The use of software, databases, and computer and network resources at SMU (“SMU IT Resources”) is a revocable privilege. All faculty, staff, students and authorized users using SMU’s IT facilities are responsible for using these resources and facilities in an effective, ethical, and lawful manner. The use of these resources have been made available for the purpose of supporting teaching, learning, research, professional development and administration within SMU.

The following policies (and accompanying Supplementals) are intended to help users with the appropriate use of SMU IT Resources. If a user does not abide by these policies, his/her computer account may be suspended and denied access to SMU IT Resources. Depending on the severity, disciplinary actions ranging from a fine, examination exclusion, expulsion from SMU, employment termination and/or legal action may be taken. Users are also reminded that unauthorized access, modification or interception of computer programmes or data can amount to serious criminal offences under the Computer Misuse Act (Cap 50A), Spam Control Act (Cap 311A) and under the general Singapore law.

SMU reserves the right to amend this AUP (and its Supplementals) 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 SMU IT Resources and complying with all other applicable policies.

Failure by users to observe the policies below may 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, 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.

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 designee.

General Policy

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

Files owned by individual users are considered private property, whether or not they are accessible by others. Under no circumstances may a user alter a file that does not belong to him without prior permission of the file’s owner. The ability to alter another user’s files does not in itself imply the permission to alter those files.

Network Policy

1. SMU IT Resources may not be used for making unauthorized connection to, 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.

2. 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.

3. When accessing other organizations' IT facilities & resources from the SMU network, users are responsible for abiding by these guidelines and the relevant policies of such other organizations.

4. Users must not tamper with SMU network outlets, such as extending the cable to relocate the outlet to another room or open area temporarily or permanently, blocking it for access from other users if it is on a shared basis, or to connect certain devices for wire taping, etc.

5. Users must inform IITS to remove their SMU network configuration setting before they sell their PCs, termination of employment, leaves the university before graduation or upon graduation.

6. Users must not attempt to intercept, capture, alter, or interfere in any way with information on local, campus or global network pathways. This also means users may not run "sniffers" (programs used illegitimately to capture information being transmitted) on the campus network or any portion thereof.

7. 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.

8. The privilege of using SMU equipment, wiring, 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 authorization.

Accounts and Passwords Policy

1. Accounts are assigned to individuals and are not to be shared unless specifically authorized by the IITS. Users are solely responsible for all functions performed from the accounts assigned to them. Do not allow others to use your account.

2. Users should safe guard their computer accounts and passwords. They should not carelessly or negligently give or allow any person access to their computer accounts or passwords.

3. 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 authorized to use.

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

5. Users are responsible to ensure the secrecy of their passwords by
   - changing any pre-assigned default password at the first possible opportunity.
   - avoiding composing passwords based on their personal information (e.g. name, user ID, date of birth, etc.)

E-Mail & Web Policies

The following conduct/actions are prohibited for users of the SMU E-mail account and the offender will be held liable for:

1. harassing, sending pornographic or defamatory materials/messages via E-mail or through posting to Web pages

2. sending or posting forged E-mail (masquerading), web pages and newsgroups messages

3. massive or unsolicited E-mailing without explicit approval from IITS

4. flooding a user or site with very large or numerous pieces of E-mail

5. sending or forwarding of confidential SMU information via E-mail

Software Policy

SMU provides ONE University Licenced Software license per user (meaning ONE for each student, faculty and staff) regardless of the number of PCs or purchased via SMU's PC Tender.
Users:

1. should have the anti-virus software running on their PC and update the anti-virus signature file regularly
2. should regularly update the Windows Update patches on their PC
3. must uninstall all University Licensed Software from their PC when selling their PCs, termination of employment, leaves the university before graduation or upon graduation.

Users must not:

1. develop and/or use programmes that may/will harass or harm other users of the system;
2. develop and/or use programmes that may/will attempt to bypass system security mechanisms, steal passwords or data;
3. 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;
4. develop or use programmes designed to replicate themselves or attach themselves to other programmes, commonly called worms or viruses; and/or
5. develop and/or use programmes designed to evade software licensing or copying restrictions.

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

Users must:

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

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

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

References:
Computer Misuse Act (Cap 50A), Spam Control Act (Cap 113A) & General Laws: [http://agcvldb4.agc.gov.sg/](http://agcvldb4.agc.gov.sg/)
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 included in this collection and the relevant user acceptance forms, are available from IITS Helpdesk.

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 (a copy of the licence is available from IITS Helpdesk).

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

(a) any event, with the exception of graduation, which causes me 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).

*Graduating Student Licence Scheme - Microsoft*

Graduating SMU students will be given an option to convert some Microsoft software under the Microsoft Campus Licence to a perpetual personal license (meaning a licence granted from Microsoft to a SMU graduate student personally). This scheme is only applicable for SMU graduate students and is generally not available for faculty and staff.

To convert the relevant licence, a Student License Confirmation Form, must be obtained from IITS Helpdesk, prior to graduation.

Graduating SMU students who have not obtained and signed the Student License Confirmation Form, will be required to remove the Microsoft software from their personally-owned computer, prior to graduation.
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.

Please enquire with the Li Ka Shing library staff for details.

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 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 Commercial Databases to support internship work is strictly prohibited.