# NBSS Acceptable Use Policy

**General Policy**

1. Students are to read this Policy in relation to the Government Instruction Manual, IM8: Information Technology.

2. Students shall use the ICT resources according to the purpose for which they are provided, which is for learning activities.

3. Students 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.

4. Students shall use only software that meets legal requirements, such as having valid licences.

5. Students shall not use, modify or adapt ICT resources for commercial purposes or financial gains.

6. Students 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.

**Account UserIDs and Passwords**

7. Students shall be responsible and accountable for all activities conducted via his/her account.

8. Students shall not reveal their login userIDs and passwords (to any school system) assigned to them.

9. Students 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.

10. Students 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**

11. Students shall ensure that their systems are adequately protected before connecting to SSOE 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.

12. Students shall not place their computing devices near an external window or public access area where it could be subjected to physical theft.

13. Students shall not leave their computing devices unattended. If it is not possible, the device shall be securely locked away when not in use or secured with a cable lock by attaching it something immovable.

**Internet Access, Usage and Social Networking**

21. Students shall be discerning when accessing websites. They shall avoid websites of unknown or disreputable origin.

22. Students shall be responsible for all content that they upload, post, email, transmit or otherwise make available via the school network.

23. Students 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.

24. Students 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.

25. Students 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.

26. Students shall be mindful of public nature of the internet and shall not discuss or disclose confidential and proprietary information.

27. Students shall be respectful to staff and students and their rights for privacy.

28. Students shall be mindful of the need to protect your own privacy.

**Network Connection**

30. Students 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.

31. Students shall not install or use diagnostic and/or vulnerability scanning tools on the SSOE network under any circumstances, as such tools may be used to compromise the security of the network.

32. Students 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 degrade network performance.

33. 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 device from the school's network and/or disable the user account for further pending actions and notify the user accordingly.

**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.**