Communities Connected *for* Kids

Series:	1100 Information Technology		
Policy Name:	1117		
Policy Number:	Device and Media Control		
Regulations:	CCKids 1108		
Origination Date:	7/8/2022	**Revision Date:**	

Policy: PHI and other sensitive data should not be physically removed or transported from a Communities Connected for Kids (CCKids) service location, whether in paper or electronic format, unless such information will be used for the performance of job duties including response to an action approved by the Supervisor.

Procedure: All PHI, PII and other sensitive data that is extracted from CCKids systems must be stored on an approved, encrypted, password protected storage device. Use of unencrypted devices for this purpose is prohibited.

1. All original files and documents must be stored on the CCKids network. Approved methods for creating and accessing CCKids files and documents are dependent on the type of device on which the work is being done.

2. Extracted data may be kept as long as its use is needed. After extracted data is no longer needed, appropriate steps must be taken to remove data from the portable device or removable media prior to re-use or final disposal. Storage devices which are the property of CCKids must be returned when employment or business relationship ceases.

DocuSigned by:

Approved: Carol Deloach ____________________ Date: 7/27/2022 ____________________

96C0E7A7E02E4BA...

Carol Deloach, CEO