1. POLICY STATEMENT

The risk of unauthorized disclosure of Highly Sensitive Data is elevated when that data is stored on Individual-Use Electronic Devices and Individual-Use Electronic Media, or on Cloud Services outside of the control of The Community Solution Education System ("The System" or "System"). Therefore, the System limits the circumstances under which Highly Sensitive Data may be stored in these locations. It further mandates that all of the requirements that follow be met when Highly Sensitive Data must be stored on individual-use electronic devices or electronic media.

It is the responsibility of individuals to determine if they maintain or have access to Highly Sensitive Data on their device(s) and media and, if so, to ensure compliance with this Highly Sensitive Data Policy ("Policy"). Failure to comply with requirements of this Policy will result in disciplinary action up to and including termination.

2. PURPOSE

As a component of the System IT Security Program, the purpose of this Policy is to limit the risk of unauthorized access to Highly Sensitive Data. While other types of sensitive data exist and must be handled appropriately, the negative impact of unauthorized exposure of data specifically covered by this Policy is especially acute.

3. APPLICABILITY

This Policy applies to all System and Member College employees, contractors, temporary workers, student workers, and agents who are involved in any way with the System IT environment.

4. DEFINITIONS

4.1 Member College

Member College means any educational institution that is part of an affiliated education system or group of educational institutions with the System, including but not limited to The Chicago School, Pacific Oaks Education Corporation, the Santa Barbara and Ventura Colleges of Law, Saybrook University, University of Western States, and the Kansas Health Science Center.

4.2 Cloud Service

Any system, infrastructure, platform, or software hosted by a third-party provider through the internet and providing on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the System.

4.3 Highly Sensitive Data

For purposes of this Policy, Highly Sensitive Data means Personal Information that may cause serious and potentially irreparable harm if disclosed or used in an unauthorized manner.

4.4 Personal Information

An individual's name, or any other direct or indirect identifier of an individual, in combination with any one or more of the following data elements about the individual:

- Social security number
- Driver's license number or state identification card number
- Passport or Foreign Visa number
- Financial account number, or credit card or debit card number
- FERPA education record information
- Protected health information

4.5 Individual-Use Electronic Devices

Computer equipment, whether owned by the System, a Member College, or an individual, that has a storage device or persistent memory, such as desktop computers, laptops, tablets, smart phones, and other mobile devices, such as servers (including shared drives), printers, routers, switches, firewall hardware, clinical workstations, medical devices, etc.

4.6 Individual-Use Electronic Media

All media, whether owned by the System, a Member College, or an individual, on which electronic data can be stored, including but not limited to external hard drives, magnetic tapes, diskettes, optical media, and USB storage devices (e.g. thumb drives).

4.7 IT Environment

The IT environment encompasses all System IT systems, resources, and facilities and all electronically stored, processed, transmitted, printed, or faxed information.

5. PROCEDURES

5.1. Storing Highly Sensitive Data on Individual-Use Electronic Devices and Individual-Use Electronic Media

- Highly Sensitive Data must be securely encrypted on the Individual-Use Electronic Device or Individual-Use Electronic Media, according to encryption methods recommended by the System IT department.
- Where possible, a log-in password must be enabled for any Individual-Use Electronic Devices or Individual-Use Electronic Media containing Highly Sensitive Data. The password must meet or exceed appropriate complexity levels consistent with ongoing IT directives or instructions. The password must not be shared with anyone and follow the requirements stated in the User Password Policy.
- No device may be left unattended if it is not locked.
- Any Highly Sensitive Data stored on an Individual-Use Electronic Device or Individual-Use Electronic Media must be deleted from the device or media as soon as storage of the Highly Sensitive Data on that device or media is no longer necessary.
- Management of the Individual-Use Electronic Device or Individual-Use Electronic Media may not be outsourced to any party external to the System.

5.2. Cloud Services

The System may use Cloud Services for some computing and data storage activities based on business needs. Cloud Services store data and provide services in internet-accessible data centers that may be located almost anywhere. Cloud Services vary significantly in their service levels and security measures. While Cloud Services may offer an attractive cost model, they also present significant risks. Using them may also affect TCS's ability to comply with some laws. Before using any Cloud Services to collect, create, store, or otherwise manage Highly Sensitive Data, you must obtain approval from the System's Information Technology department.

5.3. Compliance with Policies

Users agree that their use of the System's IT resources is subject to this Policy and any additional policies, procedures, standards, and processes the System implements, including but not limited to, the Highly Sensitive Data Policy, Privacy and User Awareness and Training Policy, Data Incident Notification Policy, Mobile End-User Device Policy, and Social Media Policy

6. RELATED DOCUMENTS

- Computing Device Refresh Policy
- Computer and Email Usage Policy
- User Password Policy
- Mobile End-User Device Policy

7. CONTACTS

- Information Technology