ICEF Public Schools Student Internet Safety Policy

As a Children's Internet Protection Act (CIPA) complaint organization we are required to have protection measures in place to block or filter access to pictures that are: (a) obscene; (b) pornography; or (c) harmful to minors (for computers that are accessed by minors).

Our Student Internet Safety Policy is intended to provide a safe online educational environment for all students. Students play a big role in their online safety and education.

ICEF and its family of schools' computers, network, electronic data, e-mail, Internet access ("information systems") are educational tools made available to students in order to enhance efficiency in providing educational resources. These systems should be used for school educational purposes only, and not for personal purposes.

Students cannot expect personal privacy rights to extend to information contained on, stored in, or traveling through ICEF schools' systems (internet, and electronic mail). All information or educational systems are subject to periodic, unannounced inspections by the school at ICEF's discretion for any reason deemed necessary by ICEF. ICEF has access to all such information regardless of the use of passwords or other security protection.

ICEF's information systems may not be used in any way that may be disruptive, offensive to others, or harmful to morale or violating school policy or law. For example, ICEF prohibits the display or transmission of sexually explicit images, messages, or cartoons, or any transmission or use of communications that contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparaging of others based on their race, national origin, ethnic group identification, religions, age, sex, sexual orientation, color or physical or mental disability. Students are expected to utilize ICEF's schools' information systems with the same degree of respect and courtesy as is expected of personal face-to-face interactions.

Prohibited Uses and Activities: In addition to the above, students may not:

- Enter websites with inappropriate content
- Use Proxy websites
- Connect computers (including laptops and personal computers) not owned or leased by ICEF to the schools' information systems network without the prior consent of the principal or his or her designee(s).
- Use the access code, log-on or password of other students to gain access to their e-mail, voice-mail or computer records.
- Disclose access codes, log-on or passwords or otherwise make ICEF's electronic Relations available to persons not authorized to have such access; or
- Violate any copyright or license to software, information (including, but not limited to, text images, icons, programs, etc.) whether created by ICEF or any other person or entity. Information on ICEF's information systems, including software, data, and research materials, is proprietary to ICEF schools, and may not be used for personal purposes.

- Infringe on others' access and use of ICEF's information systems, including, but not limited to:

  - o Damage or vandalize ICEF computing facilities, equipment, software, or computer files.
  - o Develop or use programs which disrupt other computer users, access private or restricted portions of the system, and/or damage software or hardware components of the system.
  - o Violate any federal, state or local laws in the use of ICEF's information systems.

Any student who violates this policy may be subject to appropriate disciplinary action, up to and including expulsion.

Social Media Policy

ICEF Public Schools recognizes that students may have personal social media accounts on Facebook, Twitter, etc., and Web-based email accounts such as Gmail, Hotmail, and Yahoo. While ICEF realizes the potential usefulness and increasing importance of social media websites, ICEF also recognizes the potential for misuse. Students **shall not** join or comment in the social media account of others using ICEF provided accounts. Students are not allow to access to their personal social media accounts using ICEF provided equipment or connectivity.

The following Social Media Policy restrictions apply:

• School equipment, including school computers and electronic systems may not be used for these purposes

• Students are prohibited from making discriminatory, defamatory, libelous or slanderous comments of other students.

• Students must comply with all School policies, including but not limited to, rules against unlawful harassment and retaliation.