SMU IT POLICIES & PROCEDURES

Title: **Acceptable Use Policy**	
Prepared by: IITS	Approved by: Chief Information Officer and Vice President, IITS

1. INTRODUCTION

Singapore Management University (SMU) provides information technology (IT) resources for the shared and responsible use by members of its community who are in turn, expected to use them in an efficient, ethical, professional, and legal manner consistent with the University's objectives and values. Inappropriate use exposes the University and community members to risk of data theft/loss and unintended disclosure. The University, therefore, has a responsibility to protect the University, its IT resources and its users from illegal or damaging actions, intentional or unintentional, on the part of individuals or computer systems.

Participation in a community of networked computers and users requires adherence to an ethical code of conduct. The fact that an activity is technologically possible does not legitimise its use. Users of the University IT resources have a responsibility not to abuse the resources and to respect the rights of the members of the community as well as the University itself.

2. PURPOSE

The purpose of this Acceptable Use Policy (the "Policy" or "AUP") is to articulate the acceptable use procedures for the appropriate use of the IT resources provided by SMU as well as for SMU's right to access information about and management of these resources.

In effecting this Policy, the University aims to meet the following goals:

a. To ensure the integrity, reliability, availability and superior performance of University IT resources.
b. To ensure that University IT resources are used for their intended purposes.

3. ENTITIES AFFECTED BY THIS POLICY

This AUP applies to all users of University IT resources including faculty, staff, students, alumni and guests. It also applies to technology resources administered

by individual departments as well as centrally, to personally owned computers and devices connected to the campus network by wire as well as through wireless, and to off-campus computers that connect remotely to the University.

4. DEFINITIONS

For the purposes of this document, the following definitions apply:

4.1. **Data:** is a collection of information that may include alphanumeric characters, words, sounds, symbols, images or videos, etc. stored in a form suitable for a computer.

4.2. **Equipment:** refers to information handling technologies and equipment including, but not limited to standalone or networked personal computers, digital mobile devices, printers, network devices and all forms of telecommunication equipment.

4.3. **Personal Computer**: refers to a general-purpose, cost-effective computer that is designed to be used by a single end-user. It can be a desktop, a laptop or any personal device and typically runs on Windows (Wintel), Mackintosh (Mac OS) or Linux, Mobile etc. operating systems.

4.4. **Personal Information:** refers to the information on an individual, including his/her name, IP address, University Log-in accounts, through which one can be identified.

4.5. **Personal Data**: shall mean; data whether true or not, about an individual who can (a) be identified from that data; or (b) from that data and other information to which the university has or is likely to have access.

4.6. **University IT resources:** refer to University Licensed Software and databases; data and equipment, support services and University connectivity to electronic information such as wired and wireless access to computer and telephone networks.

4.7. **University Licensed Software**: refers to the software or licences acquired by the University for its community for purposes of teaching and research. Such software could be acquired under a single user licence or campus-wide licence. In all circumstances, the provision is ONE University Licenced Software per user (meaning ONE copy for each student, faculty and staff) regardless of the number of personal computers or devices owned or acquired.

4.8. **Users:** refer to persons that have been authorised to use any IT resources from any location and/or given SMU accounts to accomplish tasks related to their respective relationships and statuses with the University. Current faculty, staff, students and other affiliates of SMU are considered as authorised users.

5. POLICY STATEMENT

General Provisions

5.1. This AUP sets forth the general parameters of acceptable use of University IT resources. Users should consult the respective governing policies, where available, for more detailed statements on permitted use and the extent of use the University considers appropriate. In the event of conflict between IT policies, the respective governing policies will prevail.

5.2. Users have the responsibility to utilise the University IT Resources properly for purposes consonant with the mission of the SMU.

5.3. Files that are used in the cause of official business are the property of SMU. The ability to alter another user's files does not in itself imply the permission to alter those files. Under no circumstances may a user alter a file that does not belong to him without prior permission of the file's owner or SMU.

5.4. Security is the responsibility of all members of the SMU community. Users must not store personal confidential information such as credit / debit card details or passwords on University IT Resources.

5.5. A user is not permitted to allow third parties access to University IT Resources without prior written consent from the Chief Information Officer (CIO) of Integrated Information Technology Services (IITS) or his designee. In addition, a user is not permitted to transfer or sell/resell resources/materials sourced from University IT Resources to third parties in return for a fee or any other forms of payment-in-kind.

5.6. **Deleting Electronic Communications.** Users of the University IT Resources, particularly SMU's email system should be aware that electronic communications are not necessarily erased from the computer system when the user "deletes" the file or message. Electronic communication may

continue to be stored on as a backup copy long after it is "deleted" by the user. As a result, deleted messages can be retrieved and recovered after they have been deleted within the retention period specified in the SMU email policy under Backup and Retention of Email Data.

5.7. **Inspection of electronic Information.** Information located on University IT Resources may be subject to examination, as deemed necessary, to maintain or improve functioning of technology resources, investigate alleged violations of University policies and/or Singapore law or to comply or verify compliance with the University policies and/or Singapore law.

5.8. **Disclosure.** In disciplinary proceedings, the University at its discretion may submit results of investigative actions to authorised University personnel and/or law enforcement agencies. Information and communications created with/communicated through University IT Resources may be subject to legally binding demands such as court orders. Ultimately it is the University that owns IT resources, not the users who use them.

5.9. **Right of University Access.** The University reserves the right for authorised personnel to access a users' stored information to investigate cases of computing abuse and for systems maintenance purposes. Such access shall be approved by the University's Chief Information Officer and Vice-President, IITS, and in consultation with the President and University counsel when necessary.

5.10. **Right to Identity Verification.** The University has a right to request users of University IT resources to produce a valid University identification or evidence of authorised use.

5.11. **Security and Privacy.** The University employs various measures to protect the security of its information technology resources and of user data and accounts. Users may have a reasonable expectation of unobstructed use of information technology resources, certain degrees of privacy, and protection from abuse and intrusion. Security precautions cannot always guarantee users security or privacy, however. Users should exercise caution in using University IT Resources to store and/or transmit confidential data.

5.12. **Disclaimer**. The University accepts no responsibility for any damage to or loss of data, hardware or software arising directly or indirectly from use of

the University's IT resources or for any consequential loss or damage. The University makes no warranty, express or implied regarding the facilities offered, or their fitness for any particular purpose.

Specific Prohibitions on Use

The following categories of use are inappropriate and prohibited:

5.13. **Use that attempts to damage the integrity of University or other IT Resources.**

5.13.1. University IT Resources may not be used for making unauthorised connection to, monitoring of, breaking into, or adversely affecting the system performance, whether these system(s) belongs to SMU or not. The ability to connect to other systems via the network does not imply the right to use or connect to them unless given proper authorization by the system owners.

5.13.2. Users must not steal or attempt to use methods of electronic or any means (e.g. software, hardware or firmware) to eavesdrop on passwords, contents and information that he/she is not authorized to access.

5.13.3. University IT Resources shall not be used to access, transmit, store, display or request for inappropriate content such as obscene, pornographic, erotic, profane, racist, sexist or defamatory or offensive materials.

5.14. **Use that impedes, interferes or otherwise causes harm to activities of others.**

5.14.1. Users should not engage in any actions that may interfere with a systems' supervisory or accounting functions, cause network congestion or interfere with the work of others. Examples of prohibited conduct include placing unlawful information on the system, the transmitting of data or programmes likely to result in the loss of recipient's work or system downtime, sending of "chain letters" or "broadcast" messages to lists or individuals, spamming or gaming via the SMU network.

5.14.2. Users must not:

a. develop and/or use programmes that may/will harass or harm other users of the system
b. develop and/or use programmes that may/will attempt to bypass system security mechanisms, steal passwords or data
c. develop and/or use programmes that, by design, attempt to consume all of an available system resource. Special arrangements can be made with IITS to accommodate such requests
d. develop or use programmes designed to replicate themselves or attach themselves to other programmes, commonly called worms or viruses and/or
e. develop and/or use programmes designed to evade software licensing or copying restrictions.

5.15. **Use in Violation of the Law.**

5.15.1. **Unauthorised Access or Use.** It is a violation to use another person's account, with or without that person's permission. Users should use only the computer accounts they are authorised to use.

5.15.2. Users should not attempt to crack, guess and/or capture another person's computer password.

5.15.3. **Disguised use.** Users must not conceal their identity when using the University IT resources, except when the option of anonymous access is explicitly authorised. Users are expressly prohibited from masquerading as or impersonating others or otherwise using a false identity.

5.15.4. **Use in Violation of Laws.** Users must not use their SMU account in any way that violates the laws of any country. The University expects its users to be cognisant with and abide by the provisions stipulated in the Computer Misuse Act (Chapter 50A) and Cybersecurity Act 2018 and the Sedition Act (Chapter 290).

5.15.5. **Copyright.** Users are responsible for ensuring that no copyrighted material (including music, film, podcasts, books, games and/or software) is downloaded using, published on, or distributed from SMU network without the copyright holder's permission. Users should be aware of the *Copyright Act (Chapter 63)* and the *Digital Copyright Policy* in force across the University. Users are also to note

that in some instances and depending on the type of contents, they may be subjected to the laws of a foreign jurisdiction.

5.15.6. **Personal Data Protection Laws**. Users are responsible for ensuring that the collection, use and disclosure of Personal Data are in compliance with Singapore's Personal Data Protection Act 2012 (PDPA). Generally, users should obtain valid consent before they collect, use or disclose Personal Data, unless any exception applies.

5.16. **Use in Violation of University Contracts.**

5.16.1. **Copyrighted Materials and Licensed Software, Programmes and Data.**

Users must:

- not transfer, duplicate, make available or obtain illegally, any copyrighted material including, but not limited to, agreements, license software, programmes and data
- respect the rights of others by complying with all SMU policies regarding intellectual property
- not install unlicensed or unauthorised software in the local (meaning desktop / laptop / computing devices) hard disk or server drives.

5.16.2. **University Licenced Software.** SMU provides ONE University Licensed Software license per user (meaning ONE for each student, faculty and staff) regardless of the number of PCs, desktops, laptops and/or computing devices purchased via SMU's PC Tender. Users must:

- uninstall all University Licenced Software from their PC when selling their PCs, termination of employment, leaves the university before graduation or upon graduation.

5.16.3. **Guidelines from Third-party or subscribed services**. When accessing other organizations' IT facilities and resources from the SMU network, users are responsible for abiding by these terms and conditions and the relevant policies of such other organizations.

5.17. **Use in Violation of University Policies.**

5.17.1. The privilege of using SMU equipment, including the network cabling, wireless access, computer and network systems and servers, broadcast media, and access to global communications and

information resources is provided by SMU and may not be transferred or extended by the campus community to people or groups outside the SMU, without authorisation.

5.17.2. **Account Removal**. Users must inform IITS to remove their SMU network configuration settings before they sell their PCs, termination of employment, leaves the university before graduation or upon graduation.

5.17.3. **Email and Web Policies**. Users must manage the use of emails and web pages in accordance with the policies outlined in the *SMU Email Policy* and the *Web Policy* Offenders will be held liable and sanctioned in accordance with the established University guidelines stipulated in the appropriate University policies. As a general guidance, the following conduct / actions are prohibited:

a. harassing, sending pornographic or defamatory materials / messages via email or through posting to Web pages
b. sending or posting forged email (masquerading), web pages and newsgroups messages
c. massive or unsolicited emailing without explicit approval from IITS
d. flooding a user or site with very large or numerous pieces of email
e. sending or forwarding of confidential SMU information via email.

Responsible and Acceptable Use

5.18. **Personal Account Responsibility**. Accounts are assigned to individuals and are not to be shared unless specifically authorised by the IITS. Users are solely responsible for all functions performed from the accounts assigned to them.

5.18.1. **Do not allow others to use your account.** Users should safe guard their computer accounts and passwords. Peer pressure and/or negligence cannot be accepted as defense.

5.18.2. Users are responsible to ensure the secrecy of their personal accounts and passwords by:

a. changing any pre-assigned default password at the first possible opportunity
b. avoiding composing passwords based on their personal information (e.g. name, user ID, date of birth, etc.).

5.19. **Responsibility for safeguarding University IT Resources.** Users should actively protect and defend University IT Resources against unauthorised access and use. Users:

5.19.1. should have the anti-virus software running on their PC and update the anti-virus signature file regularly

5.19.2. should regularly update the operating system (OS) updates or patches on their PC.

5.20. **Backup.** All data on the University computer systems is subject to backup at the sole discretion of the University. While the IITS will do its utmost efforts in ensuring the integrity of the backed up data, IITS cannot guarantee that all backed up data can be restored. Users, therefore have the responsibility to backup for their own critical files and systems.

5.21. **Use of University IT Resources by Faculty and Staff**. The University provides IT resources and services to employees of the University, for University business use. Prohibited use for employees includes, but is not limited to political campaigning, solicitation, unauthorised financial gain, or conducting business that has no official relationship with the University. Additional limits may be imposed by a supervisor, appropriate office, applicable University policies and/or Singapore laws.

5.22. **Use of University IT Resources by Students.** Student's use of the University's IT resource must be for academic advancement in teaching and research and must adhere to the provisions of this AUP and other University policies such as the *Email Appropriate Use* and *Web* policies detailing specific use of the services. Uploading to or sharing of SMU Information or digital resources, (e.g. eLearn Course Materials) on non-SMU endorsed systems, social websites or public platforms (e.g. CourseHero, etc.) are strictly prohibited. Additional restrictions, where applicable, may be imposed by the Deanery of their respective schools and Dean of Students.

Policy Enforcement

5.23. **Use is Revocable**. The use of software, databases, and/or computer and network resources at SMU is a revocable privilege. All faculty, staff, students and authorised users using SMU's IT facilities are responsible for using

these resources and facilities in an effective, ethical, and lawful manner. The use of University IT Resources has been made available for the purpose of supporting teaching, learning, research, professional development and administration within SMU.

5.24. **Disciplinary measures** for violation are normally applied by the University office or department appropriate to the violation. Violators may be subject to additional penalties and disciplinary actions by the University and are also subject to international and Singapore laws governing interactions that occur on information technology systems and the Internet. The University may restrict or deny access to information technology resources temporarily or permanently, prior to the initiation or completion of disciplinary procedures when it appears necessary to protect the integrity, security, or functionality of the University's IT resources.

5.25. **SMU's right to Indemnity**. Failure by users to observe the policies within this AUP may also result (directly or indirectly) in SMU being involved in claims and/or suffering damages, losses and expenses. The user shall indemnify SMU and its officers from such claims, damages, losses and expenses resulting from the user's intentional failure to observe the policies. In addition, the user must understand that SMU will cooperate in any official investigations resulting from any breach of the policies and may, in its discretion, decide to furnish the relevant authorities/parties with the relevant information and your consent to any such disclosure shall be deemed by your acceptance of this policy.

5.26. **Waiver**. When restrictions in the policies interfere with the research, educational or service missions of the SMU, members of the SMU community may request for a written waiver from the Chief Information Officer of Integrated Information Technology Services or his designee.

6. SUB-POLICIES OR OTHER GUIDELINES

6.1. AUP Supplemental: University Licenced Software
Supplemental provides additional guidance on removal of University licenced software due to conclusion or termination of program.

6.2. AUP Supplemental: Commercial Databases
Supplemental provides further guidance on permitted access to SMU-subscribed Commercial Databases that SMU Authorised Users are expected to comply.

SMU IT POLICIES & PROCEDURES

7. ROLES AND RESPONSIBILITIES

7.1 All Users of University IT Resources

7.1.1 All SMU faculty, staff, students and authorised users have an obligation to report misuse of University IT resources or suspected breaches of conditions in this AUP to the IT Help Centre.

7.2 University Administration and School Deanery

7.2.1 Investigate and manage all breaches or suspected breaches of this AUP concerning Faculty members in accordance with established University guidelines and policies stated in the University Handbook.

7.3 Office of Dean of Students and Schools

7.3.1 Investigate and manage all breaches or suspected breaches of this AUP concerning students in accordance with established University guidelines and policies in the University Handbook.

7.4 Office of Human Resources

7.4.1 Investigate and manage all breaches or suspected breaches of this AUP concerning SMU administrative staff and other non-faculty users in accordance with established University guidelines and HR policies.

7.5 Office of Integrated Information Technology Services

7.5.1 Provides the technology support for investigating infringements or alleged breaches of this AUP.

7.5.2 Executes the technology related sanctions where applicable.

7.6 Office of Legal and General Affairs

7.6.1 Provides legal guidance to the University.

8. POLICY REVIEW

SMU reserves the right to amend this AUP (and its Supplemental) and/or implement additional policies periodically. Although Integrated Information Technology Services (IITS) will inform users of policy changes, users must share the responsibility of staying informed about SMU policies regarding the use of the University IT Resources and complying with all other applicable policies.

SMU IT POLICIES & PROCEDURES

9. RELATED DOCUMENTATION, FORMS AND TOOLS

- Computer Misuse Act (Chapter 50A)
- Cybersecurity Act Singapore 2018
- Copyright Act (Chapter 63)
- Personal Data Protection Act 2012 (PDPA)
- Sedition Act (Chapter 290)
- SMU Academic Policies
- Spam Control Act (Chapter 311A)
- Digital Copyright Policy
- SMU Email Policy
- Web Policy

10. CONTACT INFORMATION

Please address queries to

Tang Ai Chee, IITS
Email: ITpolicies@smu.edu.sg

SMU IT POLICIES & PROCEDURES

11. DOCUMENT CHANGE HISTORY

Sno	Change Date	Version No	Reference	Description of Change	Effective Date
1	09 Jul 2013	2.1	Addendums	Added Supplemental on University Licenced Software and Supplemental on Use of Commercial Databases	9 Jul 2013
2	11 Feb 2014	Version 2.1	Item 5.15.4 Item 5.15.5 Item 5.17.3 Item 5.22 Item 9 and References	Replaced “Computer Misuse Act” with “Computer Misuse and Cybersecurity Act” and all Internet url links.	31 Jul 2014
3	11 Aug 2014	Version 2.2	Item 5.15.4 Item 5.15.5 Item 5.17.3 Item 5.22	Replaced “Computer Misuse Act” with “Computer Misuse and Cybersecurity Act”, SMU Email Policy and Web Policy url links.	14 Aug 2014
4	11 Aug 2014	Version 2.2	Item 4.5	Append new statement in item 4.5 to include PDPA Act (with Legal advised).	14 Aug 2014
5	11 Aug 2014	Version 2.2	Item 5.15.6	Append new statement in item 5.15.6 to include PDPA Act (with legal advised).	14 Aug 2014
6	11 Aug 2014	Version 2.2	Item 9 References	To include PDPA link and update all other url links.	14 Aug 2014
7	23 Apr 2015	Version 2.2	Approved by:	Chief Information Officer and Vice President, IITS	22 Jun 2015
8	28 Nov 2017	Version 2.4	Header, Item 5.13.2 Item 5.13.3	1. Insert SMU Classification. 2. Replaced old para 5.13.2 and 5.13.3 with the following: a. 5.13.2 - “Users must not steal or attempt to use methods of electronic or any means (e.g. software, hardware or firmware) to eavesdrop on passwords, contents and information that he/she is not authorized to access.” b. 5.13.3 - “University IT Resources shall not be used to access, transmit, store,	1 Dec 2017

SMU IT POLICIES & PROCEDURES

				display or request for inappropriate content such as obscene, pornographic, erotic, profane, racist, sexist or defamatory or offensive materials." 3. Updated definitions of Data and PC 4. Added statement "Uploading to or sharing of SMU Information or digital resources, (e.g. eLearn Course Materials) on non-SMU endorsed systems, social websites or public platforms (e.g. CourseHero, etc.) are strictly prohibited."	
			Item 4.1 and 4.3 Item 5.22		
9	22 Sep 2019	Version 2.5	Item 5.15.4, Item 5.15.5, Item 5.15.6, Item 6.1, 6.2 Item 9	1. Edit Hyperlinks for : • Computer Misuse Act, Cybersecurity Act 2018, • Sedition Act (of Singapore) (Chapter 290). • Copyright Act (Chapter 63) • Personal Data Protection Act 2012 (PDPA) • General Laws, • Spam Control Act, • SMU Academic Policies • University Licenced Software 2. Update para 6.1. 3. Update related documentation, forms and tools 4. Due to PDPA, remove NRIC/FIN requirement in Appendixes.	23 Sep 2019

SINGAPORE MANAGEMENT UNIVERSITY
ACCEPTABLE USE POLICY (AUP)
Supplemental on University Licenced Software

Software licenced by the University

SMU has acquired the license for the use of a collection of software ("University Licenced Software") to facilitate and enhance the teaching and learning experience at SMU and extends to users the right to use the Software on a personally-owned computer (in the case of students) or an institution-owned computer designated for the respective user's use, if the relevant user acceptance forms have been signed.

Details of the software Software Licensed by the University can be obtained in this url link: https://itsupport.smu.edu.sg/hc/en-us/sections/200627710-Software-Acquisition-and-Support.

For avoidance of doubt, users do not own the license to the University Licenced Software; rather, a user is authorized to use the Software and associated media pursuant to the terms and conditions of the license(s) granted to SMU for the term of relevant software licence.

Whilst a user is a student, faculty or staff at SMU and receives a copy of the University Licenced Software for use, the user must read and abide by the license(s) associated with the Software.

The licence to use the relevant University Licenced Software will terminate upon

(a) any event, with the exception of graduation, which causes the user to no longer to be a student of SMU; or
(b) expiration of the relevant campus software licence ("Campus Licence") licensed period.

Upon such termination of the relevant University Licenced Software licence, the user must delete or remove the associated software immediately from his/her personally owned computer(s).

~~~~~~~~~
~~~~~~~~~

SINGAPORE MANAGEMENT UNIVERSITY
ACCEPTABLE USE POLICY (AUP)
Supplemental on Use of Commercial Databases

Use Of Commercial Databases Policy

Providers of commercial databases ("Commercial Databases"), who licence their databases for use in educational institutions, usually restrict the authorized user group to currently enrolled students and currently employed faculty and staff ("Authorized Users"). Additional restrictions may also apply.

In order to be permitted access to SMU-subscribed Commercial Databases, Authorized Users must agree to use such subscribed databases in the manner required by the respective providers, in particular, any use must be for personal and academic purposes only. "Personal use" may include preparation for job interviews, manuscript writing and other activities strictly related to one's work at SMU. "Academic use" must be directly related to research and/or classroom activities.

Authorized Users are not allowed to use their database accounts for any other activities, including but not limited to consulting or other purposes, for which a fee is charged. The use of SMU-subscribed Commercial Databases to support internship work is strictly prohibited.

~~~~~~~~~~ ~~~~~~~~~~
~~~~~~~~~~

SMU IT POLICIES & PROCEDURES

APPENDIX A – ONLINE ACKNOWLEDGEMENT FORM

By clicking on the "I Accept" button in this webpage, I indicate that I have read, understood and accepted the Acceptable Use Policy set out above, including any revisions to the same.

Name: _____

Faculty / Staff / Student Campus ID.: _____

School / Office: _____

User name issued: _____

Date: _____

Accept / Decline (buttons)

SMU IT POLICIES & PROCEDURES

APPENDIX B – USER ACKNOWLEDGEMENT FORM

I have read, understood and accepted the Acceptable Use Policy set out above, including any revisions to the same.

Name: _____

Faculty / Staff / Student Campus ID.: _____

School / Office: _____

User name issued: _____

Signature: _____

Date: _____

Note:

Kindly return the signed blue copy to
Office of Integrated Information Technology Services (IITS),
C/o IT Help Centre
Concourse, SOA/SOL
Singapore Management University