



# Parent-Student Information Technology Acceptable Use Policy

It is the school's mission to empower students with access to technology, information, and digital resources while fostering safe, responsible, and ethical learning environments.

We are committed to upholding important security, privacy, and safety regulations, protocols, and standards. Users of school devices, networks, accounts, and other resources must adhere to school policies. Users must comply with local, state, and federal laws, regulations and ordinances. Failure to adhere to these policies or laws, regulations, or ordinances may result in discipline, legal action, or other remedies determined to be within the rights of the school. Relevant laws and regulations include (but are not limited to):

- The Family Educational Rights and Privacy Act (FERPA)
- Children's Internet Protection Act (CIPA)
- Individuals with Disabilities Education Act (IDEA)
- Children's Online Privacy Protection Act (COPPA)
- Health Insurance Portability and Accountability Act (HIPAA)

The school shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, but not be limited to, maintaining the student's online reputation and ensuring their personal safety by keeping their personal information private, the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying. Students are expected to follow safe practices when using school technology.

## **DEFINITIONS:**

1. School, Organization, and or We – The Cottonwood School and its subsidiaries, programs, and divisions
2. ITD - Inspire Charter Services Information Technology Department
3. You, Your, and or I - The parent/guardian, student, and signer of this Acceptable Use of Technology Policy
4. Resources - Devices, systems, services or networks owned, operated or issued by the school
5. User - Any person(s) accessing or utilizing school resources that is not a resource operator
6. AUP - Parent/Student Information Technology Acceptable Use Policy

## **USER RESPONSIBILITIES:**

Access to school technology, resources, and support is a privilege that offers a wealth of educational benefits. To maintain these privileges, all users must agree to learn about and comply with all information within this Acceptable Use Policy (AUP) document.

1. You agree to learn about and comply with all the information outlined in this AUP document.
2. Persons to whom items are assigned are expected to exercise reasonable care to protect those items against damage, loss and theft. "Reasonable care" is defined as:
  - a. Never leaving items unattended
  - b. Never lending, giving or releasing items to a person other than an authorized school employee, such as a Tech Team member
  - c. Never removing protective accessories or features (e.g. cases, bumpers)
  - d. Keeping items away from dangerous conditions (e.g. liquids, heat sources, unstable surfaces or items) and preventing actions which promote damage beyond normal wear and tear
  - e. Maintaining student supervision by parent/guardian during access and usage
3. You must immediately report damaged, lost or stolen items/resources. Items reported stolen or missing will require a police report.
4. Parents/guardians are expected to provide supervision and monitor device/Internet access and usage.
5. You are expected to make a reasonable effort to protect your passwords, information and data.
6. You must safeguard internal safety and security policies, such as authentication methods and password conventions.
7. You are obligated to notify ITD of continued access to resources beyond student departure (e.g. withdrawal, graduation, expulsion) in the event ITD has not contacted you to do so.
8. Items, devices and resources issued by the school are school property and must be returned or relinquished to the school upon request.

The Cottonwood School advises students:

- a. To never share passwords, personal data, or private photos online.
- b. To think about what they are doing carefully before posting and by emphasizing that comments cannot be retracted once they are posted.
- c. That personal information revealed on social media can be shared with anyone including parents, teachers, administrators, and potential employers. Students should never reveal information that would make them uncomfortable if the world had access to it.
- d. To consider how it would feel receiving such comments before making comments about others online.

#### **ACCEPTABLE USE OF ICS RESOURCES BY USERS:**

1. All school-issued technology and accounts are intended solely for educational use by the person authorized to use the technology and account.
2. When sharing or exposing personal information or data online, extreme caution should be exercised.

3. Any information or communication accessible via any school network should be assumed as private property.
4. The school reserves the right to verify whether specific uses of school technology or networks are consistent with this acceptable use policy.
5. The school is bound by certain licensing agreements. Users must comply with those agreements.
6. Educational and instructional use as related to the school only.

#### **UNACCEPTABLE USE OF SCHOOL RESOURCES:**

1. All commercial or for-profit usage is prohibited.
2. The access, use or transmission of objectionable material (e.g. materials that are obscene, bullying, profane, lewd, threatening, disrespectful, hateful, pornographic) is prohibited.
3. Violation of any local, state or federal laws, regulations or ordinances as well as School, board or administrative policies are prohibited. Example: Federal copyright laws ([Title 17, USC](#))
4. Any attempt to circumvent ICS security measures, content filters or access restricted resources is prohibited.
5. All malicious and nefarious activities are prohibited. Examples include (1) unauthorized trespassing or infiltration of a network or device, (2) the intentional distribution of malware, (3) any attempt to deny a remote service. Malicious actors may also be in violation of *California's unauthorized computer access law, Penal Code 502(c) PC*.
6. The intentional collection, mining or uncovering of personal information, files, passwords belonging to a user other than yourself is prohibited.
7. Publicly advertising internal authentication methods and/or password conventions.
8. Impersonation of any user other than yourself is prohibited.
9. Unauthorized falsification or modification of any school records is prohibited.
10. The collection or transmission of personal information (e.g. home address, phone number, personal email) which may be useful to identify an individual without written consent is prohibited.
11. Political lobbying or advertising is prohibited.
12. Unauthorized maintenance, service, repairs, or upgrades are prohibited. School-owned or operated resources must be maintained by ITD or authorized third parties.

#### **EXPECTATION OF PRIVACY:**

For email, networks, systems and other resources owned or operated by the school, users should have no expectation of privacy. The school reserves the right to manage and monitor all aspects of its own resources. The following are examples of actions which may be performed for reasons deemed legitimate by the school:

1. Obtain emails, messages and their attachments transmitted to or through school-owned or operated email systems
2. Monitor an individual's use of school-owned resources
3. Locate or track the location of a school-owned resource
4. Confiscate, search, disable or wipe any school-owned device, item or their contents/data

Personal devices are private. The ITD does not and will not access personal devices.

### **CYBERBULLYING:**

Cyberbullying is the use of technology resources to willfully harm either a person or persons through electronic systems (e.g. texts, photos, videos, messages, and social media). Cyberbullying is prohibited. Examples of this behavior include but are not limited to:

1. Transmitting false, cruel, hateful or embarrassing information or media targeting others
2. Creating posts or websites that have stories, cartoons, pictures, or jokes ridiculing others
3. Unauthorized access to any resource (e.g. social media, email) for purposes of downloading or transmitting vicious or embarrassing materials
4. Engaging someone in electronic communication, tricking that person into revealing sensitive personal information and transmitting that information or media to others
5. Posting a student picture without their permission
6. The use of derogatory comments, including those regarding race, age, gender, sexual orientation, religion, ability, political persuasion, body type, physical, or mental health.

### **STUDENT DEPARTURE:**

1. Upon student departure (e.g. withdrawal, graduation, or expulsion) from the school, all issued items must be returned within 30 days. Contact the ITD for a schedule of mobile return locations or request prepaid return labels.
2. For information regarding technology returns, please review our *ICS Tech Center and Issued Technology Agreement* or contact ITD.

### **CONTACT INFORMATION:**

Inspire Charter Services Information Technology Department

Phone: (626) 433-8094

- Email: [tech-help@inspireschools.org](mailto:tech-help@inspireschools.org)
- Submit a Request: [inspireschools.teamwork.com/support](https://inspireschools.teamwork.com/support)

### **DISCLAIMER & ACKNOWLEDGEMENTS:**

1. The school reserves the right to modify its policies at any time.
2. All items, devices, and resources issued by the school are school property. School property must be returned or relinquished to the school upon request or departure from the school.
3. The school reserves the right to issue penalties (e.g. denial of access to resources, withholding of transcripts) or seek legal remedies in response to non-compliance.
4. The school will not be held liable for the information or data retrieved, stored, or transmitted by means of the school-owned or operated resources, devices, networks, or systems.

5. Users should not have an expectation of privacy in the use of school resources, email, systems, or networks.
6. Illegal activities performed using school devices, networks, and systems may be reported to the proper authorities when discovered.
7. The school will not be held responsible for losses or damages suffered by any user, including loss of data, interruption of service, delays, or non-deliveries.
8. School issued property reported as lost, missing or stolen may be remotely tracked, located and/or disabled at the discretion of the school.
9. The school may confiscate and search any school technology.
10. The school is not in any way an Internet Service Provider.
11. The school shall ensure that all school computers with Internet access have a technology protection measure that blocks or filters Internet access to websites that have no educational purpose and/or contain visual depictions that are obscene, constitute child pornography, or that are harmful to minors. While the school is able exercise reasonable control over content created and purchased by the school, it has limited control over content accessed via the internet and no filtering system is 100% effective. Neither the school nor its staff shall be responsible for the failure of any technology protection measures, violations of copyright restrictions, or user mistakes, misuse or negligence.

#### **USER AGREEMENT:**

I have read, understand, and will abide by the above PARENT/STUDENT ACCEPTABLE USE OF TECHNOLOGY POLICY while using any school technology and other electronic resources issued, owned or operated by the school. I further understand that any violation of the policies above are considered unethical and in some cases may constitute a criminal offense. Should I violate any of the policies outlined in this agreement, I understand my access to any school resource may be limited or revoked, and disciplinary and or legal action may be taken.

**BY SIGNING THE PARENT/STUDENT HANDBOOK SIGNATURE OF RECEIPT AND ACKNOWLEDGEMENT SECTION, PARENT(S)/GUARDIAN(S) & STUDENT AGREE THEY HAVE READ, UNDERSTOOD, AND ACCEPT THE TERMS WITHIN THIS PARENT/STUDENT ACCEPTABLE USE OF TECHNOLOGY POLICY.**