Data Protection and Acceptable Use of Electronic Devices

1. Introduction

The purpose of the Community Partnership for Child Development (CPCD) Data Protection and Acceptable Use Policy ("Policy") is to describe the acceptable use and accessing of Information Systems (defined below). This Policy applies to all CPCD employees and temporary staff ("Personnel") as well as contractors, external consultants, advisors, and other additional third parties performing services for or on behalf of CPCD ("Service Providers", and collectively with Personnel, "Users").

For purposes of this Policy, the term "Information Systems" broadly includes desktops, laptops, servers, external storage drives, mobile communications devices (such as tablets, smart phones, etc.), networks and application software (such as operating system software, e-mail, web browsers, etc.), databases and data that are owned, leased, or managed by or for CPCD.

2. General Acceptable Use of Information Systems

CPCD permits the use and accessing of Information Systems to assist Users in conducting business for, or on behalf of, CPCD. The use and accessing of Information Systems is a privilege, not a right, and CPCD reserves the right to terminate any Users' access and use of Information Systems at any time. Users may access and use only those Information Systems that the User has been authorized to access and use by the User's manager in the case of Personnel, or CPCD supervisor in the case of Service Providers. All data created using such Information Systems, or stored on such Information Systems, are the property of CPCD, not its Users. As more fully described in Section 13 of this Policy, Users should not have an expectation of privacy in the materials that are created, stored, sent, or received by them while using CPCD Information Systems.

Users are responsible for knowing and complying with this Policy and all other CPCD policies or procedures regarding use of Information Systems that have been provided to the User. Moreover, all Users have a responsibility to use and access Information Systems in a manner that increases productivity and protects the confidentiality and security of CPCD trade secrets, intellectual property, and other assets owned or licensed by CPCD and in accordance with Head Start Performance Standards (2016), applicable laws, and CPCD policies.

All Users must report suspicious or unauthorized activities or Prohibited Activities (defined below) to their department director or Human Resources Department (HR) in the case of Personnel, or to their CPCD supervisor in the case of Service Providers.

3. General Prohibited Activities

Prohibited activities when using or accessing the Information Systems include, but are not limited to, the following (collectively, “Prohibited Activities”):

a. Engaging in illegal or fraudulent activities including, but not limited to, gambling, trafficking in drugs or weapons, creating or forwarding "chain letters" or other "pyramid" schemes of any type, sending Internet postings other than statements protected by applicable law from a CPCD e-mail address other than in the course of business duties

and approved by each department and the Information Technology (IT) Department, or participating in terrorist acts;

b. Engaging in activities or transmitting e-mail, texting, or instant messaging content that are harassing, threatening, intimidating, vulgar, obscene, pornographic, or constitute discrimination, harassment, or hostility on account of age, race, religion, sex, ethnicity, national origin, disability or any other protected class, status or characteristic, as provided in CPCD Human Resources policies, CPCD Internet Safety Policy IT-104 or under applicable law;

c. Cell phones, whether personal or agency provided, will not be used while driving during CPCD work hours or when conducting business on behalf of CPCD. Users must pull over and stop vehicles in a safe location should there be a need to talk or text on cell phones. (See CPCD Policy IT-109)

d. Transmitting via instant messaging CPCD Personally Identifiable Information (PII), as defined in the CPCD GMS-7 Recordkeeping and Retention Policy, with any party including, but not limited to, personnel, suppliers, dealers, distributors, contractors, or customers;

e. Using non-CPCD sanctioned cloud storage services (*e.g.,* Box, GoogleDocs, Dropbox, etc.) to store or share CPCD Restricted Information with any party; in the case where CPCD restricted information is stored on cloud storage services, the data must be handled as defined in the CPCD IT Data Security IT-108;

f. Transmitting, downloading, or storing any information, data, or material that could infringe on any copyright, trade secret, or other intellectual property right of CPCD or a third party, including but not limited to, engaging in any activity that is prohibited under Section 4 (Intellectual Property and Software Usage) of this Policy;

g. Downloading or installing unauthorized software products, video files, or music as described in Section 4 (Intellectual Property and Software Usage) of this Policy;

h. Expanding or bypassing CPCD office(s) networks or assigned network port connections by installing switches, routers, wireless devices, or accessing internal devices outside authorized VPN solutions;

i. Misrepresenting or obscuring one's own identity (or another person's identity) or using the identity of another in any electronic communications (*e.g.,* e-mail, instant messaging, virtual meetings, online chat rooms, etc.);

j. Using any CPCD domain names (*e.g.,*cpcdheadstart.org or any derivation) or e-mail addresses to create any personal or private accounts for social media or messaging services unless otherwise approved by the Community Relations Department or the IT Department where applicable;

k. Exceeding authorized access to CPCD information and data, including without limitation unauthorized access to private files or accounts of CPCD Personnel or third parties;

l. Intentionally disabling or circumventing the operation or the configuration and security of installed CPCD Information Systems, including but not limited to antivirus and asset management software, or preventing their automated updates or scans;

m. Using hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, and decrypt encrypted files or compromise information security by any other means;

n. Downloading, installing, or attempting to introduce viruses and any computer code designed to damage, self-replicate, or otherwise hinder the operability, security, performance of, or access to any Information Systems. Users should immediately contact the IT department or CPCD director upon discovery of a virus on their device, or when inadvertently introducing a virus into any Information Systems;

o. Intentionally damaging or destroying Information Systems or assets owned by CPCD;

p. Intentionally damaging or destroying data proprietary to CPCD including source code, content, customer data, strategic plans, etc.; and

q. With regard to software, unless otherwise permitted by authorized administrators, Users may not:

- install software on CPCD Information Systems unless such software has been approved (or pre-approved) by the CPCD IT Department or other authorized personnel as more fully described in Section 5 of this Policy;
- use CPCD Information Systems to download, transmit, or store copies of software unless such software has been approved (or pre-approved) for download, transmittal, or storage by the CPCD IT Department or other authorized personnel;
- make copies (other than archive copies) of any software licensed by CPCD; or
- distribute, transfer, or loan any software licensed by CPCD to any third party.

4. Intellectual Property

Users must comply with all licenses (including, but not limited to, software licenses), copyrights, and applicable laws and regulations governing intellectual property used for, or on behalf of, CPCD. Users shall not engage in any conduct that infringes upon or violates any such intellectual property rights or licenses. Unauthorized copying of copyrighted material including, but not limited to, digitizing and distributing photographs from magazines, books or other copyrighted sources, copyrighted music, and installing any copyrighted software for which CPCD or the end user does not have an active license is strictly prohibited.

Users should be mindful that all software may be subject to third-party intellectual property rights under applicable law and specific license restrictions, including, without limitation, any software that may be available for "free." License restrictions for software may vary greatly depending on the particular software license. Users who have questions regarding a particular software license, including any rights or restrictions in connection with such license, should contact the CPCD IT department for assistance.

5. Software License and Usage

All CPCD Information Systems given to Users shall be prepared and configured by the IT department or authorized third-party suppliers. This is required to ensure all pre-installed software is properly licensed and can be supported. Users may request additional software to be installed on their devices (*e.g.,* software that is not included in the standard image or if the User requires a different version of the installed software) if software is properly licensed for use by the User, approved by the relevant director or CPCD supervisor and software is not prohibited by the CPCD IT Department.

Users may install updates to software only if such software has been pre-installed (*e.g.,* Java, Adobe Flash, Adobe Reader, etc.) or pre-approved by the IT Department and the application prompts the User to install an update to such software.

Exceptions can be requested in the case of research and development or authorized proof of concepts. Exceptions must be approved by the CPCD IT Department.

6. Confidentiality

Passwords

Users are granted access to a wide variety of information and data (depending on their role/function in the organization), including CPCD internal data, child/family data, personally identifiable information (PII), donor data, and partner and/or third-party data. Password policies are in place to ensure confidentiality of data is maintained at all times. Passwords are to remain confidential and should be changed at least annually. In the event a User feels their password was compromised, contact the IT Department to change immediately.

Children/Family Data

Users must handle and protect all children/family information and data in accordance with the CPCD Confidentiality Policy H-07, CPCD Data Protection Policy IT-107, and Head Start Performance Standards (2016) 1303 Subpart C—Protections for the Privacy of Child Records. Users may not use or disclose personally identifiable information (PII) in a manner that is prohibited by CPCD. (See H-07, IT-107, HR 304)

Donor Information

CPCD takes every precaution to protect the safety and security of donor transactions both online and off-line. CPCD makes use of the HTTPS security protocol, SSL, to communicate with most browser software. This method is the industry standard security protocol, which helps keep personally identifiable information (PII) as secure as possible. (Ex. DonorPro, Adopt A Family, etc.)

CPCD uses SSL encryption to protect sensitive information online, also precaution is taken to protect donor information off-line. Only CPCD authorized employees are granted access to PII through secure networks by way of username and password. All servers that store personally identifiable information will be maintained in a secure hosted environment. (See IT-107)

7. Physical Security

Users must protect CPCD Information Systems and portable data storage devices (*e.g.,* CDs, flash drives, or memory sticks), and security devices (*e.g.,* tokens and smart cards) used to perform work for and/or on behalf of CPCD from unauthorized access and theft at all times (including, but not limited to, while in the office, in the car, or in a hotel). Laptops, mobile communication devices, portable data storage devices, and security devices should be carried onto airplanes as hand luggage if possible. All Users are responsible for exercising good judgment and common sense. For example:

- Users should never leave laptops, mobile communications devices, or portable data storage devices unless such devices are in a physically secure location; and
- Users should review travel restrictions or limitations that may apply to them and/or their devices while travelling outside the United States.

8. Clean Desk and Clear Screen

To prevent unauthorized use of or access to Information Systems, all Users must secure their devices used to perform work for and/or on behalf of CPCD with a password-protected screen-saver with the automatic activation feature enabled, or by logging off when the system will be unattended. To prevent unauthorized individuals from using the privileges associated with a User's login ID, each User must be sure to log off from multi-user computers when they leave their desks for more than a few minutes. In addition, all Users must log off of their sessions and computers when leaving their workstations at the end of the workday or for an extended period of time. Failure to log off may increase the likelihood that unauthorized users may be able to take over an authorized User's open sessions to gain access to Information Systems.

At the end of a business day, or when away from the desk for any extended period of time, all confidential or restricted information and media containing such information, to include PII, must be properly stored and secured to prevent unauthorized access or acquisition.

9. E-mail Use

Users must use extreme caution when opening e-mail attachments received from unknown senders to prevent malicious programs (like malware, ransomware, viruses, worms, Trojan horses, e-mail bombs) from accessing CPCD Information Systems. Users will exercise caution with e-mails from trusted sources that appear out of character for the sender. If an e-mail message received seems suspicious, Users should contact the IT Department to ask about the validity of the e-mail before opening any attachment. Immediately delete any untrustworthy e-mail.

10. Incidental Personal Use

Users may make occasional, incidental, and limited personal use of devices owned, leased, or otherwise managed by CPCD to access the Internet (including e-mail), but only if such use does not distract from work duties, does not detrimentally impact network resources, and is otherwise in compliance with all applicable CPCD policies; provided, however, that by engaging in such incidental personal use, User expressly agrees that:

a. User will comply with this Policy and not engage in any Prohibited Activities;
b. User agrees that CPCD may access, review, monitor and use any information or data User directly or indirectly views, creates, uploads, downloads and/or stores on any CPCD

Information Systems (in accordance with and to the fullest extent permitted by applicable law), including any data or information viewed, created, uploaded, downloaded, and/or stored on computer hard drives, RAM, or temporary memory caches created by software applications; and

c. User assigns and/or waives all rights, title, and interest in and to any and all information or data (to the fullest extent permitted by applicable law) to or for the benefit of CPCD that User directly or indirectly stores on or downloads from the Information Systems. This includes any information or data that resides in temporary or permanent memory on Information Systems after the User's engagement or employment with CPCD has terminated.

d. User understands that CPCD information systems have priority for all network resources and that personal devices will be disconnected to free up resources if necessary.

CPCD does not grant any warranties of any kind, whether express or implied, regarding the Information Systems. If Users use Information Systems for personal use, Users do so at their own risk. CPCD will not be responsible for any damage that Users suffer in connection with use of or access to Information Systems, whether caused by CPCD's own negligence, Users' errors or omissions, or the fault of third parties.

11. Use of Personal Equipment

Users may use personal devices such as laptops, tablets, smartphones, etc. to conduct CPCD business or access CPCD Information Systems only under the following conditions:

a. Devices meet or exceed CPCD security configuration, as defined in CPCD IT-102 for such device type, including such items as antivirus, updated patches, and encryption on such devices;

b. There is no expectation of technical support by the CPCD IT Department or authorized third-party suppliers. Requests to support personal devices are not permitted.

c. CPCD may install a device management agent(s) on the Users' personal device and, if required, force a password on the device, encrypt data, or wipe the device if reported stolen\lost;

d. When storing CPCD information, Users must separate into different folders personal data unrelated to work performed for or on behalf of CPCD, from data that is owned or otherwise created in performing work for or on behalf of CPCD such that CPCD information can be easily deleted from the personal device after the employee leaves the organization and is no longer authorized to have access to that data;

e. CPCD does not provide software to be installed on Users' personal devices that is in violation of CPCD software license terms and conditions. CPCD will not be liable for or pay for the software license(s) used on Users' personal devices; Users are responsible, at their own expense, for software licenses that are installed on their personal devices.

By using personal devices to conduct CPCD business or access Information Systems, Users expressly acknowledge, agree, and authorize that such equipment, and all data that resides on such equipment, can be inspected by CPCD notwithstanding any claims of personal privacy, and Users further agree to make such equipment and data accessible to CPCD as requested. By

using personal devices to conduct CPCD business or access Information Systems, Users also agree that CPCD may image the memory on such device in connection with suspected unauthorized use, when required to comply with applicable legal processes or as otherwise permitted by law. Users are solely responsible for complying with the terms and conditions of any software installed on personal equipment that is not licensed by CPCD but used for business purposes. Users agree to indemnify and hold CPCD harmless for the use of any such software installed on personal equipment. Users are additionally solely responsible for complying with all applicable laws and CPCD policies in their use of personal devices, and Users understand and agree that their permission to use personal devices to conduct CPCD business or to access Information Systems can be revoked by CPCD at any time. Further, by using personal devices to conduct CPCD business or access Information Systems, Users expressly authorize CPCD to remove any CPCD information from their personal device and agree to delete, and not to copy, any such information upon instruction from CPCD.

12. Software Export

Exporting software, technical information, encryption software, or technology to certain jurisdictions may violate applicable laws, including export control laws. CPCD management and the IT Department must be consulted prior to exportation of any such material.

13. Privacy

Users should not have an expectation of privacy in the use of or access to CPCD Information Systems or the materials that are created, stored, sent, or received by them using CPCD Information Systems.

Authorized personnel and/or automated monitoring and data collection tools installed and operated by authorized personnel on Information Systems may, without prior notice and to the extent permitted by applicable law, (i) copy, retain, and examine all material stored on any and all Information Systems, or (ii) monitor any aspect of a User's use and accessing of Information Systems including, but not limited to, monitoring websites visited by Users, monitoring chat groups and news groups, reviewing material downloaded or uploaded from the Internet by Users, and reviewing e-mail and instant messages sent and received by Users through the Information Systems.

CPCD may use automated monitoring software to monitor material created, stored, sent or received on the CPCD Information Systems to limit the creation, download, installation, transmittal, or storage of inappropriate material through CPCD Information Systems. CPCD's use of these automated tools, however, does not diminish the Users' responsibility to ensure that he or she does not create, store, or transmit inappropriate material as defined in the CPCD IT Security Policy.

14. Sanctions

Noncompliance or violations (including careless, accidental, intentional, or willful violations) of this Policy will be grounds for disciplinary actions up to and including possible termination of employment or engagement. The disciplinary measures to be taken, including legal action, will be evaluated on a case-by-case basis depending on the particular facts and circumstances of the violation, consistent with applicable law.