



Information Technology Department

Policies and Procedures

Overview

This document serves as a rulebook and roadmap for successfully and properly utilizing the technology resources at Blue Ridge Academy (BR). 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 the school'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 the school 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 BR 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 BR ITD does encourage all BR employees and associates to err on the side of caution should a difficult or questionable situation present itself. Please contact the ITD if you require assistance or have any questions.

Contents

Overview	1
Acceptable Use of Information Technology	3
Unacceptable Use	6
Enforcement	7
Password Policies and Procedures	8
Internet and Email Policy	10
Equipment Configuration Policy	17

Acceptable Use of Information Technology Resources

Overview

Blue Ridge Academy's 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, Blue Ridge Academy (BR) is committed to protecting itself and its students, faculty, and staff from unethical, illegal, or damaging actions by individuals using these systems.

BR is committed to upholding important security, privacy, and safety regulations, protocols, and standards. Users of BR devices, networks, accounts, and other resources must adhere to BR 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 BR. 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. **BR or School or Organization or We** – Blue Ridge Academy
2. **ITD** – Blue Ridge Academy Information Technology Department
3. **You or Your or I** - employee of BR and or signer of this Acceptable Use of Technology Policy
4. **Resources** - devices, systems, services or networks owned, operated or issued by BR
5. **User** - any person(s) accessing or utilizing BR 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 Blue Ridge Academy. These rules are in place to protect students, faculty, and staff; i.e., to ensure that members of the Blue Ridge Academy community have access to reliable, current IT resources that are safe from unauthorized or malicious use.

Insecure practices and malicious acts expose Blue Ridge 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 school's 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 Blue Ridge Academy. This policy applies to all IT resources owned or leased by Blue Ridge Academy and to any privately owned equipment connected to the school's 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 BR community who accesses and uses IT resources. Therefore, every user of Blue Ridge 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 BR 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 BR 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 ITD(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 BR'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 on your final day of employment. If any attempt to collect the items have failed, all matters will be handled by local law enforcement. ***For more information, please contact the BR 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. BR computers 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.

Unauthorized Use of BR 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 Blue Ridge 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 a Blue Ridge 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 a Blue Ridge 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 use all electronic communications appropriately and professionally.

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 Blue Ridge 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 Blue Ridge 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 or school 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 Blue Ridge Academy entire network. As such, all employees (including contractors and vendors with access to Blue Ridge 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 BR facility, has access to the BR database, or stores any non-public information pertaining to BR. **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 Blue Ridge 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 characteristics:



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 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

✓ 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!

Password Protection Standards

Do not use the same password for Blue Ridge Academy accounts as for other non-Blue Ridge 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 email message.

- X** Don't talk about a password in front of others.
- X** Don't hint at the format of a password (e.g., "my family name").
- X** Don't reveal a password on questionnaires or security forms.
- X** Don't share a password with family members.
- X** Don't reveal a password to co-workers while on vacation.
- X** 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 BR 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.

Internet and Email Policy

Overview

Voicemail, email, and internet usage assigned to an employee's computer or telephone extensions are solely for the purpose of conducting Blue Ridge Academy business. Most job responsibilities at BR require access to the internet and the use of software. Only people appropriately authorized, for BR 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 Blue Ridge Academy time, using BR-owned devices that are connected to the school's 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 BR, potential access to BR 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 BR owned computers or other electronic equipment, including devices owned by the employee, be used on BR 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 students and or employees and enhances our school brand. Many employees have social media responsibilities in their job description including the social media marketers, tech support, and School Growth/Public Relations staff.

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 BR. You are strongly encouraged not to share disparaging information that places BR 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 BR'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 BR harassment policy.

Email Usage at BR

Email is to be used for BR business only. BR confidential information must not be shared outside of the school, without authorization, at any time. You are also not to conduct personal business using BR 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 supervisor.

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 BR owns any communication sent via email or that is stored on BR

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 Blue Ridge 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

BR 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 Blue Ridge Academy (BR) 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 employee's full name
- Supervisor or Director
- 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)
- Email address to be assigned

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

1. Laptop which usually includes touchscreen
2. Wireless printer/scanner/fax machine
3. 1 or 2 displays, keyboard, mouse, and dock (offered to office staff ONLY)
4. Office phone

Please note, all requests should have prior approval from a supervisor or director and be made by submitting a ticket via helpdesk: Helpdesk@theblueridgeacademy.com. For detailed instructions on placing orders, please see the Technology Ordering Policy. **All devices are subject to change without notice.*

BR Owned Equipment

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

Staff Use of Equipment/Materials

The equipment at BR 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 its 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 employee's possession if caused by the employee's gross negligence. 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 BR 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 BR 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 supervisor or director 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. BR abides by legal requirements for licensing software. Only licensed software will be installed on school owned equipment. The ITD 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 Information Technology staff will not be liable for licensing issues when software is not in accordance with use for school related business and did not 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 BR to insure that we are compliant with local, state and federal laws prohibiting the unfair use and distribution of confidential information. Every member of the BR community is responsible for protecting the security of school information and information systems by adhering to the objectives and requirements stated within all BR 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 BR 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 BR 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 BR. 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 BR 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 an BR 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, 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.)

Ring Central 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 would like more instructions on how to use Ring Central Virtual Office, please contact your ITD 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/guardian. If at any time there is an issue with a computing device, please contact the ITD for more instructions. Access to BR technology, resources, and support 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. Students/parents/guardians are required to know and understand policies related to student/parent usage of BR devices.

1. Students are never allowed to leave a device unattended
2. Never lend out or transfer devices to other BR 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. Windows laptop or MacBook
2. Student Chromebook
3. iPads
4. Color Printer

**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 BR.

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 BR upon withdrawal or graduation. Students who graduate early, are suspended or expelled, or terminate enrollment at BR 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 device.

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 BR 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 BR policy to replace devices if there is a reasonable cause. Any technology purchased with the use of the Planning Amount is considered the property of Blue Ridge Academy. It is the parent/guardian's responsibility to see that reasonable care is always taken when any item is loaned to a student. Therefore, BR prohibits loaning any equipment more than 3 times during a school year per student. If a student damages an item and requests 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 further investigation.

Technology Orders

Overview

Technology is an important part of our student's learning environment. Making sure these resources are accessible is extremely important to the mission of Blue Ridge 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 BR IT Department shall make every effort to ensure that each and every student and or staff is presented with an equal or comparable environment technology resources.

Policy

This policy establishes the ordering guidelines for all BR-owned technology resources. The purpose of this policy is to ensure that every BR 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 Catalog

The Tech Catalog is an integral solution for students to request items relevant to their specific needs. All student requests should be made through the Tech Catalog in the Procurify system. Employees that assist families with making technology requests are expected to familiarize themselves with the use and function of the Tech Catalog .

Special Education Orders (SPED)

The ITD will work in collaboration with the Special Education Department to ensure that technology items required to meet the needs of a student, as outlined in their IEP, are ordered and delivered to the family.

Returns

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

Refund/Credit

- Returns qualifying for Refund or Credit
 - Items eligible for a 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 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.

Return Process for students

Upon withdrawal, please check if the student has technology loaned/purchased through BR and immediately initiate the return process. It is the policy of BR that all students, once withdrawn from the school, must return any item within 30 days from their exit date. The ITD will email the parent with a shipping label to return all school devices. The Blue Ridge employee is also welcome to return items on behalf of a student, however, you will therefore be liable if an item is not returned. Students returning products 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 other reason, please:

1. Contact our helpdesk:
 - a. Email: Helpdesk@theblueridgeacademy.com
 - b. Call: (661) 412-9363
2. Please include and have ready:
 - a. Your reason for the return
 - b. BR Asset Tag number or Tech order number
 - c. Your mailing address
 - d. Current phone number
 - i. Please include the student's 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.
5. Item(s) will be returned to the Blue Ridge Academy Technology Department in San Dimas, 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 behalf of BR. Any missing technology will be noted in the student's record by the Records Department.

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

Stolen Technology

Blue Ridge provides:

- o Remote security to monitor and protect each device
- o Reporting tools that give hardware and software information
- o Web filtering to protect students on and off school networks
- o Adherence to CIPA regulations around internet security policies

Additionally, we reserve the right to utilize digital features for the purposes of recovering property that is believed to be lost or stolen.

BR will work with local law enforcement to recover any stolen device.

BR 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 for further investigation. ITD will then continue their process by tracking the device, contacting the person in question, communicating 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 BR ITD to begin the investigation process. ITD will do their best to recover and replace any device that has been reported as lost, stolen or missing. A police report must be provided prior to starting the investigation.

For more details, please contact: helpdesk@theblueridgeacademy.com.

Personal Technology Policy

The ITD does not service technology equipment for personal devices. **Employees should not use their personal devices** to access confidential school information unless otherwise given permission from a Director or the Information Technology staff.