilitated promptly by immediately engaging a member of the Quality Management team, or a senior manager. CCKid's Policy 901 (Contents & Organization of Electronic Client Records) and the 1300 Policy Series provides further guidance on public records and records release.

D. Community Partners utilization of office space

1. Community partners requesting to use our offices will be given a copy of this policy, and are required to adhere to all guidelines within this policy and all related policies and procedures of the building.
2. Community partners will give the receptionist a list of all potential visitors when they are in the office.
3. Utilization of office space by community partners is available during regular business hours (Monday-Friday 8am to 5pm). After hours use must be pre-approved by the CEO or COO.
4. Community partners should also provide insurance coverage if available.

Approved: Carol Deloach

Carol Deloach, CEO