Information Technology Department

Policies and Procedures

Created by Tina Overstreet 1/10/18

Overview

This document serves as a rulebook and roadmap for successfully and properly utilizing the technology resources at Cabrillo Point Academy (CPA). You, the employee, should always take careful consideration to verify that all actions fall within the authorized parameters for access, utilization, distribution, and modification of CPA's technology resources set forth within this document.

Any misuse, misappropriation, negligence, or deliberate disobedience concerning these policies and procedures will not be tolerated. It is up to each individual employee and affiliate of CPA to familiarize him/herself with the policies and procedures set forth prior to signing the agreement form associated to these policies and procedures.

It is the purpose of the CPA Information Technology Department (ITD) to provide these policies and procedures in order to address potential situations and to provide steps to take during these situations. However, not all situations can ever be addressed so it is up to each individual employee and affiliate to use these policies and procedures as an example of what action to take.

The CPA Information Technology Department does encourage all CPA employees and associates to err on the side of caution should a difficult situation present itself. Please contact the ITD if you require further assistance or have any questions.

Contents

Acceptable Use of Information Technology Resources

Overview

Cabrillo Point Academy Acceptable Use of Information Technology Resources policy (AUP) provides for access to information technology (IT) resources and communications networks within a culture of openness, trust, and integrity. In addition, Cabrillo Point Academy (CPA) is committed to protecting itself and its students, faculty, and staff from unethical, illegal, or damaging actions by individuals using these systems.

CPA is committed to upholding important security, privacy, and safety regulations, protocols, and standards. Users of CPA devices, networks, accounts, and other resources must adhere to CPA policies. Users are 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 CPA. 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)

DEFINITIONS:

1. **CPA** or **School** or **Organization** or **We** - Cabrillo Point Academy and its subsidiaries, programs, and divisions
2. **ITD** - Cabrillo Point Academy Information Technology Department
3. **You** or **Your** or **I** - employee of CPA and or signer of this Acceptable Use of Technology Policy
4. **Resources** - devices, systems, services or networks owned, operated or issued by CPA
5. **User** - any person(s) accessing or utilizing CPA resources that is not a resource operator
6. **AUP** - INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

Purpose

The purpose of this policy is to outline the ethical and acceptable use of information systems at Cabrillo Point Academy. These rules are in place to protect students, faculty, and staff; i.e., to ensure that members of the Cabrillo Point Academy community have access to reliable, current IT resources that are safe from unauthorized or malicious use.

Insecure practices and malicious acts expose Cabrillo Point Academy and individual students, faculty, and staff to risks including virus attacks, compromise of network systems and services, and loss of data or confidential information. Security breaches could result in legal action for individuals or the school. In addition, security breaches damage the schools reputation and could result in loss of services. Other misuses, such as excessive use by an individual, can substantially diminish resources available for other users.

Scope

This outline is an integral part of IT security policies and applies to faculty, staff, and students as well as any other individuals or entities who use information and IT resources at Cabrillo Point Academy. This policy applies to all IT resources owned or leased by Cabrillo Point Academy and to any privately owned equipment connected to the schools network and includes, but is not limited to, computer equipment, software, operating systems, storage media, and the Internet.

Securing and protecting these significant and costly resources from misuse or malicious activity is the responsibility of those who manage systems as well as those who use them. Effective security is a team effort involving the participation and support of every member of the CPA community who accesses and uses IT resources. Therefore, every user of Cabrillo Point Academy IT resources is required to know the policies and to conduct their activities within the scope of the AUP, and the **Policies, Standards, and Guidelines for IT Security** (see Resources below). Failure to comply with this policy may result in disciplinary action.

Acceptable Use Policy

Unless otherwise specified in this policy or other CPA policies, use of school information technology resources is restricted to purposes related to the school's mission. Eligible individuals are provided access in order to support their job duties as employees, official business with the school, and other school-sanctioned activities. Individuals may not share with or transfer to others their user accounts including passwords, or other access codes that allow them to gain access to CPA Information Technology resources. The protection and privacy of our students and staff information is the highest priority and each staff member is expected to enact safe privacy measures according to current state and federal laws. Violation of this could result in disciplinary action or termination.

Other administrative units have considerable latitude in developing complementary technology use policies and procedures, as long as they are consistent with this policy and any other applicable technology use policies of the school. For more information about developing technology policies and procedures, please contact the Information Technology Department (ITD).

Incidental personal use of information technology resources must adhere to all applicable school policies. Under no circumstances may incidental personal use involve violations of the law, interfere with the fulfillment of an employee's school responsibilities, or adversely impact or conflict with activities supporting the mission of the school.

Users are prohibited from engaging in any activity that is illegal under local, state, federal, or international law or in violation of school policy. The categories and lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of acceptable/unacceptable use.

IT Resources include but are not limited to:

- Computers
    - Desktop Computers (if applicable), Mobile Devices, Laptops, etc.
- Network Equipment
    - Routers, Network and Communication Cabling, VoIP Phones, HotSpots, Cradlepoints, etc.
- Audio/Video Equipment
    - Projectors, Cameras, Copiers/Printers, Fax Machines, Security Cameras, TVs, etc
- Software
    - Operating Systems, Application Software

- Resources
    - Group Drive File Storage, Website File Storage, Email Accounts, Social Networking Accounts, etc.

The following activities provide a general roadmap to use CPA's technology resources in an acceptable manner:

1. You agree to, learn about and comply with all 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:
    - Never leaving items unattended
    - Never lending, giving or releasing items to a person other than an employee of the ITD
    - 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
3. You must immediately report damaged, lost or stolen items/resources. Items reported stolen or missing will require a police report.
4. You are expected to make a reasonable effort to protect your passwords, private information and data.
5. Employees must use extreme caution when opening email attachments received from unknown senders
6. All users should lock the workstation when unattended
7. Upon termination of employment, all technology must be returned immediately on your final day. If any attempt to collect the items have failed, all matters will be handled by local law enforcement. ***For more information, please contact the CPA Information Technology Department.***

Unacceptable Use

Excessive Non-Priority Use of Computing Resources

Priority for the use of IT resources is given to activities related to the school's missions of teaching, learning, research, and outreach. CPA computer and resources are limited in capacity and are in high demand. To conserve IT resource capacity for all users, individuals should exercise restraint when utilizing computing and system resources. Individual users may be required to stop non-priority use of IT resources, such as recreational activities and non-academic, non-business services.

Unacceptable system and network activities include:

Engaging in or effecting security breaches or malicious use of system communication including, but not limited to:

1. Obtaining configuration information about a network or system for which the user does not have administrative responsibility.
2.

Unauthorized Use of CPA Property

Users are responsible for complying with all applicable laws and regulations regarding the dissemination and protection of data and information that is confidential, particularly with regards to the Family Educational Rights and Privacy Act of 1974 (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), Children's Internet Protection Act (CIPA) , and any other applicable state and federal legislation dealing with information privacy. Violations include, but are not limited to:

1. Except as provided by fair use principles, engaging in unauthorized copying, distribution, display, or publication of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources; copyrighted music or video; and the installation of any copyrighted software without an appropriate license.
2. Using, displaying, or publishing licensed trademarks, including Cabrillo Point Academy's trademarks, without license or authorization or using them in a manner inconsistent with any terms of authorization.
3. Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws.

Inappropriate or malicious use of IT systems includes:

1. Setting up file sharing in which protected intellectual property is illegally shared.
2. Intentionally introducing malicious programs into the system or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
3. Inappropriate use or sharing of school-authorized IT privileges or resources.
4. Changing another user's password, access, or authorizations.
5. Using an Cabrillo Point Academy computing asset to actively engage in displaying, or transmitting material that is in violation of sexual harassment policy or laws, hostile workplace laws, or other illegal activity.
6. Using an Cabrillo Point Academy computing asset for any private purpose or for personal gain.

Misuse of Electronic Communications

Electronic communications are essential in carrying out the activities of the school and for individual communication among staff, faculty, students, and their correspondents. Individuals are required to know and comply with the school's policy on **Mass Email and Effective Electronic Communication** (see Resources below).

Key **prohibitions** include:

1. Sending unsolicited messages, including "junk mail" or other advertising material, to individuals who did not specifically request such material, except as approved under the policy on Mass Email and Effective Electronic Communication.
2. Engaging in harassment via electronic communications whether through language, frequency, or size of messages.
3. Masquerading as someone else by using their email or internet address or electronic signature.
4. Soliciting email from any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters" or solicitations for business schemes.
6. Using email originating from Cabrillo Point Academy's provided accounts for commercial use or personal gain.

Enforcement

The Acceptable Use of Information Technology Resources policy is enforced through the following mechanisms. Any user who discovers unauthorized access attempts or other improper usage of Cabrillo Point Academy technology should report the infraction to the Information Technology Department, or other appropriate administrators. Management personnel are responsible for ensuring employees are aware of and trained in the provisions of this policy.

Interim Measures

The school may temporarily disable service to an individual or a computing device, when an apparent misuse of school computing facilities or systems has occurred, and the misuse:

1. Is a violation of criminal law
2. Has the potential to cause significant damage to or interference with school facilities or services
3. May cause significant damage to another person
4. May result in liability to the school

An attempt will be made to contact the person responsible for the account or equipment prior to disabling service unless law enforcement authorities forbid it or Information Technology staff determine that immediate action is necessary to preserve the integrity of the school network. In any case, the user shall be informed as soon as possible so that they may present reasons in writing why their use is not a violation or that they have authorization for the use.

Suspension of Services and Other Action

Users may be issued warnings, may be required to agree to conditions of continued service, or may have their privileges suspended or denied if:

- After hearing the user's explanation of the alleged violation, an IT administrator has made a determination that the user has engaged in a violation of this code, or
- An employee disciplinary body has determined that the user has engaged in a violation of the code.

Password Policies and Procedures

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Cabrillo Point Academy's entire network. As such, all employees (including contractors and vendors with access to Cabrillo Point Academy network) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any CPA facility, has access to the CPA database, or stores any non-public information pertaining to CPA. **The Password Protection Standards** below also apply to the use of family accounts and should always be handled with care and common sense.

Standards

A. General Password Construction Guidelines

Passwords are used for various purposes at Cabrillo Point Academy. Some of the more common uses include: user-level accounts, web accounts, email accounts, screensaver protection, voicemail password, and local router logins. Everyone should be aware of how to select strong passwords.

1. Poor, unacceptable passwords have the following characteristCPA:

   ✗ The password contains fewer than ten characters

   ✗ The password is a word found in a dictionary (English or foreign)

   ✗ The password is a common usage word such as:

   - Names of family, pets, friends, coworkers, fantasy characters, etc.
   - Computer terms and names, commands, sites, companies, hardware, software
   - Acronyms for the agency or city.
   - Birthdays and other personal information such as addresses and phone numbers
   - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
   - Any of the above spelled backwards
   - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

2. Strong (acceptable) passwords have the following characteristCPA:

   ✓ Contain both upper and lowercase characters (e.g., a-z, AZ)

- ✓ Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*()_+|~-=\` {}[]:";í<>?,./)
- ✓ Are at least ten alphanumeric characters long
- ✓ Are not based on personal information, names of family, etc.
- ✓ Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: ?This May Be One Way To Remember? and the password could be: ?TmB1w2R!? or ?Tmb1W> r~? or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for Cabrillo Point Academy accounts as for other non Cabrillo Point Academy access (e.g., personal ISP account, personal email accounts, etc.).

Here is a list of "don'ts":

- ✗ Don't reveal a password over the phone to ANYONE.
- ✗ Don't reveal a password in an e-mail message.
- ✗ Don't talk about a password in front of others.
- ✗ Don't hint at the format of a password (e.g., "my family name").
- ✗ Don't reveal a password on questionnaires or security forms.
- ✗ Don't share a password with family members.
- ✗ Don't reveal a password to co-workers while on vacation.
- ✗ Don't write a password in an obvious place that is accessible to others.

Do not share passwords with anyone, including passwords associated to ANY student accounts. All passwords are to be treated as sensitive, confidential CPA information. If a password is requested by a parent or student, simply forward them an associated link to reset their password. We are not responsible for creating passwords for end-users.

Disabling Login Password

Internet and Email Policy

Overview

Voice mail, email, and internet usage assigned to an employee's computer or telephone extensions are solely for the purpose of conducting Cabrillo Point Academy business. Most job responsibilities at CPA require access to the internet and the use of software. Only people appropriately authorized, for CPA purposes, may use the internet to access and download additional software.

This authorization is generally exclusive to decisions that the ITD makes in conjunction with the need to perform your job duties and any request made from managers or directors.

Software Access

Software needed, in addition to the Google products, must be authorized by your manager and downloaded by the ITD staff. If you need access to software or websites, please talk with your manager and consult with the ITD to explain what you expect to receive from the product.
All reasonable requests that are not considered a security risk will be considered for you and other employees.

Internet Usage

Internet use on Cabrillo Point Academy time, using CPA-owned devices that are connected to the schools network, is authorized to conduct school business only. Internet use brings the possibility of breaches of the security of confidential information. Internet use also creates the possibility of contamination to our system via viruses or spyware. Spyware allows unauthorized people, outside of CPA, potential access to CPA passwords and other confidential information.

Removing such programs from the network requires IT staff to invest time and attention that is better devoted to making technological progress. For this reason, and to assure the use of work time appropriately for work, we ask staff members to limit internet use.

Additionally, under no circumstances may CPA owned computers or other electronic equipment, including devices owned by the employee, be used on CPA time at work to obtain, view, or reach any pornographic, or otherwise immoral, unethical, or non-business-related internet sites. Doing so can lead to disciplinary action up to and including termination of employment.

Social Media

We understand that part of what you do in social media is outreach that recruits new employees and enhances our school brand. Many employees have social media responsibilities in their job description including the social media marketers, tech support, and recruiters.

We strongly encourage you to limit the use of social media to work-related content and outreach during work hours. Additionally, you are prohibited from sharing any confidential or protected information that belongs to or is about CPA. You are strongly encouraged not to share disparaging information that places CPA or coworkers in an unfavorable light.

The school's reputation and brand should be protected by all employees. The lives and actions of your coworkers should never be shared online. Please note the confidentiality of all students should be kept at all times.

There are great advantages to the use of social media and disadvantages; those include but are not limited to:

- The overuse and availability of bandwidth to all employees
- Malware and network hijack
- Decrease in work productivity
-

In social media participation from work devices or during working hours, social media content that discriminates against any protected classification including age, race, color, religion, gender, national origin, disability, or genetic information is prohibited. It is CPA's policy to also recognize sexual preference as qualifying for discrimination protection. Any employee, who participates in social media, who violates this policy, will be dealt with according to the CPA harassment policy.

Email Usage at CPA

Email is to be used for CPA business only. CPA confidential information must not be shared outside of the school, without authorization, at any time. You are also not to conduct personal business using CPA computers or emails.
Please keep this in mind, also, as you consider forwarding non-business emails to associates, family or friends. Non-business related emails waste time and attention.

Viewing pornography, or sending pornographic jokes or stories via email, is considered sexual harassment and will be addressed according to our sexual harassment policy. Immediate termination is the most frequent disciplinary action. ***Please keep all email messaging appropriate and professional when communicating with co-workers and families***.

Mass Email and Effective Electronic Communication

All electronic communications are expected to comply with federal and state laws, as well as school regulations and policies.

Permission to mail to a group is not needed if you are the authorized sender for the group or are conducting normal school business. Before using a list that someone else owns, you must ask permission to use it. Access to a list does not necessarily imply permission to use.

If you wish to do a large mailing to a group you must get approval from a manager.

Mass Email Checklist

Before you send a large-scale mailing, you should ensure you can answer "yes" to each of the following questions:

- Is email the best or appropriate method to get information to your intended audience?
- Is the message relevant to the school's core missions?
- Have you included in the content of the message:
    - A "From:" address where replies will be received
    - The office, organization, or individual sending the message
    - Contact information if there is a question, comment, or complaint about the message
    - An explanation of why the recipient is receiving the message
    - Required information presented
    - Pointers to our website or elsewhere for additional information
- Do you have authorization to use the mailing list?
- If your mailing will go to more than 1,000 recipients, do you have approval to do a mass mailing to your intended audience?

Please note that Gmail has strict sending limits when sending bulk mail. Contact your ITD for more information about these limitations.

Employee Email

Keep in mind that CPA owns any communication sent via email or that is stored on CPA equipment. Management and other authorized staff have the right to access any material in your email or on your computer at any time. Please do not consider your electronic communication, storage or access to be private if it is created or stored on work devices.

Emails That Discriminate

Any email content that discriminates against any protected classification including age, race, color, religion, sex, national origin, disability, or genetic information is prohibited. Any employee who sends an email that violates this policy will be dealt with according to the harassment policy. Threatening or offensive emails are prohibited at Cabrillo Point Academy.

Phishing Emails are SCAMS

Phishing is a type of attack carried out in order to steal usernames, passwords, credit card information, Social Security Numbers, and other sensitive data by masquerading as a trustworthy entity. Phishing is most often seen in the form of malicious emails pretending to be from credible sources. We ask that you do your due diligence to ensure the email is safe and coming from a reputable source. No institution, bank or otherwise, will ever ask for private information via email. It may not always be easy to tell whether an email or website is legitimate, but there are many ways to help:

- In the body of an email, you might see questions asking you to “verify” or “update your account” or “failure to update your records will result in account suspension.” It is usually safe to assume that no credible organization will ever ask you to re-enter it, so do not fall for this trap.

- Any email that asks for your personal or sensitive information should be seriously scoured and not trusted. Even if the email has official logos or text or even links to a legitimate website, it could easily be fraudulent. **Never give out your personal information.**
- Do not respond to warning messages claiming you have a virus or have been hacked
- Check the email address - ask yourself: “does it come from someone you know, are you expecting an email from that source, does it match or legitimize the organization it is tied to”
- Hover over the link, don’t click it. (Look at the bottom left corner of your monitor to reveal the URL)
- Never forward emails that aren’t work related. Emails with advertisements and/or suggestions to forward to someone else are usually a trap and could introduce viruses to all users

If you suspect any malicious activity, please contact the ITD immediately.

Staff Equipment Policy

Overview (Pending review)
CPA attempts to provide sufficient equipment to allow employees to manage their duties efficiently. Equipment is usually assigned and issued immediately upon hire for all new employees. All new devices require a minimum of 1-3 weeks for delivery and configuration, therefore management is advised to notify the ITD immediately upon hiring a new staff member.

This document provides Cabrillo Point Academy (CPA) policy requirements to assure appropriate and equitable issuance to faculty and staff of basic computer technology equipment. This policy guides faculty and staff concerning utilization and support of computer and peripheral needs and basic network access, as well as personal responsibilities of the employee and supervisor.

New Hire Details - When welcoming a new employee on board, it is required that management send the Information Technology Department (ITD) with the following details:

- The employees full name
- Supervisor or manager
- Address (only necessary for staff that work off-site)

- Title of position (please include department)
- Start Date
- Equipment needed (only if they require additional equipment)
- E-mail address you'd like to assign

Standard devices and equipment offered to all employees include, but are not limited to:

1. HP Elitebook 15.6 - a fast 15.6 laptop which usually includes touchscreen
2. Brother MFC-J985DW - wireless printer/scanner/fax machine
3. 1 or 2 displays, keyboard, mouse, and dock (offered to office staff ONLY)
4. Office phone (offered to office staff ONLY)

Please note, all request should have prior approval from a manager and be made by submitting a ticket via helpdesk: tech-stafforders@inspireschools.org. For detailed instructions on placing orders, please see the Technology Ordering Policy. **All devices are subject to change without notice.*

CPA Owned Equipment

Any device or computer including, but not limited to, desk phones, smartphones, tablets, laptops, desktop computers, and iPads that CPA provides for your use, should only be used for school business. Keep in mind that CPA owns the devices and the information in these devices. If you leave the school for any reason, CPA will require that you return the equipment on your last day of work.

You may use personal electronic devices that are **not** connected to the CPA network to access any appropriate internet site during breaks and lunch.

Staff Use of Equipment/Materials

The equipment at CPA is for the benefit of staff and student instruction. The care of all devices is the responsibility of each staff member. If at any time there is an issue with a computing device, please contact the ITD for more instructions. Employees may use equipment for non-instructional and not-for-profit use, subject to the following conditions:

1. If school owned equipment is to be removed from it's assigned location, prior approval must be given by management.
2. The employee is responsible for the cost of repairing any damaged and lost item while in the employees possession. Please immediately contact your manager and the ITD with any reports of loss or damage.
3. In no circumstance may equipment be used for private or personal business ventures, only school business.
4. Upon departure from CPA all staff are asked to return their items on the last day. If all attempts to collect a device is unsuccessful, the matter will be handed over to local law enforcement.

Pre-Purchase Review Requirements

To ensure sound purchasing, supportability, appropriate pricing and assure security of the school's resources, the purchase of all CPA technology equipment and software, regardless of the source of funds, shall be approved by the ITD prior to purchase. If there is an item that is "out of the ordinary," prior approval from a manager must be given.

*Please note, the school has a large list of vendors or suppliers that support our organizational needs, therefore the lead time for items purchased through these vendors may vary.

Software

The school considers software piracy a serious offense. CPA abides by legal requirements for licensing software. Only licensed software will be installed on school owned equipment. The Information Technology Department will be responsible for purchasing licenses for applications that are appropriate and included as part of the standard configuration.

We strongly discourage the purchase of licensing for individual and small groups, unless this is apart of your job duties. The Information Technology staff will not be liable for licensing issues when software isn't in accordance with use for school related business and didn't have prior authorization of purchase. Licensing purchases that have not been approved by management may be classified as a personal purchase and may not be reimbursed, this also applies to hardware. In order to provide a software recovery mechanism for individuals and small groups, each department is required to maintain the licensing documentation and original media of software purchases.

Software purchased through the school shall not be installed on personally owned computers without approval.

Security

Providing technology to all staff and students opens up to a certain amount of threats and malicious activity. It is the responsibility of CPA to insure that we're compliant with local, state and federal laws prohibiting the unfair use and distribution of confidential information. Every member of the CPA community is responsible for protecting the security of school information and information systems by adhering to the objectives and requirements stated within all CPA policies. If multiple policy statements or security standards are relevant for a specific situation, the most restrictive security standards will apply.

Failure to comply with established policies and practices may result in loss of computing privileges and/or disciplinary action.

Replacement Cycle and Redeployment

Where possible every opportunity to reuse or find new uses for retired computers will be explored before equipment is retired. Redeployment and/or replacement is at the discretion of the department manager and ITD. All employees are asked to contact their manager prior to requesting a replacement device from the Information Technology Department.

Disposal of Equipment

The CPA ITD is solely responsible for the sale and disposal of all computing equipment and peripheral storage devices when they are deemed surplus. No department or individual may arrange for the sale or collect money for school owned equipment, computers, furniture, or other supplies/materials purchased

with school funds, regardless of the source of funds. Departmental personnel may not gift or donate equipment, computers, cell phones, furniture, or other items without CPA approval. School owned equipment, computers, laptops, tablets, cell phones, furniture, and materials may not be removed from the school, converted to personal property, or retained for personal use when deemed excess.

Equipment Configuration Policy

Overview

This policy has been established to create a standard configuration for all technology resources at CPA. Because of the variances between the types, makes, models, configurations, builds, versions, and brands of technology resources available, it is necessary to standardize all technology resources to make service and maintenance easier and also to help keep costs down.

Policy

All employees shall order and utilize equipment that is serviceable and recommended by the CPA IT Department. Since equipment availability changes over time, especially when referring to technology, a comprehensive list indicating appropriate hardware would be almost impossible to create. Because of this, any individual or department wishing to purchase technology equipment should first consult a CPA ITD staff member for current specifications for any given piece of equipment.

This applies to any and all technology equipment including, but not limited to:

- Computers (Servers, Desktop, Laptop, Tablets and Mobile Devices, etc.)
- HDTVs, Printers, scanners, copiers, fax machines, or all-in-one devices
- Projectors, and screens
- VoIP phones
- Digital cameras and camcorders
- Software (Application, Operating System, Network-Based, etc.)

8x8 Virtual Office Phone System

What is Virtual Office?
Virtual Office is a secure, cloud-based service that integrates voice, messaging, and meetings all in one place. You can use your virtual office with a traditional desk phone or a computer based softphone application. Providing this software makes it easy and fun to receive and place calls. If you'd like more instructions on how to use 8x8 Virtual Office, please contact your Information Technology Department for more details and instructions.

*Do not provide your internal phone number or extension to the public, always use your external number and/or call queue extension.

Student Equipment Policy

Overview

Use of technology is a privilege extended to students in order to enhance learning and exchange information. The use of available hardware and software (including both external and internal resources) is for the purpose of facilitating the best learning experience. All students and families are required to comply with the Information Technology Acceptable Use Policy and any accompanying protocols.

Student Use of Equipment/Materials

The care of all equipment is the responsibility of each student/parent. If at any time there is an issue with a computing device, please contact the ITD for more instructions. Access to CPA 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. Staff member's are required to know and understand policies related to student/parent usage of CPA devices.

1. Students are never allowed to leave a device unattended
2. Never lend out or transfer device's to other CPA students unless given permission
3. Keep all items away from dangerous conditions (e.g. liquids, heat sources, unstable surfaces or items) and keep away from conditions that would promote damage beyond normal wear and tear.
4. 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.
5. The parent/guardian is expected to monitor and supervise device usage when their child is on the internet
6. All damages are to be immediately reported to the ITD

All parents are given a copy of the Acceptable Use Policy in addition to any support documents and policies.

Standard devices and equipment offered to all students include, but are not limited to:

1. HP 255 G6 - 15.6 inch laptop or Macbook Air 13 inch
2. Apple iMac 21 inch desktop
3. Amazon Fire Tablets and Ipads (versions may vary)
4. HP Officejet or Brother printers

**All available devices are subject to change without notice.*

Equipment Transfer

We do not allow students to transfer their devices to someone else, even those students that are currently enrolled in CPA without first contacting the Information Technology Department. There are times when exceptions can be made, depending on the circumstances. For instance, devices can be transferred within the same family from one sibling to another, however we must be informed of this transfer so all related records can be updated. If there are other circumstances, the device must be sent back to us so we can properly re-assign, image, refurbish, wipe/clear all personal information and user-installed software.

Damage Caused by Carelessness

Much of the damage that occurs is the result of student carelessness. Damage caused by carelessness is not considered "Accidental Damage." Tablet and accessory damage resulting from carelessness will be assessed. Examples of student carelessness would be: iPad (pens) that are noticeably damaged, latches that hold the lid closed being pulled out of the computer case, sticky devices from liquid spills, broken LCD screens that result from shutting the lid with objects still in the keyboard, and the continual loss of keys from the keyboard. When asked how the damage occurred, the answer "I don't know", or "it was fine when I put it in my bag" will be considered damage caused by carelessness. *Habitual damage is considered abuse of school property.*

Individual school laptop computers and accessories must be returned to CPA at the end of each school year. Students who graduate early, are suspended or expelled, or terminate enrollment at CPA for any other reason must return their individual school technology on the date of termination or no later than 30 days after termination. Failure to return the computer will result in a theft report being filed with the local law enforcement. The student will also pay the replacement cost of the computer, or, if applicable, any insurance deductible.

Furthermore, the student will be responsible for any damage to the computer, consistent with the Acceptable Use Policy and must return the computer and accessories to the CPA Technology Department in satisfactory condition. The student may be charged a fee for any needed repairs not to exceed the replacement cost of the device.

Multiple Device Replacements

It is CPA policy to replace devices if there is a reasonable cause. Any technology purchased with the use of Instruction Funds is considered the property of Cabrillo Point Academy. It is the parents responsibility to see that reasonable care is always taken when any item is loaned to a student. Therefore CPA prohibits loaning any equipment more than 3 times during a school year per student. If a student damages an item and request for a replacement more than the allotted privileges, those consecutive occurrences will be considered abuse of school property and no device will be given out to that family/student for the remaining year. Excessive abuse of school property will lead to penalties placed on the students records and further investigation.

Technology Orders

Overview

Technology is an important part of our learning environment and making sure we have those resources available is extremely important to the success of Cabrillo Point Academy. A reasonable attempt shall be made at all times to address the needs of our students and employees, particularly when those needs are due to an accessibility issue presented by a physical impairment or learning disability of some kind. The

CPA IT Department shall make every effort to ensure that each and every student and or staff is presented with an equal or comparable environment regardless of the hurdle they may face.

Policy

This policy establishes the ordering guidelines for all CPA-owned technology resources. The purpose of this policy is to ensure that every CPA student is presented with an equal opportunity to learn and that all employees can adequately use the required technology equipment for the purpose of their required occupation. There are state regulated requirements that must be met where any physical and/or learning impairment exists for any student or work limitation exists for any employee. Please refer to Work Limitations guideline to determine if there are any reasonable accommodations that must be met. Please note that, the ITD is prohibited from making orders for "out of the ordinary" items for Special Education (SPED) students. If you require assistance with a SPED order, please contact your local Director.

Types of accessibility requirements include, but are not limited to, the following applications or devices.

- Screen reading software
- Stereo headsets or other sound devices
- Touchscreen laptops

Work Limitations/Reasonable Accommodations

The California Fair Employment and Housing Act requires that employers of five or more employees to provide reasonable accommodations for individuals with a physical or mental disability to apply for jobs and perform their essential job duties, unless it would cause an undue hardship. Reasonable accommodations include, but not limited to:

1. Changing job duties
2. Providing leave for medical care
3. Changing work schedules
4. Relocating the work area
5. Providing mechanical and electrical aids

Employers must initiate an "interactive process" when an applicant or employee requests reasonable accommodations. The ITD attempts to provide the most useful resources available to employees and students with a disability in a timely manner. If you want more information please contact the HR Director.

Student Orders - Tech Store

The Tech Centre is an integral solution for students to purchase items relevant to their specific needs. All student purchases should be made through the website. Employees that assist families with making technology purchases are expected to familiarize themselves with the use and function of the Tech Centre. To learn more about this great and easy way to place orders, please visit: **techstore.inspireschools.org.**

Transferring Devices

Swapping or transferring devices amongst enrolled family members is allowed. However there are some restrictions and standards that must be followed. In order to better track and update our student data, all technology transfers must first qualify before any transfer is approved.

1. The student/family requesting to transfer their device must inform and update their assigned teacher
2. The student/family or teacher must report the student as "Withdrawn" before a device can be transferred
3. Transfers can ONLY exist amongst enrolled siblings. You can not transfer or loan a device to any other person(s) that is not a sibling currently enrolled with Cabrillo Point Academy
4. Any and all damages to the device will be the responsibility of the transferee
5. No reimbursements will be made to the previous student's account
6. A helpdesk ticket must be submitted requesting to transfer a device to another student. Details must include the current student's name, exit date, assigned teacher, technology serial and asset number and name of the related sibling

The CPA tech department has a responsibility to update and track the inventory systems and data regularly. For safety regulations, it is important to always stay informed about the usage of each device. Properly updating information is apart of ensuring all safety precautions are taken at all times.

Special Education Orders (SPED)
(pending information)

Returns

All items purchased using Instructional Funds must be returned and is the property of CPA. The return requirements are as followed:

Full Refund/Credit

- Returns qualifying for Full Refund or Credit
    - Items eligible for a full refund/credit:
        - Must be undamaged and same condition as received
        - Must be complete with all accessories
        - Working (i.e. non-defective) items may be returned within 30 days of receipt of item for full refund/credit.
        - Defective items may be returned within 90 days of receipt. "Defects" are determined by manufacturer. Must not show signs of physical abuse, misuse or abnormal treatment for full refund/credit.

Partial Refund/Credit

Partial refunds / partial credit are given at the discretion of Cabrillo Point Academy and may (or may not) be given for any reason. Worn, abused, misused or damaged items may or may not qualify for refund/credit.

- Returns qualifying for Partial Refund or Credit
    - Items eligible for partial refund/credit:
        - Working items beyond 30 days
        - Defective items beyond the 90 days

Return Process for students

We are a non-profit school, therefore any monies obtained for educational resources is the responsibility of Cabrillo Point Academy. Upon the withdrawal process, please ensure that the student has technology loaned/purchased through CPA and immediately initiate the return process. It is the policy of CPA that all students, once withdrawn from the school, must return any item within 30 days from their exit date. Please instruct students/parents to follow the return process below. You are also welcomed to return items on behave of a student, however, you will therefore be liable if an item isn't returned. Students returning product due to damages must provide the damaged item before a replacement can be given. The IT Department will evaluate the severity of the damages and determine the best course of action thereafter. If damages are beyond normal wear and tear, applicable charges may be applied.

To return an item for any reason, please:

1. Contact our helpdesk:
    a. Email: tech-help@inspireschools.org
    b. Call: (626) 433-8094
2. Please include and have ready:
    a. Your reason for the return
    b. CPA Asset Tag number or Tech Centre order number
    c. Your mailing address
    d. Current phone number
        i. Please include the student name and associated email
3. Return authorization will be given by a tech support agent
4. A shipping label will be provided at no cost. Home pick-up services may also be available at no additional cost
5. Item(s) will be returned to the Cabrillo Point Academy Technology Department in Duarte, CA.
    a. Do not give your devices to anyone other than as instructed
6. Once returned, the item will be evaluated
7. A refund, credit, or replacement will be issued, if eligible

8. If an item is not returned within the allotted time, local law enforcement will pursue the device on behave of CPA. Any missing technology will be added to the students record by the Records Department.

Note, if you support a student or family that requires a specialty device not provided by the Tech Centre, please contact the Enrichment Department in your location for more instructions.

Stolen Technology

CPA is proud to work with Absolute Software - a solution that allows for effective security technology and student safety programs that track, locate and recover your endpoints in the event of a theft, while ensuring safety for students. Absolute provides:

- Remote security to monitor and protect each device
- Reporting tools that give hardware and software information
- Remote device freeze with user verification messaging
- Track assets on Google Maps, including recent and historical locations
- Web filtering to protect students on and off school networks
- Adherence to CIPA regulations around internet security policies
- Thief investigation services, remediation and more

The Recovery Investigation team will work with local law enforcement to recover any stolen device that is tracked through Absolute. They will attempt to collect the device up to 60 days. If they're unsuccessful, CPA may be compensated up to $500 for that device. *Pricing may vary and is subject to change without notice and is not guaranteed.

The CPA ITD always tries to take the most cautious and diplomatic approach when attempting to recover any stolen items. If the student has withdrawn from the School and the return process has been initiated but failed, three attempts will be made to contact the family using all forms of communication. Once our attempts have been unsuccessful, a police report is established and all information is handed over to the Absolute Recovery Team for further investigation. Absolute will then continue their process by tracking the device, contact the person in question, communicate with local law enforcement and if found provide a warrant to search for the device.

If a student has a lost or stolen device while still enrolled with the School, please report the device to local law enforcement and contact the CPA Technology Department to begin the investigation process. We will do our best to recovery and replace any device that has been reported as lost, stolen or missing. A police report must be provided prior to starting the investigation. ***Please note that this does not apply to all devices. Exclusions include purchases made through a third party vendor, Amazon Tablets or any related Amazon purchase, Apple devices, and older computers without Absolute Software. For Apple device's please contact the IT Department for more detail.***

For more details, please visit: www.absolute.com/en/about/legal/agreements/absolute

Personal Technology Policy

Overview

This policy will set forth the rules and regulations which will determine how the CPA faculty, staff and customer are to perform work on personally-owned employee products. The ITD does not service technology equipment for personal devices. **It is strongly advised that no employee use their personal devices** to access confidential school information unless otherwise given permission from a Director or the Information Technology staff.

Policy

The IT Department always strives to ensure that CPA employees, students, and affiliates receive the best possible technology assistance available. However, this can leave something to be desired for non-CPA, personally-owned technology equipment owned by employees, students, and affiliates.

This policy will set forth the rules, regulations, and guidelines for which the Information Technology Department staff may provide services for personally-owned technology equipment.

All personal technology work will be performed within the following restrictions:

For Faculty and Staff

- Personal technology work may be performed during regular business hours, only if such work does not directly interfere or delay the normal operations or job duties of the CPA employee.
- No parts purchases for personal devices.
- CPA is not responsible for damages, repairs, placements or upgrades to any personally owned hardware or software
- Access to confidential school information is prohibited on personally owned devices, and is only allowed on a case by case basis. Your Director must grant approval.

For Students and Affiliates

- The ITD is prohibited from installing software on personal devices unless it is strictly for school purposes.
- Staff are prohibited from assisting with repairs or work on personal devices for customers (students and or/parents)
    - This includes installing or assisting with software not purchased through Instructional Funds
    - Guiding and directing the customer on how to fix or repair an issue
- If a personally owned device doesn't meet the needs necessary to complete an assignment, the ITD will offer to place a tech order for a new device that may fit their needs. Instructional Funds will be used for all technology purchases.

***CPA ITD is prohibited from placing orders for students and/or staff with the use of personal funds.*