1. POLICY STATEMENT

The Community Solution Education System ("The System" or "System") provides employees and others with hardware, networks, systems, and software to support its business requirements and functions. This Computer and Email Usage Policy ("Policy") limits how Users may use those resources and explains the steps Users must take to protect them.

2. PURPOSE

As a component of the System IT Security Program, the purpose of this Policy is to maintain the confidentiality, integrity, and availability of the System's information assets, and to ensure compliance with legal, contractual, and regulatory requirements.

3. APPLICABILITY

This Policy applies to all System and Member College employees, contractors, temporary workers, student workers, and agents who use IT resources or 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 User(s)

Any System or Member College employee, contractor, temporary worker, student worker, and agent who uses resources provided by System IT or accesses System or Member College networks, services, and systems.

4.3 Highly Sensitive Data

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

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

4.4 Digital Millennium Copyright Act (DMCA)

For the purposes of this Policy, the DMCA refers to U.S. federal legislation enacted to address the rights of copyright holders. It provides guidelines for copyright protection and enforcement, imposing liabilities for the unauthorized copying, distribution, and use of copyrighted digital materials. This Act requires people to comply with copyright laws, particularly in the context of Internet and digital media, to prevent the illegal duplication and distribution of copyrighted content.

5. PROCEDURES

5.1. General Use of IT Resources

The System provides network resources and systems for business purposes. Any incidental non-business use of the System's IT resources must be for personal purposes only. Users must not use the System's IT resources for commercial purposes, personal gain, or any purpose that may create a real or perceived conflict of interest with the System.

Users must not use the System's IT resources in a manner that negatively impacts their job performance or impairs others' abilities to do their jobs. The System's network and systems are subject to monitoring.

Users must not use the System's IT resources for activities that may be deemed illegal under applicable law including DMCA. If the System suspects illegal activities, it may report them to the appropriate authorities and aid in any investigation or prosecution of the individuals involved.

5.2. Prohibited Activities

The System prohibits using its resources to engage in activities such as (but not necessarily limited to) the following:

- hacking, spoofing, or launching denial of service attacks;
- gaining or attempting to gain unauthorized access to others' networks or systems;
- sending fraudulent email messages;

- distributing or attempting to distribute malicious software (malware);
- spying or attempting to install spyware or other unauthorized monitoring or surveillance tools;
- committing criminal acts such as terrorism, fraud, or identity theft;
- downloading, storing, or distributing child pornography or other obscene materials;
- downloading, storing, or distributing materials in violation of another's copyright;
- creating undue security risks or negatively impacting the performance of the System's network and systems;
- causing embarrassment, loss of reputation, or other harm to the System or a Member College;
- uploading, downloading, or disseminating defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene, or otherwise inappropriate or offensive messages or media;
- distributing joke, chain letter, commercial solicitations, or hoax emails or other messages (spamming);
- disrupting the workplace environment, creating a hostile workplace, or invading the privacy of others;
- using encryption or other technologies in an attempt to hide illegal, unethical, or otherwise inappropriate activities;
- bypassing, or trying to bypass, any copyright protection mechanisms, such as, but not limited to, Digital Rights Management (DRM) technologies;
- downloading, copying, changing, or distributing any digital media, such as, but not limited to, software, music, movies, and books, in a way that violates security protection rules;
- sharing, uploading, or hosting copyrighted material online without proper authorization; and
- uploading or downloading copyrighted material without a license or explicit permission from the copyright holder;

5.3. Internet Use

The internet offers a variety of services that Users depend on to work effectively. However, some technologies create undue risks to the System's assets. Some uses are not appropriate in the workplace. The System may block or limit access to particular services, websites, or other internet-based functions according to risks and business value. Inappropriate or offensive websites may still be reachable, but Users must not access them using System resources. Users must limit their web browsing and access to streaming media (such as videos, audio streams or recordings, and webcasts) to business purposes or as otherwise permitted by this Policy. Users' internet use must comply with this Policy.

All internet data that is composed, transmitted, or received via the System's IT Environment is considered to be part of the official records of TCS and, as such, may be subject to disclosure to law enforcement or other third parties.

Consequently, Users should always ensure that the information contained in email messages and other transmissions is accurate, appropriate, ethical, and lawful.

5.4. Sending E-Mail

Users must exercise utmost caution when sending any email from inside the System network to an outside network. Highly Sensitive Data should never be forwarded to an outside network by any means. System email must not be configured to auto-forward to an external email address.

5.5. Expectation of Privacy

To ensure compliance with this Policy, Users' use of IT resources, including but not limited to devices and internet or email usage, may be monitored. Therefore, Users should have no expectation of privacy when using the System's IT resources.

5.6. 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 Computing Policy, and Social Media Policy.

5.7. Duty to Report/Violations of Policy

Users should notify the VP of IT Services upon learning of any violations of this Policy. Users who violate this Policy will be subject to disciplinary action, up to and including termination of employment.

6. RELATED DOCUMENTS

- Highly Sensitive Data Policy
- Privacy and User Awareness and Training Policy
- Data Incident Notification Policy
- Mobile Computing Policy
- Social Media Policy

7. CONTACTS

- Information Technology
  - VP, IT Services
  - Director, Information Security

- Legal Affairs legalaffairs@tcsedsystem.edu

POLICY APPROVAL

Policy Sponsor (*Endorsement*): Steve Schneck
Steve Schneck (Jun 4, 2024 13:28 CDT) Date: Jun 4, 2024

Local Risk & Compliance Committee (*Validation*): Kylana N. Garrison-Reid
Kylana N. Garrison-Reid (Jun 5, 2024 11:30 CDT) Date: Jun 5, 2024

System Office Cross-Functional Operations Leaders Group (*Final Approval*):
Shari Mikos (Jun 6, 2024 20:22 CDT) Date: Jun 6, 2024

Computer and Email Usage Policy -FINAL for Signatures

Final Audit Report 2024-06-07

Created:	2024-06-04
By:	Lisa Catalano (LCatalano@tcsedsystem.edu)
Status:	Signed
Transaction ID:	CBJCHBCAABAANfuuc035SAQyayL8FtiTbmetqb8UtZN2

"Computer and Email Usage Policy -FINAL for Signatures" History

Document created by Lisa Catalano (LCatalano@tcsedsystem.edu)
2024-06-04 - 5:22:44 PM GMT- IP address: 99.39.160.181

Document emailed to sschneck@tcsedsystem.edu for signature
2024-06-04 - 5:24:22 PM GMT

Email viewed by sschneck@tcsedsystem.edu
2024-06-04 - 5:41:50 PM GMT- IP address: 98.227.27.53

Signer sschneck@tcsedsystem.edu entered name at signing as Steve Schneck
2024-06-04 - 6:28:31 PM GMT- IP address: 98.227.27.53

Document e-signed by Steve Schneck (sschneck@tcsedsystem.edu)
Signature Date: 2024-06-04 - 6:28:33 PM GMT - Time Source: server- IP address: 98.227.27.53

Document emailed to kgarrison@tcsedsystem.edu for signature
2024-06-04 - 6:28:34 PM GMT

Email viewed by kgarrison@tcsedsystem.edu
2024-06-05 - 4:30:09 PM GMT- IP address: 104.47.73.126

Signer kgarrison@tcsedsystem.edu entered name at signing as Kylana N. Garrison-Reid
2024-06-05 - 4:30:55 PM GMT- IP address: 108.241.79.252

Document e-signed by Kylana N. Garrison-Reid (kgarrison@tcsedsystem.edu)
Signature Date: 2024-06-05 - 4:30:57 PM GMT - Time Source: server- IP address: 108.241.79.252

Document emailed to Shari Mikos (smikos@tcsedsystem.edu) for signature
2024-06-05 - 4:30:58 PM GMT

Email viewed by Shari Mikos (smikos@tcsedsystem.edu)

2024-06-05 - 5:13:23 PM GMT- IP address: 104.47.73.126

Document e-signed by Shari Mikos (smikos@tcsedsystem.edu)

Signature Date: 2024-06-07 - 1:22:16 AM GMT - Time Source: server- IP address: 76.136.132.89

Agreement completed.

2024-06-07 - 1:22:16 AM GMT