Springfield Secondary School
Acceptable Use of ICT Policy (AUIP) for 2015

Computers are used to support and enhance learning. Internet access allows users to share resources, innovations, experiences and interact with people from all over the world. This policy is intended to prescribe the appropriate behaviour and use of ICT resources by users in an effective, ethical and lawful manner.

This policy applies to the use of the ICT resources owned and managed by Springfield Secondary School, as well as those brought in for use by users. ICT resources include computer accounts, servers, disk storage, software, email, public folders, network and the Internet. All users are to comply with this Policy.

General Policy
1. Users shall use the ICT resources according to the purpose for which they are provided, which is for the administrative, teaching and learning activities in the school.
2. Users shall not use engage in any activities relating to the use of the ICT resources that will be in violation of the laws of Singapore, in particular (but not limited to), the Computer Misuse Act (Cap 50A, available at http://statutes.agc.gov.sg/) as may be amended from time to time. Some examples of such illegal uses are:
   (i) Downloading, distribution, sharing or storing of seditious, obscene or pornographic materials;
   (ii) Infringement of any copyright and intellectual property right.
3. Users shall use only software that meets legal requirements, such as having valid licences.
4. Users shall not use, modify or adapt ICT resources for commercial purposes or financial gains.
5. Users shall immediately report any violations or suspected violations of laws or policies as well as any loopholes or potential loopholes in the security of the ICT resources to the ICT Department.

Copyrighted Materials & Licensed Software, Programmes & Data
Users shall:
6. not transfer, duplicate, make available or obtain illegally, any copyrighted material including, but not limited to, agreements, licensed software, programmes, data, music, films and other literary and artistic works;
7. not make, store transmit, upload or make available unauthorized copies of copyrighted material on the school's systems, equipment or storage media, or via the School Network or the Internet using the school's systems, equipment or storage media;
8. not assist or participate in any infringement of copyrighted materials by operating or connecting to a peer to peer network or index, using the school's systems, equipment or storage media;
9. respect the rights of others by complying with all the school policies regarding the protection and use of intellectual property;
10. not install unlicensed or unauthorized software in the local hard disk or server drives; and comply with the guidelines of any third party organization that the School may from time to time agree to adopt for its implementation.

Failure by users to observe the abovementioned policies may result, whether directly or indirectly, in the school being involved in claims and/ or suffering damages, losses and expenses. A user shall indemnify the school and its officers for any such claims, damages, losses and expenses resulting from the user's failure to observe any of the above stated policies.
Account UserIDs and Passwords
11. Users shall be responsible and accountable for all activities conducted via his/her account.
12. Users shall not reveal their login userIDs and passwords (to any school system) assigned to them.
13. Users should change the temporary or issued password at the first logon. They shall change their passwords regularly to prevent break-in and whenever there is any indication of possible system or password compromise.
14. Users shall not use the user account for any illegal activities. These include making unauthorised attempts to gain access to any account not belong to him/her, hacking into computer systems, spreading computer viruses or sending undesirable materials.

Computer System and Electronic Storage Media
15. Users shall ensure that their systems are adequately protected before connecting to the school’s network.
   (i) An up-to-date anti-virus software installed and activated;
   (ii) A personal firewall installed and activated;
   (iii) Latest software security patches installed.
16. Users shall not place their computer and portable electronic storage media near an external window or public access area where it could be subjected to physical theft.
17. Users shall not leave their computer and portable electronic storage media unattended. If it is not possible, the computer shall be securely locked away when not in use or secured with a cable lock by attaching it something immovable.

When Travelling Overseas for Internationalisation Programme
18. Users are not allowed to use MOE-issued notebooks for overseas travel without the Principal’s permission. After permission has been granted by the Principal, users shall only hand-carry their computer and portable electronic storage when travelling overseas. These shall not be checked in as check-in luggage.
19. When clearing customs, users shall hold onto their computer and electronic storage device until the person in front has gone through the method detector and shall continue to keep an eye on them when they go through the X-ray belt and emerge on the other side of the screener.

Email Usage
20. Users shall not transmit libelous, slanderous, defamatory in nature, threatening or abusive messages or any messages that may be reasonably construed as such.
21. Users shall not forward messages containing general appeals or warnings like ‘virus warnings’, ‘request for help’, by mass mail or otherwise.
22. Users shall not forge the identity of or impersonate another person in an email.
23. Users shall not knowingly transmit by email any harmful or malicious content (e.g. viruses) or any other content or material that may otherwise violate the civil and criminal laws of Singapore.
24. Users shall not flood an individual, group or the email system with numerous or large emails.

Internet Access, Usage and Social Networking
25. Users shall be discerning when accessing websites. They shall avoid websites of unknown or disreputable origin.
26. Users shall be responsible for all content that they upload, post, email, transmit or otherwise make available via the school network.
27. Users shall not upload or download, send or post, enter or publish any content to the internet that is objectionable or illegal under the Singapore Law.
28. Users shall not upload or download, send or post, enter or publish any content to the internet that is against the public interest, public order, national interest, racial and religious harmony, or which offends good taste or decency, or is otherwise indecent, obscene, pornographic or defamatory.
29. Users shall not upload or download, send or post, enter or publish any content to the internet that is confidential, distasteful or prejudicial to the good name of the school.
30. Users shall be mindful of public nature of the internet and shall not discuss or disclose confidential and proprietary information of the school or any organisation.
31. Users shall be respectful to staff and students and their rights for privacy.
32. Users shall be mindful of the need to protect your own privacy.

**Segregated Wireless School Network Connection**

33. Users are allowed to use the wireless school network SWN@SSOE available in the school premises.
34. Users are not allowed to share their IAMS userid and password to anyone else to use the SWN@SSOE wireless network. Users are to refer to the guidelines found on the school website to enable them to access the SWN@SSOE network.
35. Users shall not install and operate their own wireless Access Points emulating or interrupting the performance of the school’s network infrastructure wireless access points.
36. Users shall not attempt to monitor another user’s data communications nor access, read, copy, change or delete another person’s files or software without authorisation.
37. Users shall not install or use diagnostic and/or vulnerability scanning tools on school’s network under any circumstances, as such tools may be used to compromise the security of the network.
38. Users shall not indiscriminately issue search instructions and download data manually or via automated intelligent agents that may potentially consume large amount of network/ internet bandwidth and ICT resources, or which may degrade the network performance.
39. In an event that the situation poses an immediate security threat to the ICT resources or other external systems, the school may disconnect the user’s computer or ICT equipment from the school’s network and/or disable the user account for further pending actions and notify the user accordingly.

**ICT facilities in Computer Labs / Special room**

40. Users may enter or work in the Computer Labs/ Special rooms with ICT facilities with a teacher being present.
41. Users are to ensure that teachers are to be with them.
42. Users are to be responsible for the computer facility/terminal/desktop/notebook/tablets used.
43. Users are to ensure that they scan their external storage devices/media for virus. Users are to inform the relevant IT personnel or teachers immediately if they detect the presence of the virus. Users are not allowed to delete or rename or move files in the hardisk.
44. Walking about, playing and running about is not allowed in these premises.
45. Eating and Drinking are not allowed.
46. Users are to ensure general cleanliness of the premises and ensure furniture is returned to its original position.
47. Users are to ensure that all ICT equipment used are returned to the teacher or IT personnel.

**Loan of ICT notebook/tablets or Use of Personal smart devices/notebook/tablets**

48. Users are allowed to do a short term loan / home-loan of notebooks and iPads from the school library or ICT Executive personnel with the permission of their teachers. Please refer to the loan form.
49. Users are responsible for the safe-keeping of the equipment at all times. Users are to check and ensure that the ICT equipment loaned are returned back in good working condition. Users will have to bear the cost of any repair or loss of equipment.
50. Users are allowed to bring to school their own smart devices/notebooks/tablets for their use.
Additional Guidelines on use of Personal smart devices/notebooks/tablets in school

1. Students are allowed to bring to school their own personal smart devices/notebooks/tablets with/without internet connectivity during school hours.
2. Students are allowed to use the SWN@SSOE wireless available in the school for internet connectivity.
3. Students are to ensure that all personal ICT/ smart devices are kept secured under their safe-keeping at all times. Students are to be responsible for any loss of such ICT devices.
4. Students are allowed to use the internet connection for their personal use and are to abide the guidelines stipulated under the AUIP for Springfield Secondary School.

In the classroom/special rooms/computer labs
5. Students are allowed to use personal smart devices/notebooks/tablets in the classroom only after permission is granted by the teacher. Otherwise, students are to keep this device.

Failure to adhere to the policy and guidelines above may result in the suspension or revocation of the user account. In serious cases, students may also face disciplinary action in school and/or prosecution in the court of law if he/she uses his/her account for illegal purposes.

ICT department
Springfield Secondary School
Updated on 28 February 2015