IST Campus Network Guidelines

Purpose

The IST campus network consists of hardware, software, network equipment, wireless and private lines. The campus network supports the school's academic requirements, administrative activities, e-learning, etc. These guidelines are formulated to strengthen information ethics and to safeguard legal rights and shall be used as the basis of reference for administrators and users of the campus network.

Users are to utilize networks and Internet services for school-related purposes only. To connect to the school network, users must comply to the campus network acceptable use policy, and related polices and regulations.

Hardware

- Users are allowed to bring personal devices to school.
- Students are not allowed to change school computers/tablet PCs configuration or system settings.
- School laptops, tablets, and other equipment are valuable educational resources. Without approval from school director, users are not allowed to take school hardware off campus.
- Users are not allowed to connect personal network equipment (e.g., wireless AP, Mini Mobile station, etc.) into the school network.

Software

Users should respect intellectual property rights and may not engage in any of the following behaviors that infringe upon network intellectual property rights:

- Unauthorized use of the computer program/APPs.
- Illegal downloading or copying of work protected by copyright Law.
- Uploading protected work onto open websites without authorization of the copyright holder.
- Reproduction of articles on websites or other online forums unless explicitly approved in advance by the author.
- Set up websites for the public to download protected work.

- Other acts that may infringe upon intellectual property rights.
- All school licensed software on private devices will be removed before users leave IST.

Inappropriate use of network

Network users may not engage in the following behaviors.

- Distribute malware intentionally or execute any malicious program to cause interference and/or unusual network traffic;
- Intercept network communications without authorization;
- Spy on the individual login identification of other users;
- Attack school servers or other users' computers;
- Share one's own login identification;
- Spy on or illegally access unauthorized files, emails, etc.
- Exploit network resources to perform malicious actions (e.g., sending spam or other malicious programs) that may adversely affect networks and/or systems;
- Use emails, online chats, websites or other similar tools to commit actions that are against social etiquette, and which include but are not limited to the dissemination of rumors, fraud, slander, insult, defilement, harassment, or threats;
- Use email, social networks, websites or other similar tools to publish any opinions that attack others' religious beliefs, or spread political views that challenge Chinese laws;
- Engage in activities that violate the objectives of the campus network;
- Abuse network resources or school Internet bandwidth.

Privacy and Confidentiality

Network administrators should respect individual privacy. All personal data will be treated as strictly confidential. Only in the following situations will a user or administrator be asked to disclose user data and thereby compromise said confidentiality:

- For maintenance or inspection of system security.
- Finding evidence of network resource abuse or infringement of intellectual property rights.
- In cooperation with investigation(s) conducted by law enforcement officials, subject to approval from the school director.
- For troubleshooting purpose, under consistent complaint/request from relevant users directly, with the system administrator clearly explaining to the user/s the need to

access confidential information.

Enforcement

Violation of this policy by network users will lead to:

- Temporary suspension of network resource privileges.
- In serious cases, users may also be subject to IST disciplinary action.
- In addition to the first two provisions of the disciplinary action, if a user engages in activities prohibited by law, he/she is solely responsible for his/her actions.