



Parent Student Technology Use Policy

Cabrillo Point Academy is committed to providing our students with access to technology, information, and digital resources while fostering safe, responsible, and ethical learning environments. The Charter School is committed to upholding important security, privacy, and safety regulations, protocols, and standards. Users of the Charter School's devices, networks, accounts, and other resources must adhere to the Charter School's policies. Users are also expected to fully comply with local, state, and federal regulations. Failure to adhere to these policies or regulations may result in discipline, legal action, or other remedies determined to be within the rights of the Charter School. Relevant 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 purpose of the Cabrillo Point Academy Governing Board approving this Parent-Student Information Technology Acceptable Use Policy is to accomplish the following:

1. Define Technology Use Terms and Phrases
2. Identify the User Responsibility
3. Outline Acceptable Use of Resources
4. Outline Unacceptable Use of Resources
5. Outline the Expectation of Privacy
6. Define Cyberbullying
7. Outline Stolen Technology Procedures
8. Outline the Student Departure Procedures
9. Identify the Disclaimers and Acknowledgements
10. Establish the User Agreement

1. Definitions:

- **School or Organization or We** – the Charter School and its subsidiaries, programs, and divisions
- **ITD** – Cabrillo Point Academy's Information Technology Department
- **You or Your or I** - the parent/guardian, student, and signer of this Acceptable Use of Technology Policy

- **Resources** - devices, systems, services or networks owned, operated or issued by the Charter School.
- **User** - any person(s) accessing or utilizing the Charter School's resources that is not a resource operator
- **AUP** – Parent-Student Information Technology Acceptable Use Policy

2. **User Responsibilities:** Access to the Charter School's technology, resources, and support is a privilege which offers a wealth of educational benefits. To maintain these privileges, all users must agree to, learn about, and comply with all information within this AUP document.

- You agree to, learn about and comply with all information outlined in this AUP document
- 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:
 - Never leaving items unattended
 - Never lending, giving or releasing items to a person other than an employee of the ITD or Charter School
 - Never removing protective accessories or features (e.g. cases, bumpers)
 - 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
- You must immediately report damaged, lost, or stolen items/resources. Items reported stolen or missing will require a police report.
- Parents/guardians are expected to provide supervision and monitor device/Internet access and usage.
- You are expected to make a reasonable effort to protect your passwords, information and data.
- You are obligated to notify the ITD of continued access to resources beyond student departure (e.g. withdrawal, graduation, expulsion) in the event the ITD has not contacted you to do so.
- **Items, devices and resources issued by the Charter School are School property and must be returned or relinquished to the Charter School upon request.**

3. **Acceptable Use of Resources:**

- All of the Charter School-issued accounts are intended solely for use by the person authorized to use the account.
- When sharing or exposing personal information or data online, extreme caution should be exercised.

- Any information or communication accessible via any of the Charter School networks should be assumed private property.
- The Charter Schools reserves the right to verify whether specific uses of the Charter School technology or networks are consistent with this acceptable use policy.
- The Charter School is bound by certain licensing agreements. Users are expected to comply with those agreements.
- Educational and instructional use as related to the Charter School only

4. Unacceptable Use of Resources:

- All commercial or personal for-profit usage is prohibited.
- The access, use or transmission of objectionable material (e.g. materials that are obscene, bullying, profane, lewd, threatening, disrespectful, hateful, pornographic) is prohibited.
- Violation of any local, state, or federal laws as well as School, board or administrative policies are prohibited. (e.g. Federal copyright laws - [Title 17](#), USC)
- Any attempt to circumvent the Charter School's security measures, content filters or access restricted resources is prohibited.
 - 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*.
- The intentional collection, mining, or uncovering of personal information, files, passwords belonging to a user other than yourself is prohibited.
- Impersonation of any user other than yourself is prohibited.
- Unauthorized falsification or modification of any school records is prohibited.
- The collection or transmission of personal information (e.g. home address, phone number, personal email) which may be useable to identify an individual without written consent is prohibited.
- Political lobbying or advertising is prohibited.
- Unauthorized maintenance, service, repairs, or upgrades are prohibited. The Charter School's owned or operated resources must be maintained by the ITD or authorized third parties.

5. Expectation of Privacy: For email, networks, systems, and other resources owned or operated by the Charter School, users should have no expectation of privacy. The Charter 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 Charter School:

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

Personal devices are private. The Charter School must obtain permission to access personal devices.

6. 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, social media). Examples of this behavior include, but are not limited to:

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

7. Stolen Technology: All devices issued by the Charter School are encrypted via industry standard technologies, including Bitlocker, FileVault, iOS Data Protection. Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. Data on a lost or stolen computer is vulnerable to unauthorized access, either by running a software-attack tool against it or by transferring the computer's hard disk to a different computer. Encryption helps mitigate unauthorized data access by enhancing file and system protections.

8. Student Departure: Upon student departure (e.g. withdrawal, graduation, or expulsion) from the Charter School, all issued items must be returned within 30 days. Prepaid return labels and pick up services may be provided at no cost as long as the device is being returned from a location within the state of California. Please review the Charter School's *Tech Centre and Issued Technology Agreement* for complete details regarding returns.

If all attempts to collect a device are unsuccessful, the matter will be handed over to local law enforcement and pursued on behalf of the Charter School. Any missing technology will also be added to the student's records.

For information regarding technology returns, please review the Charter School's *Parent Student Handbook* or contact ITD.

9. Disclaimer & Acknowledgements:

- The Charter School reserves the right to modify its policies and rules at any time.
- **ALL DEVICES, ITEMS AND SOFTWARE ISSUED BY THE CHARTER SCHOOL ARE SCHOOL PROPERTY. YOU ARE REQUIRED TO RETURN ALL ITEMS ISSUED TO YOU UPON REQUEST BY OR DEPARTURE FROM THE CHARTER SCHOOL.** We reserve the right to issue penalties (e.g. denial of access to resources, withholding of transcripts) or seek legal remedies in response to non-compliance.
- Access to the Charter School's technology, resources and support is a privilege, not a right. These privileges are offered at the discretion of the Charter School.
- The Charter School will not be held liable for the information or data retrieved, stored, or transmitted by means of the Charter School owned or operated resources, devices, networks, or systems
- Users should not have an expectation of privacy in the use of the Charter School's resources, email, systems, networks
- Illegal activities performed using the Charter School's devices, networks, and systems will be reported to the proper authorities when discovered
- The Charter 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
- The Charter School's issued property reported as lost, missing, or stolen may be remotely tracked, located and/or disabled at the discretion of the Charter School.
- The Charter School may confiscate and search any of the Charter School's resource for any reason deemed reasonable by the Charter School including in response to violation of school policies or government regulations
- The Charter School is not in any way an Internet Service Provider

10. User Agreement Statement: I have read, understand, and will abide by the PARENT-STUDENT INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY when using any of the Charter School's technology and other electronic resources issued, owned or operated by the Charter 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 of the Charter School's technology resources may be limited, revoked or returned and disciplinary and or legal action may be taken.

STUDENT NAME (please print)

PARENT/GUARDIAN SIGNATURE

Date

