Series: 1100 Information Technology

Policy Name: **Internet Safety and Safeguards**

Policy Number: 1101

Regulations: 45 C.F.R 164.530 (c); Communities Connected for Kids Information Technology 1102, 1105, 1106, 1107

Origination Date: 6/22/2015 **Revision Date:** June 14, 2022

Policy: It is the policy of Communities Connected for Kids to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via the Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act (CIPA) [Pub L. No. 106-554 and 47 USC 254(h)].

Administrative, technical and physical safeguards have been put in place to protect all Personal Health Information (PHI) from intentional, unintentional use or disclosure Information contained within CCKIDS' systems is proprietary, and confidential access is restricted to those persons whose jobs require them to input or review the information to carry out their job responsibilities. Any review of PHI contained in Communities Connected for Kids IT systems shall occur only on a NEED-TO-KNOW basis in order to either 1) provide direct clinical care to the consumer/client involved or 2) access authorized record reviews. Any and all unauthorized access of this information will subject the person to employer sanctions up to and including dismissal and/or other resulting legal actions. Safeguards have been put in place to reasonably safeguard protected health information to limit incidental use or disclosures made pursuant to an otherwise permitted or required use or disclosure.

Certain terms in this policy should be understood expansively to include related concepts. The words 'company' and 'Communities Connected for Kids' include all of our subcontractors. The word 'document' covers all files that can be read on a computer screen as if it were a printed page, including the HTML pages read by an Internet browser, any file meant to be accessed by a word processing or desktop publishing program, or its viewer, and files prepared for any electronic publishing tool. The word 'graphics' includes all types of photographs, pictures, animations, movies, or drawings.

Procedure:

Communities Connected for Kids reserves the right to record the address of each World Wide Web site visit, each chat, newsgroup, or e-mail message, and each file transfer into and out of its internal networks. No employee should have any expectation of privacy as to his or her Internet usage.

The display of any kind of sexually explicit image or document on any company system is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using Communities Connected for Kids' network or computing resources.

To the extent practical, technology protection measures (or “Internet Filters”) shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by CIPA, blocking shall be applied to visual depictions of material deemed obscene or child pornographic, or to any material deemed harmful to minors.

One of the CIPA allowances is that the technology protection measure may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Specifically, as required by CIPA, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called ‘hacking’, and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

CCKIDS’ Internet facilities and computing resources must not be used knowingly to violate laws and regulations of the United States or any other nation, or the laws and regulations of any state, city or other local jurisdiction. Use of any company resources for illegal activity is grounds for immediate employee dismissal, and Communities Connected for Kids will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries and archives on individuals’ Internet activities.

Employees and clients with Internet access may only download software with direct business use, and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license. Employees and clients with Internet access may not use company Internet facilities to download entertainment software or games, or to play games against opponents over the Internet. The use of non-business related streaming audio and video is prohibited (music, stock tickers, news streams).

No employee or client may use the company’s Internet facilities to deliberately propagate any virus, worm, Trojan horse, trap-door program code or any form of destructive programming.

No employee or client may use the company’s Internet facilities, knowing that such use may disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

Only those employees or officials who are duly authorized to speak to the media, to analysts, or in public gatherings on behalf of Communities Connected for Kids may communicate, in the name of the company, to any news group or chat room. Other employees may participate in news groups, or chats in the course of business when relevant to their duties, but they do so as individuals in their professional capacities, and shall identify themselves honestly, accurately and completely (including one’s company affiliation and function, where requested). Employees must refrain from any unauthorized political advocacy in the name of Communities Connected for Kids and must refrain from the unauthorized endorsement or appearance of endorsement by the company of any service not provided by this company, its subsidiaries or its affiliates.

The company retains the copyright rights to any material posted to or through any forum, news group, chat room, e-mail message or World Wide Web page created by any employee in the course of his or her duties.

Employees are reminded that chats and news groups are public forums where it is a violation of agency policy and may be a violation of law to reveal confidential company information, client data, trade secrets, and any other material covered by existing company confidentiality policies and procedures.

The company will limit Internet access to those employees who demonstrate a legitimate business need and are authorized by appropriate levels of management.

Clients' computers and computer networks must be completely separate from the employee network. This can be accomplished either by separate physical cabling to the router, or virtual VLAN setup on managed switches to the router. Clients may not use computers which have access to the employee network.

Clients will be supervised and monitored during the usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act.

Any employee who obtains a password or ID for an Internet resource must keep that password confidential. Company policy prohibits the sharing of users IDs or passwords obtained for access to Internet sites as well as all internal Communities Connected for Kids systems.

Employees should schedule communications-intensive business-related operations such as large file transfers, downloads, mass e-mailings and the like for off-peak times.

All files are ***automatically*** scanned by an active Antivirus program prior to being opened.

Employees shall not attempt to disable, defeat, or circumvent any company security facility.

Computers that use locally attached modems bypass CCKIDS' network security systems. Therefore, these modems must be removed. When business needs dictate, computers used with dial-up or leased-line connections to any outside computer or network must be physically isolated from CCKIDS' internal network. Refer to the 'Analog Line Security Policy' for detailed information.

Only those Internet services and functions having legitimate business purposes will be enabled in the Internet firewall.

FTP transactions are blocked by the corporate firewall, and exceptions must be configured within the routers.

Users with a specific business reason to use FTP must forward a written request for such access to the IT department management.

Approved: DocuSigned by: Carol Deloach 96C0E7A7E02E4BA... Date: 7/27/2022

Carol Deloach, CEO