Information Technology Department Policies and Procedures Manual for Staff

Introduction

Overview

This Information Technology Policy and Procedure Manual (Manual) sets forth Cabrillo Point Academy's (School) policies and procedures for use of the School's technology equipment, software, operating systems, storage media, mobile devices, network accounts providing electronic mail or resources, and other information technology devices and/or services (IT Resources) by employees, staff, volunteers, vendors, contractors, and other individuals employed or acting on behalf of the School (collectively referred throughout this document as "Staff").

The School's IT Resources must be used for educational and school business-related purposes with the intent to serve the interests of the students, teachers, parents/guardians, and staff. Staff are responsible for familiarizing themselves with the policies and procedures set forth in this Manual prior to obtaining and using the School's IT Resources, as well as signing any acceptable use agreement. Any misuse, misappropriation, negligence, or deliberate disobedience of the School's IT Resources will not be tolerated and the School reserves the right to take any action necessary to address misuse.

To ensure that the School keeps all IT policies and procedures current and relevant, the School may need to modify and amend this Manual from time-to-time. This Manual is not all encompassing; it is the responsibility of every user to know these guidelines and to use their best judgement and exercise reasonable care when using the School's IT Resources.

The School's IT Department encourages all Staff to take appropriate precautions in use of IT Resources. In the event that Staff may have questions or concerns regarding the use of IT Resources, they should contact the School's IT Department at the following number 619-749-1928 or email address techhelp@cabrillopointacademy.org

Purpose and Scope

The School's IT Department is committed to protecting the School's users from illegal or damaging actions by individuals who use the School's IT Resources. The purpose of this Manual is to outline the acceptable use of the School's IT Resources. Staff must ensure that all use of IT Resources provided by the School are consistent with this Manual and fall within the authorized parameters for access, utilization, distribution, and modification of the School's IT Resources.

This Manual is an integral part of the IT Department's policies and procedures. The guidelines set forth in this Manual apply to all IT Resources owned or leased by the School. Applicable sections of this Manual may also apply to privately-owned equipment that is connected to the School's network (i.e., WiFi Network), which can include, but is not limited to, computer equipment, software, operating systems, storage media, and the internet.

Users of IT Resources must adhere to the School's policies and manuals, including, but not limited to, the Employee Handbook and this Manual. Users are expected to fully comply with local, state, and federal laws and regulations. Failure to adhere to these policies or applicable law may result in discipline, legal action, or other remedies determined to be within the School's authority. These laws include, but are not limited to, the Family Educational Rights and Privacy Act (FERPA).

Other administrative units may be permitted to develop or implement additional policies and procedures related to the use of the School's IT Resources so long as those policies and procedures are consistent with this Manual and other applicable technology-related policies. For more information about developing technology policies and procedures, please contact the School's IT Department.

Definitions

- **"Cabrillo Point Academy**" or "**School**" or "**Organization**" or "**We**" means Cabrillo Point Academy
- "**IT Department**" or "**ITD**" means Information Technology Department.
- "**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,
    - Cloud Based Systems: Web Content Filter, Azure Services, Teamviewer, Adobe, Email, Google
    - Resources: Group Drive File Storage, Website File Storage, Email Accounts, Social Networking Accounts, etc.
- "**You**" or "**Your**" means employee, contractor, volunteer, or any other individual who has been issued a School IT Resource.
- "**User**" means any person(s) accessing or utilizing the Schools' IT Resources that is not a resource operator
- "**AUP**" means Information Technology Acceptable Use Policy.

Acceptable Use Policy

General Use and Ownership Rights

Use of the School's IT Resources is a privilege. As with all privileges, it is the responsibility of the user to use the IT Resources appropriately and in compliance with the School's policies and procedures, as well as applicable law. Staff are responsible for exercising good judgment regarding the use of the School's IT Resources. Staff should be aware that IT Resources and any data that is created on the network is the property of the School. Staff should not have an expectation of privacy, express or implied, in their use of the School's IT Resources. The IT Department may monitor equipment, systems, and network at any time. The IT Department reserves the right to audit networks and systems on a periodic basis to ensure compliance with applicable policies and laws. The School assumes no responsibility for any loss or damage to IT Resources not owned by the School while on the School's network.

The privacy of our students and staff is the highest priority and Staff are expected to take appropriate measures (e.g., password-protect files that have confidential information) when handing confidential information, including personally identifiable information related to a student, that is consistent with state and federal laws (e.g., FERPA). If staff require assistance in determining appropriate security measures, they must contact the IT Department. Violation of this Manual and/or related law or policies could result in disciplinary action (e.g., termination).

The following provides a general roadmap for use of the School's IT Resources:

1. Staff agree to comply with all information outlined in this Manual.

2. Staff must exercise reasonable care to protect IT Resources against damage, loss, and theft. "Reasonable care" includes, but is not limited to: never leaving items unattended; never lending, giving, or releasing items to unauthorized individuals; never removing protective accessories or features (e.g. cases, bumpers, asset tags); or 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. Staff are expected to protect all passwords and prevent the unauthorized or inadvertent disclosure of confidential information.

4. Staff are expected to back up all school information and data.

5. Staff must use exercise extreme caution when opening emails with attachments received from unknown senders; if you receive an email you don't recognize, do not open it. Delete the email and notify the IT Department.

6. All users should lock their workstations when unattended (i.e., save your work and then log off the device or turn off the device).

7. Upon termination of employment, all IT Resources must be returned immediately to the IT Department on your final day. If any attempt to collect the items have failed, all matters will be handled by local law enforcement.

Acceptable Use Policy (AUP)

Unless otherwise specified in this Manual or other School policies or procedures, use of School IT Resources is restricted to educational and school-related business purposes, which must be aligned with the School's mission. Staff are provided access to IT Resources in order to support their job duties, official School business, and other school-related activities.

Staff shall not share with, or transfer to, others their IT Resources and/or school-related accounts, including passwords, or other access codes that allow them to gain access to School IT Resources without the prior approval of the School Principal or his/her designee.

Staff Responsibilities

Staff are responsible for ensuring that they comply with the following:

1. Staff must use the IT Resources for school purposes only, in alignment with the staff's job duties, and in a professional and courteous manner.

2. Staff must respect and protect the privacy of others by refraining from distributing private information about others or themselves; using only assigned accounts; and only viewing or accessing networks to which they are authorized.

3. Staff cannot use IT Resources to access any social media platforms (e.g., Facebook, Instagram, Twitter, etc.) for non-school related activities.

4. Staff must use IT Resources in a manner consistent with the School's policies, including the policies provided in the Employee Handbook.

5. Staff must respect and protect the integrity, availability, and security of all IT Resources by observing all filters and network security practices; reporting security risks or violations; not destroying or damaging data, networks, or other resources without School's permission.

6. Staff are prohibited from using IT Resources to further other acts that are illegal or violate the School's policies. For example, Staff shall not engage in any harassing or discriminatory behaviors or accessing any sexually explicit internet sites.

7. Staff are prohibited from using IT Resources to create, access, download, edit, view, store, send or print materials that are illegal, offensive, harassing, intimidating, discriminatory, sexually explicit or graphic, pornographic, obscene or otherwise inconsistent with the values and general standards for the School.

8. Staff shall refrain from using IT Resources for purposes other than those related to the School's program. For example, Staff cannot use Information Technology to buy, sell, advertise, or otherwise conduct business.

9. Staff are prohibited from using the IT Resources to solicit for political causes, commercial enterprises, outside organizations, or other non-job-related solicitations.

10. Staff must abide by all copyright, trademark, patent, and other laws governing intellectual property. No software may be installed, except as permitted by applicable law or School administration, copied or used on School equipment except as permitted by law. All software license provisions must be strictly followed.

The duties and responsibilities set forth above by no means are exhaustive; they are intended to provide a framework and guidepost for the activities that are acceptable.

Use of IT Resources for Incidental Purposes

IT Resources are to be used for educational and school-related purposes. However, Staff may use IT Resources for incidental purposes provided that they comply with all applicable School policies, including, but not limited to, this Manual, the Employee Handbook, applicable law. Incidental use is permitted only if it does not:

1. Directly or indirectly interfere with the School's operation of IT Resources.
2. Interfere with the user's job duties.
3. Burden the School with noticeable incremental costs.
4. Violate the law or School's policies.
5. Used for commercial purposes not under the auspices of the School.
6. Used for personal financial gain except as permitted under applicable policies.

Under no circumstances may incidental personal use violate the law, interfere with the fulfillment of Staff responsibilities, or adversely impact or conflict with activities supporting the School's mission. Any incidental personal use of the School's IT Resources may be designated as the School's records subject to disclosure to the School and third parties in accordance with law.

The duties and responsibilities set forth above by no means are exhaustive; they are intended to provide a framework and guidepost for the activities that are acceptable.

Revocation of Privileges

Staff access or privilege to the School's IT Resources may be revoked or revised at any time and as necessary in the event that one of the following events occur (which are non-exhaustive):

1. Staff transfer.
2. Staff resignation.
3. Staff termination.
4. Investigation related to Staff conduct.
5. Interfere with the user's employment or other obligations to the School.
6. Burden the School with noticeable incremental costs

Unacceptable Use

General Use Restrictions

Under no circumstance are Staff permitted to engage in any activity that is illegal under local, state, or federal law, or violate the School's policies, including this Manual and the Employee Handbook, while utilizing the School's IT Resources.

The activities listed below, in general, are prohibited unless Staff are expressly exempt. The list of prohibited activities below is non-exhaustive and is intended to provide a framework of activities which fall within the category of "unacceptable use". Staff must ultimately use their best judgement and exercise reasonable care when using the School's IT Resources.

Unacceptable Use of School Systems and Networks

Users are responsible for complying with the guidelines of this Manual and all applicable laws and regulations regarding the dissemination and protection of data and information that is confidential, particularly with regards to FERPA, and any other applicable state and federal legislation dealing with information privacy.

The following activities are strictly prohibited:

1. 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 the School'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.

4. Disclosing personally identifiable information related to a student without prior written consent.

5. Setting up file sharing in which protected intellectual property is illegally shared.

6. Intentionally introducing malicious programs into the system or server (e.g., viruses, malware, worms, Trojan horses, email bombs, etc.).

7. Inappropriate or unauthorized use or sharing of School IT Resources, networks, systems, accounts, etc.

8. Revealing your account username and password to others or allowing use of your account by others (e.g., family or other household members).

9. Changing another user's password, access, or authorizations.

10. Using the School's IT Resources to actively engage in displaying or transmitting material that is in violation of the School's policies or applicable laws, including, but not limited to, the sexual harassment policy or laws, hostile workplace laws, or other illegal or impermissible activity.

11. Using the School's IT Resources for any private purpose or for personal gain, unless otherwise permitted.

12. Engaging in, or effecting security breaches, or malicious use of system communication.

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

14. Except when anonymous access is explicitly provided, engaging in activities intended to hide the user's identity or otherwise forging and/or misrepresenting the user's identity.

15. Purposefully creating nuisance traffic for the network or systems attached to the network.

16. Purposefully creating nuisance radio waves or Wi-Fi traffic which prevents successful wireless communication.

17. Purposefully deleting work related files, shared drive files, or confidential files that the School officials, teachers, staff, and IT employees utilize to perform the duties and responsibilities on the job.

18. Circumventing user authentication or accessing data, accounts, or systems that the user is not expressly authorized to access.

19. Interfering with or denying service to another user on the School's network or using IT Resources to interfere with or deny service to persons outside School.

20. Any other use that purposely causes a negative potential impact on School systems or operations or otherwise causes a loss of confidentiality, integrity, or availability of School data or services.

Unacceptable Use of Electronic Communications

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

Key prohibitions include, but are not limited to:

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 harassing or discriminatory behaviors via electronic communication, whether through language, frequency, or size of messages.

3. Masquerading as someone else by using their email, 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 the School-provided accounts for non-School related business (e.g., personal 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, researching, and outreach. School computers and resources are limited in capacity and are in high demand. To conserve IT Resources 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.

Enforcement

This Manual is enforced through various measures, including those set forth below. Any user who discovers unauthorized access or use of IT Resources or attempts to, or engages in, improper access or use of IT Resources must immediately report it to the IT Department and the School Principal. Staff are responsible for ensuring that they understand the guidelines set forth in this Manual and other applicable policies, including, but not limited to, the Employee Handbook.

Interim Measures

The School may take interim measures to prevent unauthorized or unacceptable access or use of the School's IT Resources. This can include, but is not limited to any activity that:

1. Violates the law or the School's policies.
2. Has the potential to cause significant damage to, or interfer, with the School's operations.
3. May cause harm or damage to another person (e.g., actions that are threatening, discriminatory, or violate any School policies or applicable law)
4. May result in liability to the School

Interim measures may include, but are not limited to, temporarily disabling Staff access to, or use of, IT Resources.

Violations of Policy

Violations of the policies set forth in this Manual will be taken seriously and may result in disciplinary action, including possible termination, and civil and criminal liability.

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 the School's entire privacy network. As such, all employees (including contractors and vendors with access to the School's network or utilize its IT Resources) 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, a School-affiliated account, service, or network (or any form of access that supports or requires a password). **The Password Protection Standards** below also apply to the use of family accounts and should always be handled with care and common sense.

Even if Staff use a password to access the IT Resources (or any aspect thereof), the confidentiality of any message stored in, created, received, or sent from the School's IT Resources is not certain. Use of passwords or other security measures does not in any way diminish the School's right to monitor and access materials on its IT Resources, nor does it create any privacy right of Staff in the messages and files stored or transferred through the School's IT Resources.

Any password used by Staff must be revealed to the School upon request for any reason that the School, in its discretion, deems appropriate. Further, Staff should be aware that deletion of any email messages, voicemails, or files would not truly eliminate the messages from the system. All email messages, voicemails, and other files may be stored on a central back-up system in the normal course of data management.

Password Protection Standards

General Password Construction Guidelines

Passwords are used for various purposes. Some of the more common uses include: user-level accounts, web accounts, email accounts, screensaver protection, voicemail password, and local router logins. Staff should select strong passwords when using School IT Resources.

1. Poor (unacceptable) passwords have the following characteristics:

    - ✓ The password contains fewer than 8 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 characteristics:

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

   ✓ Have digits and punctuation characters as well as letters (e.g., 0-9; !@#$%^&*()_+|~-)

   ✓ Are at least ten alphanumeric characters long

Try to create passwords that can be easily remembered. One way to do this is to 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!)

Password Protection Standards

Do not use the same password for School accounts as you use for non-School accounts (e.g., personal ISP account, personal email accounts, etc.).

Here is a list of Do NOTs related to password usage:

- ✓ Do NOT reveal a password over the phone to ANYONE
- ✓ Do NOT reveal a password in an e-mail message
- ✓ Do NOT talk about a password in front of others
- ✓ Do NOT hint at the format of a password (e.g., “my family name”)
- ✓ Do NOT reveal a password on questionnaires or security forms
- ✓ Do NOT share a password with family members
- ✓ Do NOT reveal a password to co-workers
- ✓ Do NOT 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 School information. If a password is requested by a parent or student, verify their identity, then simply forward them an associated link to reset their password. We are not responsible for creating passwords for end-users.

Internet and Email Policy

Overview

Use of IT Resources, such as sending or retrieving voicemails or emails or using the internet must be solely for School-related business and activities. Most job responsibilities at the School require access to the internet and the use of educational software. Only people appropriately authorized, for School purposes, may use the internet to access and download additional software. This authorization is generally exclusive to decisions that the IT Department makes in conjunction with the need to perform your job duties and any request made from the School Principal or his/her designee.

Staff do not have an expectation of privacy in anything they view, create, store, send, or receive through the School's IT Resources, including email accounts. Email messages must be treated as confidential by other Staff and accessed only by the intended recipient. Staff are not authorized to retrieve or read any email messages that are not sent to them or by them. Any exception to this policy must receive the prior approval of the School Principal or his/her designee.

Software Access

Software needed, in addition to the Google products, must be authorized by your immediate supervisor and/or the School Principal and downloaded by the IT Department. If you need access to software or specific websites, YouTube videos (educational), or whitelist apps, please talk with your immediate supervisor and consult with the IT Department to explain what you expect to receive from the product.

Internet Usage

Internet use during School hours or use of School IT Resources that are connected to the Schools network, must only be School-related. Internet use brings the possibility of breaches of 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 the School, potential access to the School 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 School IT Resources or other electronic equipment, including devices owned by Staff, be used on School time at work to obtain, view, purchase, or access 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.

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, the School.

The School's reputation and brand should be protected by all Staff. The lives and actions of your coworkers should never be shared online. Staff must maintain the confidentiality of all students at all times.

Social Media

If you wish to use networking protocols or set up a social media site as a part of the educational process, please work with your School Principal and IT Department to identify and use a restricted, School-endorsed networking platform. Such sites will be the property of the School who will have unrestricted access to, and control of, such sites.

Staff shall not accept students as friends on any personal social networking sites and are to decline any student-initiated friend requests. Teachers are not to initiate "friendships" with students or parents. Staff must delete any students already on their "friends" list immediately.

With regard to social networking content (e.g., Instagram, Facebook, Twitter, etc.), Staff should not use commentary deemed to be defamatory, obscene, proprietary, or libelous with regard to any School-related business or policy, employee, student, or parent. Additionally, employees should exercise caution with regards to exaggeration, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterizations. Employees should weigh whether a particular posting puts his/her effectiveness as a School employee at risk. School encourages employees to post only what they want the world to see. Imagine that students, their parents, or administrators will visit your site as most information is available to the general public even after it is removed from the site. Employees may not discuss students nor post images that include students.

Due to security risks, employees must be cautious when installing the external applications that work with the social networking site. At a minimum, it is recommended that all employees should have all privacy settings set to "Only Friends". The settings "Friends of Friends" and "Networks and Friends" open your content to a large group of unknown people, including students.

Although there are advantages to the use of social media, there are many disadvantages, including, but not limited:

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

Staff should be cautious when using social media platforms and should use their best judgement.

Email Usage at School

Email is to be used for School business only. School confidential information must not be shared outside of the school, without authorization, at any time. You are also not to conduct personal business using School computers or emails, unless otherwise permitted. Please keep this in mind as you consider forwarding non-business emails to associates, family members, or friends. ***Please keep all email messaging appropriate and professional when communicating with co-workers and families***.

Mass Email and Effective Electronic Communication

Transmission of mass emails must comply with federal and state laws, as well as the School's policies. Mass emails should be limited and for educational and school-related purposes. Mass email is appropriate for information that pertains to the majority of the recipients; is critical and/or time-sensitive; and provides the School community with essential information.

Mass emails that are not in line with the School's mission or those that are for personal gain or businesses purposes are inappropriate. You must obtain permission for any email lists to which you are not authorized to access. 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 the School Principal.

Mass Email Checklist

Before you send a mass email, 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 mission?
- 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; and
    - 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 IT Department for more information about these limitations.

Employee Email

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

Emails That Discriminate

Any email content that discriminates against any protected classification including, but not limited to, age, race, color, religion, sex, national origin, or disability is prohibited. Threatening or offensive

emails are prohibited at the School. Violation of this policy could result in disciplinary action or termination.

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 that the email you receive 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 identify, such as the following:

- 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 or disclose private account information, so do not fall for this trap.

- Any email that asks for your personal or sensitive information should not be 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 I know? Am I expecting an email from this 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 or may appear to be a scam. 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 IT Department immediately.

Staff Equipment Policy

Overview

The School's goal is to provide sufficient equipment to allow School staff to manage their duties efficiently. Equipment is usually assigned and issued upon hire for all new employees. All new devices require between three (3) days to three (3) weeks for delivery and configuration. Therefore, administrators/supervisors are advised to notify the IT Department immediately upon hiring a new staff member.

This Manual provides the School policy requirements to assure appropriate and equitable issuance to faculty and staff of the School's IT Resources. 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 staff.

New Hire Details: Upon hiring a new employee, School management must send to the IT Department the following information:

- Employee's full name
- Supervisor or manager's full name
- Employee's full address (only necessary for staff that work off-site)
- Employee's title of position (please include department)
- Employee's start date
- List of equipment needed (only if they require additional equipment)
- Requested school-affiliated email address

The School may offer the following standard devices/equipment to Staff:

1. Up to two monitors, one keyboard, one mouse, and one dock
2. Office phone extension line (approval by the School Principal or his/her designee is required)*

All IT Resources require prior approval of the Staff's immediate supervisor and should be made by submitting a ticket to the School's Helpdesk at the following address: techhelp@cabrillopointacademy.org. *All devices are subject to change without notice.

School Owned Equipment

Any IT Resource including, but not limited to, desk phones, smartphones, tablets, laptops, desktop computers, and tablets that the School provides for your use, should only be used for school-related purposes. Keep in mind that the School owns the devices and the information in these devices. If you leave the School for any reason, you must return the IT Resources upon request or on your last day of work, whichever occurs first.

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

Staff Use of Equipment/Materials

IT Resources provided on School property is for the benefit of students and staff. The care of all devices is the responsibility of each Staff member. If at any time there is an issue with an IT Resource, please contact the IT Department for more instructions. Staff 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 its assigned location, prior approval must be given by the School Principal or his/her designee.

2. Staff are responsible for the cost of repairing any damaged, lost, or stolen item in their control or possession. Staff must immediately contact the School Principal or his/her designee and the IT Department to report any damaged, lost, or stolen IT Resource.

3. Under no circumstances may equipment be used for private or personal business ventures. IT Resources can only be used for school business.

4. Upon departure from the School all Staff must return IT Resources upon request or on their last day, whichever occurs first. If the School's attempts to collect a device is unsuccessful, the School will take necessary action to retrieve the device.

Pre-Purchase Review Requirements

To ensure sound purchasing, supportability, and appropriate pricing, and to ensure security of the School's resources, the purchase of all School IT Resources shall be approved by the IT Department prior to purchase. If there is an item that is "out of the ordinary," prior approval from the School Principal or his/her designee is required.

*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. The School abides by all legal requirements for licensing software. Only licensed software will be installed on school owned equipment. The IT 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 a part of your job duties. The IT Department will not be liable for licensing issues when software isn't in accordance with use for school related business and the Staff member did not have prior authorization to access, use, or purchase the software. Licensing purchases (including software) that have not been approved by management may be classified as a personal purchase and may not be reimbursed. 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 devices without the prior approval of the School Principal or his/her designee.

Security

Every member of the School community is responsible for protecting the security of School information and information systems by adhering to the objectives and requirements stated within all School policies, including privacy and security protections. 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 IT privileges and/or disciplinary action.

Replacement Cycle and Redeployment

The School will attempt to reuse or appropriately dispose of any IT Resources that can no longer be used appropriately. Redeployment and/or replacement is at the discretion of the IT Department. All Staff must contact and obtain the approval prior to requesting replacement of any IT Resources from the IT Department.

Disposal of Equipment

The IT Department 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 of, or collect money for, school owned equipment, computers, furniture, or other supplies/materials, regardless of the source of funds. No individual may gift or donate equipment, including, but not limited to, computers, cell phones, furniture, or other items without School approval. School owned equipment, including, but not limited to, computers, laptops, tablets, cell phones, furniture, and other materials may not be removed from the School, converted to personal property, or retained for personal use.

Equipment Configuration Policy

Overview

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

Policy

Generally, staff shall order and utilize equipment that is serviceable and recommended by the School IT Department. Since equipment availability changes over time, any individual or department wishing to purchase IT Resources should first consult with the IT Department staff. This applies to any and all IT Resources, 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.)

Virtual Office Phone System

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. If you'd like more information on how to use 8x8 Virtual Office, please contact your IT 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.

Stolen Technology

All devices issued by the School are generally encrypted with data protection software (e.g., BitLocker, FileVault). This 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 device is vulnerable to unauthorized access, either by running a software-attack tool against it or by transferring the device's hard disk to a different device. BitLocker helps mitigate unauthorized data access by enhancing file and system protections.

Personal IT Resources

Overview

This policy will set forth the rules and regulations which will determine how Staff will perform work on personally-owned IT Resources, to the extent permitted. The IT Department does not service personal IT Resources. **It is strongly advised that no employee use their personal devices** to access confidential school information unless otherwise permitted by the School Principal (or designee) and the IT Department.

Policy

The IT Department always strives to ensure that School employees, students, and affiliates receive the best possible technology assistance available. The School IT Department does not provide support for personal devices.

The following rules applies as it relates to IT Department support for personal devices:

- The IT Department is prohibited from installing software on personal devices unless it is strictly for school purposes and approved by the School Principal or his/her designee.

- Staff are not permitted to assist students and/or parents/guardians with repairs on personal devices or School-owned equipment. This includes installing or assisting with software, or guiding and directing the student or his/her parent/guardian on how to fix or repair the problem. If a student or parent/guardian is having issues with the use of a personal device or school-owned equipment, staff must report this to the IT Department to determine appropriate next steps.

** The IT Department is prohibited from placing orders for staff with the use of personal funds.