Acceptable Use Policy in Technology (AUPT)

IC provides access to technology for supporting and extending the educational process, engaging in collaborative work, and obtaining, creating, and disseminating information. IC wishes to encourage the growth of technology skills among the students, and realizes that success with projects of personal interest develops skills that will ultimately improve the learning environment at IC. The primary purpose of technology hardware and software is to meet educational purposes and needs, thus computers and electronic devices are provided to the IC community. However, their use should be strictly limited to the above mentioned purposes and shall not include entertainment or private communications, especially during school hours.

IC is an American registered organization, and Lebanon is a signatory on the International Copyright Convention- therefore, software piracy is not tolerated at IC- as it is against the law. The programs on IC computers are licensed and may not be copied. There may be exceptions for donations of unused copyright software, for example, the use of freeware, demo versions, and other school approved programs, however, private software purchased privately may not be installed on IC computers. Each user's data files are personal creations and represent considerable time spent. This must be respected.

All members of the IC community (Administration, Faculty, Staff, Students, Parents, and Alumni) are committed to ensure a safe and supportive environment based on the core values of learning, integrity, tolerance, respect for individual differences, and cooperation. IC does not tolerate digital harassment or bullying practices over the Internet, instant messaging, microblogging sites, or social media platforms including-but not limited to- Facebook, Twitter, WhatsApp, Instagram, Snapchat, TikTok, and other mobile applications. Digital harassment is an act of aggression with the intent to cause

embarrassment, distress, pain, or discomfort to another and may lead to dangerous consequences. Digital harassment is a serious breach to IC's guiding statements, and is strictly forbidden among all members of the IC community. With the addition of Zoom, and other electronic meeting applications to the IC technology portfolio, it is important to remember that recorded sessions are intended solely for the use of the students to whom they are addressed. Therefore, parents and students should not share links to the sessions as well as recordings of sessions outside the classroom. Students and parents should refrain from posting screenshots, or any recordings of an online session on social media platforms, as such actions are a violation of the Acceptable Use Policy.

The normal conventions of courtesy and respect for privacy, as well as common sense rules for personal safety, and IC's internal Regulations apply to electronic communications just as they apply to written or verbal communications. Internet access adds numerous educational benefits, but it is recognized that some material on the Internet can be hazardous as it is illegal, false, or inappropriate for use in a school. Users at IC are expected to avoid inappropriate websites and are advised not to reveal personal information over the Internet and are prohibited from altering electronic communications to hide identities or impersonate another person.

In addition, The IC website is a major publication that contains information provided by, and for, the entire College Community. It is maintained in ways that reflect the mission, vision, values, and achievements of International College.

Furthermore, the importance of privacy and the protection of our students' data cannot be understated. Members of the IC community should abide by the applicable laws that prohibit sharing and distributing data and information regarding children. In that regard, parents and employees acknowledge and agree to comply with all laws and regulations that apply to IC users. Including- but not limited to- the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and the EU/UK GDPR General Data Protection Regulation.

All users must keep in mind that many people share College equipment. Work habits on shared devices impact the ability of others to work productively. When using a shared school computer, users must sign in to their own account, and, when done, sign out and clear browser history and cache as well as downloaded files. IC's computers have been carefully set up for shared use, with network administration, antivirus, security, backup, and data logging programs in use. Users should not attempt to interfere with these programs or disregard

procedures established for the maintenance of the IC network. No one may attempt to gain access to parts of the network or to files they are not authorized to use.

All IC users are required to establish strong passwords that contain small letters, capital letters, numbers, and symbols to guarantee the authenticity of the user accessing their accounts on all school electronic systems, both on campus and remotely. User's passwords need to be properly maintained and changed regularly to avoid the possibility of hacking or identity theft. IC users are strictly forbidden from sharing password information with others. Any password issue can be addressed using the links on the IC website. By accessing the school's network using school-owned or personally-owned equipment, you have consented to the school's exercise of its authority and rights as set out in this policy with respect to any such equipment, as well as with respect to any information or communication stored or transmitted over such equipment. Users are held fully responsible for their accounts and need to seek immediate help from the Administration if they believe their account has been compromised in any way.

Violations of these rules may result in disciplinary action, including the loss of a user's privileges to use the school's information technology resources. Further discipline may be imposed in accordance with the school's code of conduct up to and including suspension or expulsion depending on the degree and severity of the violation.

The use of school owned information technology resources is secure, but not private. School and network administrators and their authorized employees monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy.

Last updated: September 2020

Revised by the School Lawyer: October 2020