SUNWAY EDUCATION GROUP

IT SERVICES DEPARTMENT

Student ePolicy

IT Services Department(ITS) provides computing, networking and information technology support services to its students and staff.

This Student ePolicy outline key IT systems and services usage policies for students using IT services in Sunway Education Group (SEG) of campuses.

1. User privileges

I understand that:

1.1 The open access through the computers and network is a privilege. Thus, agree to act responsibly while using this facility.

1.2 The user may not use the computer systems to create unnecessary network traffic or send junk mail, chain letters, and any offensive or disruptive messages.

1.3 The user may not use the computer systems to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other unauthorized solicitations.

1.4 The user may not use the computer account of another user. **Account owner are advised not to share their computer account, user ID and password.**

1.5 Users are responsible for safeguarding their passwords for access to the computer system. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords.

1.6 Masking the identity of an account of machine is also prohibited.

1.7 The computer facilities are created to help us work effectively and efficiently. Personal use of the computer systems that may burden the campus with or without incremental costs is therefore not acceptable.

1.8 **The user may not use Sunway Education Group computer sytems to gain unauthorized access to any computer systems**.

1.9 The user may not knowingly perform an act which will interfere with the normal operation of computers, terminals, peripherals or networks.

1.10 The user may not knowingly run or install on any computer system or network, or give to another user, a program intended to damage or to place excessive load on a computer system or network.

1.11 **The user may not attempt to circumvent data protection schemes or uncover and exploit security loopholes**.

1.12 The user may not violate terms of applicable software licensing agreements or copyright laws.

1.13 The user may not deliberately waste computing resources provided by SEG, or unfairly monopolize resources to the exclusion of others.

1.14 The user may not post materials on electronic bulletin boards that violate existing laws or SEG codes of conduct.

1.15 The user may not attempt to monitor or tamper with another user's electronic communications, including reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

1.16 The user must respect the rights of other users as well as the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

1.17 Files may be subject to search under court order. In addition, system administrators may access files or accounts suspected of unauthorized use or misuse, or that which may have been corrupted or damaged.

1.18 SEG reserves and will exercise the right to review, audit, intercept, access, and disclose all matters concerning the computer systems.

1.19 All files and email messages transmitted by, received from, or stored in SEG computer systems are the property of SEG.

1.20 Privately owned hardware and software are not allowed to be connected to the local area network or to be attached to any equipment which is connected to the network without the approval of ITS.

1.21 All modem dial outs while connected to the SEG network is prohibited.

1.22 In-campus hostel internet access is a value added service provided by SEG to its students. Hostel residents are responsible to ensure that their personal computer has proper OS security patches installed, and antivirus software updated with latest virus pattern.

2. Compliance issues & actions

2.1 Minor infractions of this policy or those that appear accidental in nature are typically handled internally in an informal manner by electronic mail or face-to-face discussions. More serious infractions are handled via formal procedures. In some situations, it may become necessary to suspend account privileges to prevent ongoing misuse while the situation is under investigation.

2.2 Serious infractions, such as unathorized use of resources, attempts to steal passwords or data, unauthorized use or copying of licensed software, violations of campus policies, or repeated violations of minor infractions, may result in the temporary or permanent loss of access priviledges. In all cases, the offender's associated school of department will be notified of the infraction. If the offender is a student of SEG institution, the case will also be referred to the respective institution management for appropriate action.

2.3 Offences that are in violation of local, state, or federal laws will result in the immediate loss of user privileges, and will be reported to the appropriate University and law enforcement authorities. Users are advised to adhere to the Malaysia Cyberbills as follows:-

2.3.1 Computer Crimes Bill 1997

2.3.2 Copyright (Amendment) Bill 1997

2.3.3 Digital Signature Act 1997

2.3.4 Telemedicines Bill 1997

2.3.5 Communications and Multimedia Act 1998

2.3.6 Digital Signature Regulations 1998

2.4 SEG reserves the rights to modify or discontinue, temporarily of permanently computer systems access with or without notice to user. User should be aware that SEG is not to be held responsible for any modification or discountinuance of access rights to the computer systems.

2.5 Any user who discovers a violation of this policy shall notify ITS. Any such report will be classified as private and confidential.

Comprehensive version of "Sunway Education Group e-Policy" can be obtained from Sunway campus Vine intranet for further reference.

SEG management reserves the right to review and amend this policy whenever necessary. Students should understand and read the latest revision available in Sunway campus Vine intranet fromt time to time.