TEXAS STATE TECHNICAL COLLEGE

STATEWIDE OPERATING STANDARD

No. GA 1.5.5	**Page 1 of 4**	**Effective Date: 09/01/2019**
DIVISION:	**General Administration**	
SUBJECT:	**Information Resources**	
AUTHORITY:	**Executive Order**	
PROPOSED BY:	**Ray Rushing**	
TITLE:	**Vice Chancellor & General Counsel**	**Date: 08/28/2019**
RECOMMENDED BY:	**Mike Reeser**	
TITLE:	**Chancellor**	**Date: 08/28/2019**
APPROVED BY:	**Mike Reeser**	
TITLE:	**Chancellor**	**Date: 08/28/2019**

STATUS: Effective 09/01/2019

HISTORICAL STATUS: New

I. STATEWIDE STANDARD

EXECUTIVE ORDER: By order of the Chancellor, Texas State Technical College (TSTC) and its employees shall not use unapproved information resources, public messaging applications or cellular messaging platforms on personally-owned devices to transmit TSTC Data, transact TSTC business or discuss TSTC business.

II. PERTINENT INFORMATION

In accordance with the *Texas Public Information Act* (the Act), TSTC must grant the public access to information regarding its records as detailed in the Texas Government Code, Chapter 552.

During the 86th Legislative session in 2019, the Act was amended by Senate Bill 944, effective September 1, 2019 to include the following language in Section 552.004 "Preservation of Information"

> *A current or former officer or employee of a governmental body who maintains public information on a privately-owned device shall:*
>
> *(1) forward or transfer the public information to the governmental*

body or a governmental body server to be preserved as provided by Subsection (a); or
(2) preserve the public information in its original form in a backup or archive and on the privately owned device for the time described under Subsection (a).

III. GENERAL GUIDELINES

TSTC business transactions and decisions shall only be conducted via TSTC-owned and/or TSTC-managed devices using applications that automatically keep records or can easily and routinely be recorded. Appropriate tools for conducting such business processes include, but are not limited to, Google's G Suite Products, Microsoft Office Products, Telephones and Fax Machines.

The list of allowable tools may change from time-to-time and the office of TSTC Information Technology Helpdesk shall maintain a list of allowable processes. Employees may contact OIT Helpdesk to receive the latest information.

Written TSTC business shall not be transacted on personally-owned electronic devices using a text messaging system. However, email to or from an official TSTC address may be conducted using a personally-owned device.

Transitory verbal conversations, as defined by the Act, may be conducted using either TSTC-owned or personally-owned devices.

IV. DEFINITIONS

G Suite: a brand of cloud computing, productivity and collaboration tools, software and products developed by Google. G Suite comprises Gmail, Hangouts, Calendar, and Google+ for communication; Drive for storage; Docs, Sheets, Slides, Forms, and Sites for collaboration.

Microsoft Office: is a family of client software, server software, and services developed by Microsoft. Microsoft Office Desktop applications include Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Outlook, Microsoft OneNote, Microsoft Publisher, Microsoft Access, Microsoft Project and Microsoft Visio.

Personal Devices: Any employee-owned electronic devices connecting to TSTC resources. This includes, but is not limited to, smartphones, laptops, tablets, and desktops.

Public Information: Information that is written, produced, collected, assembled, or maintained under a law or ordinance or in connection with the transaction of official business:

(1) By a governmental body;
(2) For a governmental body and the governmental body:
(A) Owns the information;
(B) Has a right of access to the information; or
(C) Spends or contributes public money for the purpose of writing, producing, collecting, assembling, or maintaining the information; or
(3) By an individual officer or employee of a governmental body in the officer's or employee's official capacity and the information pertains to official business of the governmental body.

TSTC Data: All data or information held on behalf of TSTC, created as a result and/or in support of TSTC business, or residing on TSTC information resources, including paper records.

V. DELEGATION OF AUTHORITY

The Chancellor has the authority to implement this SOS and delegates to the appropriate Vice Chancellor the responsibility to deploy resources, processes, and procedures to ensure compliance with this standard and all applicable federal, state, and/or local regulations.

VI. PERFORMANCE STANDARDS

TSTC employees adhere to the standards established in this Statewide Operating Standard (SOS).

Employees who violate this SOS may be subject to discipline up and including termination and may be liable for other penalties as outlined in the Public Information Act.

APPENDIX

VII. RELATED STATEWIDE STANDARDS. LEGAL CITATIONS, OR SUPPORTING DOCUMENTS

Texas Government Code, Chapter 552
Senate Bill 944
GA 1.5.1 Records Management
GA 1.5.3 Texas Public Information Act
GA 5.1 Information Technology
GA 5.1.4 Acceptable Use of Information Technology Resources

VIII. OPERATING REQUIREMENTS:

All users of information resources owned by TSTC or personal devices used to conduct business:

- Users shall only use TSTC-approved information resources and public messaging applications;
- Users shall not attempt to access any data or programs contained on TSTC information resources for which they do not have authorization;
- Users will not share their TSTC account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), employee ID cards, or similar information or devices used for identification and authorization purposes;
- Users will not make unauthorized copies of copyrighted software;
- Users will not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of TSTC Information Resources; deprive an authorized TSTC user access to a TSTC resource; obtain extra resources beyond those allocated; circumvent TSTC computer security measures;
- Users will not intentionally access, create, store or transmit material which TSTC may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the TSTC official processes for dealing with academic ethical issues); and
- Users will not otherwise engage in acts against the aims and purposes of TSTC as specified in its governing documents or in rules, regulations and procedures.