

Title: **Internet and Online Acceptable Use**

Effective Date: March 13, 2018

References: 53A-3-422,423

Purpose

Ignite Entrepreneurship Academy recognizes the value of computer and other electronic resources to facilitate student learning and help the school's employees accomplish IEA's mission. IEA has, therefore, made substantial investments to establish a network and provide various electronic resources for its students' and employees' use. Because of the potential harm to students and the school from misuse of these resources, IEA requires the safe and responsible use of computers, computer networks including e-mail and the Internet, and other electronic resources. This policy is intended to ensure such safe and responsible use and to comply with Utah State Code 53A-3-422, the Children's Internet Protection Act, and other applicable laws.

Definitions:

Electronic Devices: Electronic media, communication devices, transmitters, receivers or players, including but not limited to mobile phones, phones with or without video or picture-taking capability, electronic music or video players, iPods, tablets, iPads, and electronic gaming devices.

School Day: The hours that make up the school day according to the school's schedule.

School-sponsored activities: Field trips, curricular and extracurricular activities, and extended school-sponsored trips or activities, including school-provided transportation to and from such activities.

Instructional time: The hours during the school day designated by the school for class instruction.

Policy

1. Electronic devices may only be possessed and used by students during the school day and during school-sponsored activities in accordance with the standards set forth herein.
2. IEA shall provide to its students and employees the opportunity to utilize electronic information resources.
3. In order to enhance learning, teach computer skills, and effectively utilize modern electronic information resources within the school, students and teachers shall have access to computers and the Internet. Other electronic information resources may include, but are not limited to, voice mail, email, and various network files or accounts.
4. In an effort to protect students and employees, the school will provide appropriate Internet filtering and monitoring for safety.
5. It must be understood that although IEA will make its best efforts to filter content, no system is 100% foolproof. Additionally, both students and employees will be issued usernames and passwords for accessing the school network.

6. All use of electronic information within the school must be consistent with the educational objectives of the school; electronic resources within the school are not intended for private, personal, or political use.
7. The Director may determine appropriateness of use of electronic information resources at his/her discretion.
8. No individual shall be allowed to use computers and/or the Internet without documentation indicating that the Electronic Information Resource Acceptable Use Policy has been carefully read, understood, and that the users agree to abide by the terms and conditions regarding proper behavior and use of all electronic information resources, including computers and the Internet.
9. Student use of electronic resources may be permitted provided the school receives annual documented parental permission and agreement to terms and conditions on behalf of their student.
10. Agreement to terms and conditions is legally binding. All user accounts are subject to IEA control and may be revoked for misuse. Violation of any part of this policy will result in disciplinary action according to defined school discipline policy, including the possibility of loss of privilege to use computers and other electronic information resources, suspension, expulsion, loss of employment, and appropriate legal action.
11. Neither students nor employees shall have any expectation of privacy in regard to utilization of electronic information resources provided by the school. This includes, but is not limited to files, disks, documents, emails, voicemails, or otherwise which have been created with, entered and stored in, downloaded to, or accessed by IEA electronic information resources.
12. IEA administration or Board of Trustees may monitor, log, and/or review any or all student or employee files and messages.

Employees' Responsibilities Regarding Students' Use of Electronic Resources

1. Employees who supervise students, control electronic resources, or otherwise have the ability to observe student use of IEA's electronic resources are responsible for educating students on appropriate use of the school's electronic resources.
2. Such employees shall make reasonable efforts to monitor such use to ensure that it is consistent with applicable rules.
3. Employees should make reasonable efforts to become familiar with the Internet and the use of the school's electronic resources to help ensure effective monitoring, instruction, and assistance.

User Responsibilities

1. Use of the school's electronic resources is a privilege intended to help employees fulfill their responsibilities and promote the school's mission. In order to maintain this privilege, users must agree to comply with this policy.
2. Users who are aware of any violation of this policy by any employee must report the violation to the Director.

3. Employees are responsible for any school electronic resources issued to them at all times and may be held responsible for any inappropriate use, regardless of the user.
4. Employees may use privately-owned electronic devices at school or at school-sponsored activities in accordance with rules and procedures established by the Director. Violation of this policy is grounds for discipline, up to and including termination. The school may also notify law enforcement as appropriate, and such actions may subject an employee to criminal penalties.

Acceptable Use of Electronic Information Resources

1. Students and employees of IEA are expected to abide by generally accepted rules of network etiquette. These rules include, but are not limited to being polite, kind, and using appropriate language.
2. Students will only use computers with the permission and supervision of teachers or staff. Students will respect and follow teacher/staff instructions.
3. Students must immediately report accidental access of unauthorized or unacceptable Internet sites to staff/teacher/administration as appropriate.
4. Students will ask for help when unable to properly use computers equipment or other electronic information resource.

Unacceptable Use of Electronic Information Resources

1. Students and employees will not intentionally harm or destroy computer equipment through abusive behavior.
2. Students are prohibited from revealing personal information, such as names, addresses, telephone numbers, passwords, credit card numbers, photographs, or social security numbers. Employees are advised against such. All individuals are prohibited against revealing the personal information of others or regarding confidential information regarding the school.
3. Students and employees will not communicate with language, graphics, or artwork that is considered to be vulgar, defamatory, threatening, or otherwise inappropriate.
4. Students and employees will not access, receive, or transmit material that is pornographic, obscene, sexually suggestive or explicit or other material related to weapons, controlled substances or alcohol, or incendiary devices.
5. Students and employees will not post or transmit content that that is considered "cyberbullying" or post or send content that contains threats or is hatefully or racially, ethnically or otherwise objectionable.
6. Students and employees will not intentionally harm or destroy school data, the network, or general network performance. This includes, but is not limited to: participating in or promoting any illegal or inappropriate activities that change the use of the computer hardware or software; corrupting, destroying, or manipulating system data; hacking or other activity, such as creating, loading, or transmitting viruses or worms, malware, password grabbers, spyware, etc. or other software which may compromise the network; erase, expire, or reset memory cache, web page links, or HTTP location history.
7. Students and employees will not use one's identity or misrepresent one's identity or the identity of another to gain unauthorized access to restricted information, systems, or programs; use the

school network to illegally access other systems; or to chat, email, or otherwise communicate electronically.

8. Students will not download, upload, install, or execute unapproved software without prior approval from teacher/staff/administration as appropriate.
9. Students and employees will not formally publish school related information on the Internet without proper approvals from administration or Board of Directors. This does not include teacher and/or staff websites that are created to communicate information on assignments and class schedules.
10. Students and employees will not violate copyright laws.
11. Students and employees will not copy system or curricular programs or files without proper approval.
12. Students and employees will not participate in unapproved and non-educational gaming.
13. Students and employees will not participate in unapproved interactive real time Internet activity, such as chat rooms.
14. Students and employees will not use the network for political purposes.
15. Students and employees will not participate in any activity that is illegal or does not conform to the rules, regulations, and policies of IEA.
16. Neither employees nor students may bring personal electronic equipment such as IPADS or laptops into the school except as allowed by express permission from the Director.
17. IEA does not make any warranties for the electronic information resources that are provided by the school. Any damages that may be suffered as a result of a student or employee using these resources are not the responsibility of the school. Damages may include, but are not limited to the loss of data as a result of delay, human error or omission, or non-delivery or service interruption caused by a network system. The school cannot be held responsible for the accuracy of information obtained through any of the electronic information resources which it provides.
18. All employees and students use the network system and the information obtained therein at their own risk.

Exceptions

1. The Director may give permission for a student to possess an electronic device for good cause, including medical reasons, if the device does not distract from the instructional or educational process and is not otherwise used inappropriately.
2. Parents may request that the Director allow a student to possess an electronic device on active mode at all times during the school day, with the exception of during tests and standardized assessments, for good cause, including medical needs or unusual family situations.
3. A student may possess an electronic device on active mode at all times during the regular school day, including during assessments, if such an accommodation is specified in a written Section 504 plan, an Individualized Education Plan, or in connection with other legitimate circumstances determined by the Director.
4. Electronic devices may be used in the event of an emergency during the limited period of the emergency in order to protect the safety of a student or school employee, visitor or volunteer.
5. Parents may make other individualized requests for exceptions to this policy to the Director.

Consequences for Violation

1. The Director will establish a clear disciplinary procedure for students or staff who are in violation of the this policy.
2. The Director, teachers, and other individuals designated by the Director may confiscate privately-owned electronic devices under this policy.
3. An individual other than a student that finds or confiscates a privately-owned electronic device may search the device for the purpose of determining the device's owner. Students may not search electronic devices.
4. Electronic devices that are used inappropriately may be subject to search by the Director if there is a reasonable suspicion that the device contains obscene or pornographic material or has been used to cheat or to threaten, embarrass, harass, or intimidate other students, teachers, volunteers, school guests, or school employees.
5. IEA is not responsible for loss, damage or theft of any privately-owned electronic devices. The school will make reasonable efforts to notify parents/guardians that the school has a student's electronic device in its possession. Parents/guardians who show identification may retrieve confiscated electronic devices during school hours or by appointment.
6. The School will retain un-retrieved electronic devices until the end of the school year, at which point the devices will be wiped of any data and donated according to procedures set forth by the Director.
7. The Director may impose additional disciplinary consequences for a student's violation of this policy, considering the nature of the violation and other disciplinary actions in which the student has been involved. Such disciplinary actions may include: loss of the privilege to possess or use electronic devices; disciplinary letter to the student's parent/guardian that is placed in the student's file; detention; In-School suspension; suspension; expulsion; loss of the privilege of participating in school-sponsored activities or of receiving honor recognition.
8. The School may contact law enforcement if school employees believe that a student has used an electronic device in connection with a violation of criminal law, and criminal penalties may arise from inappropriate use of electronic devices.

Notice of the Policy

IEA will give parents and students written notice of this policy annually. Written notice may be satisfied by posting the policy on the school's website, publishing the policy in a school handbook, sending the policy to the student's home, or any other reasonable means.

Creative and Innovative Uses for Electronic Devices Teachers and other School Staff

1. Employees are encouraged to use electronic devices creatively in order to effectively communicate with students and parents/guardians and to enhance instruction.
2. Creative uses might include notifying absent students of assignments, communicating with parents when students excel or if they are behind or absent, notifying students and parents of news articles or events that would enhance the learning experience, providing feedback to students on tests and assignments, parents notifying the School when students are absent or tardy.

Other Provisions

1. Picture taking or sound or video recording by students is prohibited in school unless authorized by a teacher or the Director.
2. Picture taking or sound or video recording by students is prohibited in private areas of the school such as locker rooms, counseling sessions, washrooms, and dressing areas.
3. Students bring electronic devices on school property at their own risk. The school is not responsible for lost, stolen or damaged electronic devices.
4. Students are responsible for their own electronic devices and may be subject to discipline if their device is misused by another.
5. Parents, guests and visitors to the school may use electronic devices at school and at school-sponsored activities only in accordance with rules established by the Director. Such individuals who use the school's electronic resources may not use such resources to access inappropriate material or information.

Date originally approved: March 13, 2018