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. Therefore, computers and electronic devices are provided to the IC community. However, their use should be strictly limited to the purposes mentioned above and shall not include entertainment or private communications, especially during school hours.

Software Privacy

As a US-registered organization, IC strictly prohibits software piracy. Lebanon's commitment to the International Copyright Convention reinforces the adherence to copyright laws at IC, making software piracy unacceptable and against the law. IC purchased applications are licensed and may not be copied or installed on other devices. There may be exceptions for using freeware, demo versions, and other school-approved programs. Each user's data files are original works of art that require a substantial time and effort commitment.

Digital Harassment and Bullying

All members of the IC community (administration, faculty, staff, students, parents, and alumni) are committed to ensuring a safe and supportive environment based on the IC core values. IC does not tolerate digital harassment or bullying practices on its digital spaces. 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 of IC's Guiding Statements and is strictly forbidden among all members of the IC community. Any inappropriate use of IC’s digital platforms will be subject to strict disciplinary action. IC is not responsible for cyberbullying cases or cases related to inappropriate conduct that takes place outside school spaces, whether digital or physical.

Recording of Online Meetings

With the addition of Zoom and other conferencing applications to the IC technology portfolio, it is important to remember that recorded sessions are intended solely for the use of their intended audience. Therefore, parents and students should not share links to the sessions and session recordings outside the classroom. Students and parents should refrain from posting screenshots or recordings of an online session on social media platforms, as such actions violate the Acceptable Use Policy. Any inappropriate use of conferencing applications will be subject to strict disciplinary action.

Data Privacy

The normal conventions of courtesy, respect for privacy, 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. They are advised not to reveal personal information over the internet and are prohibited from altering electronic communications to hide identities or impersonate another person.

Furthermore, the importance of privacy and protecting 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), the UK Data Protection Act 2018 (DPA 2018), and the EU GDPR General Data Protection Regulation.

IC Website

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

BYOD - Bring Your Own Device Policy

With their parents'/guardian's knowledge and permission and providing that teachers/staff give their consent, students of the Middle and Secondary School levels may use their privately-owned internet-enabled device on the school's wireless network subject to teacher and staff permission.

BYOD refers to any personally-owned internet-enabled device used to complete assignments, projects, and other work. These devices include but are not limited to, computers (laptops, tablets, iPads), all types of mobile phones and devices, and any other technologies as they come into use.

Use of Photos and Videos of Students in School Publications

International College may take and use images, video and photos of students and/or their work for the purpose of promoting or communicating about school activities and events across both campuses. Such activities may include, but not be limited to, athletic competitions, team photos, music and drama productions, classroom activities, group and individual projects as well as recognition of students for their exceptional talents, achievements, and awards. Images and/or published articles may be used in school print and/or electronic publications such as newsletters, yearbooks, and brochures).
Additionally, it may feature on the school website and any of IC's official social media platforms.
Unless otherwise stated in writing and submitted to the school director at the start of every school year, parents and/or legal guardians authorize IC to use photos, videos, and images of students for the above purposes. International College will avoid using personal information that, in the school's determination, represents a privacy or security issue.

IC Devices

All users must keep in mind that many people share school equipment. Work habits on shared devices impact the ability of others to work productively. When using a shared school device, 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 devices have been carefully set up for shared use, with network administration, antivirus, security, backup, and data logging programs.
Users should not attempt to interfere with these programs or disregard procedures established for maintenance and protection. No one may attempt to gain access to parts of the network or to files they are not authorized to use. Jailbreaking or tempering with IC devices is strictly forbidden.

Users are required to back up their files regularly on cloud drives to protect them from loss or theft. Any files shared on local devices (desktops, etc.) must be deleted by their users when done with them.

Passwords

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 passwords must 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 and 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 per the school's code of conduct up to and including suspension or expulsion, depending on the degree and severity of the violation.

Using 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 conform with this policy.

Last updated: May 2024