

# RULES GOVERNING THE USE OF DIGITAL DEVICES

Devices in school or brought to school that can be used to access the internet are to be used only for the purpose of enhancing and supporting one's learning. The following are stipulations that govern the use of such devices on campus in a way that is ethical.

These stipulations apply to the following: computer accounts, mobile computing devices (e.g. laptops, tablets, etc.), handphones, smartwatches that can access the internet, servers, disk storage, software, email, public folders, network and the Internet.

## General Policy

1. ICT resources are to be used only for administrative, teaching and learning activities in the school. The use of digital devices and/or resources, including the Internet, during school hours, is only permissible when supervised or granted permission by a staff member of SJI.
2. ICT resources are not to be used in violation of the laws of Singapore, in particular (but not limited to), the Computer Misuse and Cybersecurity 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) Downloading of viruses and/or software such as but not limited to hacking and file-sharing software;
  - (iii) Infringement of any copyright and intellectual property right.
  - (iv) Software that have invalid licences.
3. Students who purchase a mobile computing device under the National Digital Literacy Programme (NDLP) are to adhere to the guidelines stipulated in the Acceptable Use Policy (AUP) found at <https://www.sji.edu.sg/ndlp>.
4. ICT resources are not to be used or adapted for commercial purposes or financial gains.
5. It is the duty of all on campus to immediately report any violations of laws or policies as well as any loopholes or potential loopholes in the security of the ICT resources to the ICT Department.

## Computer System and Electronic Storage Media

6. It is the responsibility of all to ensure that the ICT resources they are using are sufficiently protected before connecting to school's network and this is achieved through the following:
  - (i) the installation of the latest up-to-date anti-virus software;
  - (ii) the installation of the latest up-to-date firewall;
  - (iii) the installation of the latest up-to-date software security patches.
7. The security of the personal ICT resources is the sole responsibility of the owner. As such, everyone should take precautions to prevent theft or vandalism. For example, the mobile computing device must never be left unattended, and must be kept in the locker secured with a reliable lock during recess and at all times when the device is not required for lessons. Students are to be careful with their device during travelling.

## **Internet Access, Usage and Social Networking**

8. Accessing or exploring online locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as but not limited to social networking sites and games, during school hours, is to be avoided unless explicitly granted permission by an academic staff member of SJI. Websites of suspicious or disreputable origin are to be avoided at all cost.
9. Content deemed to be objectionable and/or illegal under the law are not to be uploaded, downloaded, sent or posted, entered or published on the internet. This includes content that is deemed to be against
  - a. public interest and public order,
  - b. national interest,
  - c. racial and religious harmony,
  - d. decency (this includes material that is of a pornographic or defamatory nature)

It is the sole responsibility of those who use the internet to ensure that the above do not happen.

10. In addition to the above, content that is deemed confidential, distasteful or prejudicial to the good name of the school must not be uploaded or downloaded, sent or posted, entered or published on the internet.
11. The respect for the right to privacy of staff and students must be observed by all who use the internet. Cyber-bullying and playing pranks to taunt or embarrass others are acts that will result in disciplinary actions being taken against the perpetrator(s).
12. It is important to note that the internet is a public space and as such, matters of a confidential, personal or sensitive nature must not be discussed online especially if it may be prejudicial to the good name of an individual or that of the school.
13. As the purpose of the digital device is for the purpose of learning, intentionally wasting of finite resources, eg, making use of the school network for real-time video, music and gaming is not allowed. Playing music loudly is disruptive to the learning environment and is therefore not permissible.
14. Causing congestion on the school network or interfering with the work of others, e.g., chain letters or broadcast messages to list or individuals is to be avoided.
15. Tampering with others' digital devices, including attempting to log into, deleting files and wrongfully possessing others' digital devices is deemed an illegal act and will warrant disciplinary actions for be taken against the perpetrator(s).
16. Only an academic staff member may instruct students to share their digital device with other students

## **PRIVACY**

17. Making an audio or video recording and taking photographs of anyone, and reproducing them on any public or digital platform without permission is not allowed and may lead to a disciplinary action being meted out.

**Disciplinary actions will be taken against any student who fails to comply with the above and this may include suspension of accounts and confiscation of devices up to two weeks.**

## **RULES GOVERNING THE USE OF HANDPHONES IN SCHOOL**

In keeping with the school culture of solidarity with the poor and voluntary simplicity, the school strongly advises parents, if they wish their child to bring a hand phone to school, to purchase for their child only a simple 'entry model' phone, (i.e. not purchase a state of the art phone with all the latest features). This will minimize replacement costs in case of loss or damage.

1. There will be a total ban on the use of hand phones by students from 0730 hrs to dismissal every school day. Any handphone found with a student during those hours will be confiscated. Confiscated phones will be returned at the discretion of the Head of Level / Head of Discipline. Parents must come to collect confiscated handphones.
2. All hand phones should be turned off (not just put on silent mode) by 0725 hrs. Each hand phone will be clearly labelled with the owner's name and class. The hand phone of ALL Year 1 to 4 students is to be locked away in the personal locker from 0725 hrs to dismissal.
3. The hand phone may be required for a particular lesson by a teacher. The hand phone must be kept away in the locker after the lesson.
4. Students are not to use the hand phone during break time. Any student found using the hand phone during these times will have the hand phone confiscated.
5. The phone should be switched off during all afternoon lessons/remedial or CCA meetings/training.
6. The hand phone is not to be used during official school events on or off site.
7. Parents will not be able to have free telephone access to their sons during school hours because of the disruption caused to lessons. In the case of an emergency, they will have to call the school office. For a non-emergency they should SMS their son and leave a message for him to return a call as soon as he reads the message after school dismissal.
8. Making an audio or video recording and taking photographs of anyone, and reproducing them on any public or digital platform without permission is not allowed and may lead to a disciplinary action being meted out.
9. Students are to seek the approval of the Head of Discipline, Head of Level, Form/TG Tutors or CCA/CAS tutors before creating any school-related social media accounts. These accounts will be monitored and moderated by a staff member of SJI. Disciplinary actions will be meted out to students who create or upload any unauthorized or inappropriate social media account or post.

**THE FINAL INTERPRETATION OF THE ABOVE RULES RESTS WITH THE SCHOOL  
ADMINISTRATION**