Acceptable Use of IT Policy

1. Purpose

This Policy covers acceptable use of the SISTC IT resources, the SISTC Student Management System (SMS), and the SISTC Learning Management System (LMS) by staff and students. This policy applies to all system users at any location, including those using privately owned computers or systems that connect to SISTC computer and network resources. This policy represents the minimum requirements that must be met by users. Whilst SISTC does not intend to inhibit access to the Internet, IT resources, social media channels, and/or systems, the use of such services to access or attempt to access information not intended for public display or use or to circumvent or violate the responsibilities of system users or system administrators as defined in this policy, is prohibited. IT resources, social media channels, SMS and LMS, and computer resources together with access to the Internet at SISTC are primarily for educational purposes. Information about the access to and acceptable use of the IT resources, SMS, and LMS will be incorporated into staff and student training, printed materials, and related online resources.

2. Scope

This Policy applies to SISTC Users who are staff, students, and visitors, and who use any SISTC IT resources, equipment, and systems.

3. Principles of Acceptable Use

All SISTC Users have a general duty of care and are responsible for being aware of, and complying with:

- Ensuring their usage complies with this Policy, and for informing the School when they cease their association with the School;
- Reporting any suspected security problems or unacceptable use to IT Support, and not demonstrating the problem to others;
- Any user who believes their files have been tampered with should immediately change their password and contact IT Support with the specific details;
- Respecting the physical hardware and network configuration of SISTC owned network;
- Users must not extend the physical network on which their system resides;
- Not performing any unauthorised, deliberate action that damages or disrupts a computer system, alters its normal performance, or causes it to malfunction;
- Not using SISTC systems to gain unauthorised access to other computers, networks or information regardless of the intention;
- Not infringing copyright;
- Respecting the *SISTC Information Systems Management and Security: Policy and Protocol,* treating all confidential or sensitive information appropriately;

- Not using any of SISTC's official branding materials on their personal web pages, email, or other messaging facilities; and
- Users of electronic mail systems should be aware that electronic mail in its present form is not secure and is vulnerable to unauthorised access and modification.

3.1 USER ACCOUNTS

SISTC Users are ultimately accountable for all actions attributed to their User Account. To support this SISTC Users are responsible for safeguarding their passwords and/or other sensitive access control information related to their accounts or network access. As such, system users must recognise the sensitivity of all other passwords and computer or network access information in any form, and must not use, copy, transmit, share, or divulge such information. Any attempt to conduct such actions by a system user is a violation of this policy. Users shall ensure access privileges are restricted to their own use only. The following principles apply:

- Users must not share their accounts, nor grant accounts to others nor otherwise extend their own authorised computer and network access privileges to others;
- System users must not implant, execute, or use software that allows them unauthorised remote control of SISTC computer and network resources, or of SISTC accounts belonging to others;
- If specific access is required, the appropriate SISTC staff member should be contacted rather than disclosing a password;
- SISTC system users must not implant, execute, or use software that captures passwords or other information while the data are being entered at the keyboard or other data entry device;
- SISTC system users must not obtain nor attempt to obtain any electronic communication or information not intended for them;
- SISTC system users must not attempt to intercept or inspect information en-route through SISTC computer and network resources, nor use SISTC computer and network resources to attempt to intercept or inspect information en-route through networks elsewhere;
- Unattended workstations must always be logged off or left in the Workstation Locked mode when the operator leaves their workstation unattended;
- Users must be aware that removable storage like USB connected media, flash drives, CDs or DVDs are a security risk, and users are be responsible for them; and
- Where SISTC staff have confidential data stored on the removable storage, then the staff member may be required to encrypt the data. Sensitive information stored on portable devices (e.g. laptops, PDAs) should be encrypted.

3.2 USER PASSWORDS

All passwords must meet the following minimum standards:

- All SISTC accounts (e.g. computers and LMS) must have passwords;
- Passwords for accounts must not be shared, unless a team account has been specifically authorised in writing;

- SISTC Users are encouraged to regularly change the passwords for user accounts;
- Passwords must be resistant to a computer program that checks passwords against previously used passwords and passwords that are easily discovered or compromised by human or computational means;
- Passwords must use a mix of alpha and numeric characters and contain at least 6 characters if the operating system supports passwords of that length; and
- Passwords to computer and network resources containing computerised institutional data will not be issued over network media in clear text unless a secondary means of authentication is provided (e.g., smart cards).

3.3 USE OF SISTC IT PERMISSIONS AND SYSTEMS USE

3.3.1 Permissions

SISTC Users will only have access to the information and systems that they need to perform their function. Elevated local access permissions (e.g. administration for Student Management, Zoom, or the LMS) will only be granted for essential and specific purposes.

3.3.2 Systems Use

The following principles apply:

- SISTC Users may not copy any information or software stored on their desktop or laptop computer, for personal use;

Users may not use SISTC systems for any of the following activities:

- Gambling or any form of Internet gaming;
- Share trading unless you have the prior consent of the CEO;
- Copyright infringement;
- Use any SISTC systems for personal financial gain, solicitation, or private business purposes; and
- Posting any SISTC information to internet bulletin boards, discussion lists, news groups, chat groups or other internet discussion forums that are accessible by the public unless you are authorised by your line manager or lecturer to do so.

3.4 USE OF THE SISTC LMS

The LMS is part of the SISTC's intellectual property and an integral part of the SISTC learning experience. As such, staff and students must ensure that they use the LMS for educational purposes only; as per the level of permission granted; and as directed. It is an expectation that SISTC students will:

- engage with learning content on the LMS as directed by the teaching team;
- notify the lecturer of any problems with accessing and engaging with material;
- make a serious attempt to submit assessments as per the unit instructions;
- refrain from making inappropriate posts on discussion boards that deliberately attempt to subvert the discussion thread;
- refrain from redistributing assessments;

- not abuse, insult, threaten, participate in ongoing teasing, or criticise peers and/or teachers, either verbally or in written form;
- adhere to the School's guidelines on academic integrity and referencing;
- refrain from deleting or removing content or discussions without the express permission of the lecture, unless it is to edit and re-submit work; and
- not download and redistribute learning materials to peers or outside sources for your own private gain or that of another student or outside source.

4. Inappropriate Material

SISTC Users must not access, create, download, print, store, forward or send inappropriate content. Examples of which include, but are not limited to:

- Information or images containing indecent material (this includes pornographic or other sexually explicit material), or other material, which explicitly or implicitly refers to sexual conduct or preference;
- Information or images containing profane of abusive language. This includes anything that refers to or supports discrimination of any kind;
- Unwelcome propositions;
- Any defamatory, illegal, offensive, annoying or harassing material;
- Information intended to incite criminal activities or instructs others how to commit such acts; and
- If a user is in doubt as to whether the material they are accessing is inappropriate, it should be treated as such and remove it from your computer.

If you are the recipient of inappropriate material, or end up at an inappropriate website, it is important that you:

- Delete this material or close the web browser immediately; and
- You must also advise your line manager or lecturer that you have received or accessed such content.

5. Email, discussion board posts, social media, and online communication

Emails, social media posts, and discussion board posts must be written with the same consideration as any physical communication. SISTC Users, both staff and student, should ensure that all online communication is free from harassment and discrimination in any form. Students should be aware that sending or posting threatening, rude, or inappropriate content to and/or about staff and peers may results in misconduct.

When interacting on social media whether it is on an SISTC support channel or on a private site, staff and students must refrain from:

- Posting inappropriate material;

- Posting photos or comments that may cause harm to an individual or group of individuals (unflattering photos or comments); and
- Posting comments or photos that may be defamatory to the School, the staff, and or the students.

6. Legal Requirements

For legal purposes emails, discussion board posts, and other written communication has the same standing in court as paper documents. Users must be aware that SISTC can be involved in litigation. Any records relating to use and activities in relation to email, internet and intranet are discoverable by way of court order or subpoena. These include matters affecting legal proceedings, affecting personal affairs of employees, parents, students, or third parties, as well as relating to research, or other communications even if communicated in confidence. Emails and discussion board posts residing on or transmitted across the SISTC system is the property of SISTC.

7. Confidentiality and privacy of information

All staff users of the SISTC IT systems and LMS are required to comply with the *SISTC Information Systems Management and Security: Policy and Protocol,* the *SISTC Fraud, Corruption and Mismanagement Policy and the SISTC Privacy Policy.* All staff and student users are to comply with the *SISTC Academic Integrity and Misconduct Policy and Procedures.*

Relevant Legislation and Standards

Higher Education Standards Framework (Threshold Standards) 2021
Age Discrimination Act 2004
Copyright Act 1968 (Cth)
Disability Discrimination Act 1992
Racial Discrimination Act 1975
Sex Discrimination Act 1984.

Key Related Documents

SISTC Academic Integrity and Misconduct Policy
SISTC Anti-discrimination Policy
SISTC Information Systems Management and Security: Policy and Protocol
SISTC Fraud, Corruption and Mismanagement Policy
SISTC Learning Management System (Access and Support) Policy
SISTC Privacy Policy

Notes

Responsible Officer	Associate Dean, Learning and Teaching
Approval Authority /Authorities	Board of Directors
Date Approved	16 December 2020
Date of Commencement	16 December 2020
Date for Review	2022
Documents Superseded by this Policy	
Amendment History	**V1.0** approved on **16 Dec 20** **V1.1** updated with minor typographical errors made by the Responsible Officer, reference to the Copyright Act and changes in relation to the HESF 21 **1 July 2021**