

INTERNET ACCEPTABLE USE POLICY

Purpose

This policy defines acceptable use responsibilities when using the Bear Grass Charter School's (BGCS) computing systems. This policy includes an agreement form that must be signed by each User certifying that the User has read, understands and agrees to comply with this policy.

Scope

The Internet Acceptable Use Policy applies to all fulltime, part-time, and temporary school employees, students, contractors, and others employed by third parties ("**User**" or "**Users**") who perform work on the school premises or anyone granted access to BGCS's computing systems.

Computing system is defined as all computers, peripheral devices, information systems, networks, email, and other information technology resources owned, operated on-behalf of, leased by, or controlled by Bear Grass Charter School. This includes, but is not limited to computing devices that use the school's network for connectivity.

Information regarding the school's Internet Acceptable Use Policy must be made available to all Users by the Principal, Assistant Principal or designee responsible for the performance of that User.

Policy

Users shall use Bear Grass Charter School's computing systems for educational purposes. Users may use school computing systems for limited personal use so long as that use does not interfere with their work, the educational goals of the school and results in no incremental cost to the school. The intent of this policy is to ensure proper behavior when using these computing systems.

Examples of Bear Grass Charter School's computing systems include, but are not limited to: computers and related peripheral equipment, software, library resources, telephones (including cellular), facsimile machines, photocopiers, office supplies, network connectivity, mobile devices, instant messaging, and access to Internet services, and email.

This policy in no way limits the use of the computing systems for official and authorized activities. The Bear Grass Charter School administration is responsible for maintaining a signed copy of this policy for all Users.

Acceptable Use

Users shall not use the computing systems for activities that are unacceptable. Any devices attaching to, accessing or using the computer systems (e.g. wired, wireless networks, storage devices such as USB flash drives) must be

pre-approved unless signed-in using the quest network. Software shall not be installed on school's computers without prior approval by the Principal or designee. Any device connect to the computing system must meet all security standards set by Bear Grass Charter School.

Misuse or unacceptable use of the school's computing systems includes, but is not limited to:

1. Any use that causes congestion, delay, or disruption of service to any school computing system. For example: video, sound or other large file attachments can degrade the performance of the entire network.
2. Using the computing systems to gain or attempt to gain unauthorized access to other systems.
3. The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.
4. Using the school's computing systems for activities that are illegal, inappropriate, or offensive - Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
5. Using the computing systems for the creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials.
6. Using the computing systems for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g. consulting for pay, sales or administration of business transactions, sale of goods or services)
7. Using the computing systems to engage in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity
8. Posting Bear Grass Charter School's information to external news groups, bulletin boards or other public forums without permission or authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Bear Grass Charter School User (unless appropriate approval has been obtained from the Board of Directors or the Principal) or uses that do not meet the school's mission or educational goal's (such as social media websites)
9. Any use that could generate more expense to Bear Grass Charter School.
10. Sending any Restricted or Highly Restricted data, such as student data, over email without permission or authority.
11. The unauthorized acquisition, use, reproduction, transmission, distribution or installation of any controlled information including computer software, data and ID's, that includes privacy information, copyrighted, trade-marked or material with other intellectual property rights (beyond fair use),

proprietary data, or export controlled software or data (e.g. Software Key Crackers or other software used to circumvent intellectual property rights)

12. Installation on the school's computing systems of any unapproved software

Computer Viruses/Malicious Software

It is the responsibility of Users to help prevent the introduction or spread of malicious software. Bear Grass Charter School computing systems are equipped with a security software (e.g. anti-virus, firewalls, host intrusion detection, content filtering) and configured to protect the school's information. The software and the configuration of computing systems are used to protect the school's information from malicious software and intrusion attempts. In some cases it is used to automatically identify and disinfect malicious software. While using the school's computing systems, Users:

1. Shall not remove or change the configuration of security software (including but not limited to anti-virus, access controls, configuration settings) installed on Bear Grass Charter School computers.
2. Shall report any failure, out-of-date warning, or absence of security software (including but not limited to anti-virus) to the Principal or designee as soon as possible.
3. Shall report all malicious software that the security software fails to detect or disinfect to the Principal or designee as soon as possible.

Access Management

Users have no inherent right to use the school's computing systems, software, email or Internet services. All credentials (e.g. username, passwords), personal identification numbers (PIN's), or tokens, regardless of the associated hardware platform, are considered to be school property that has been issued to the User.

Users shall be responsible for the use of their credentials and for any hardware or software devices and applications associated with their credentials (login information).

Computer credentials shall be assigned to individuals. The individual is accountable for all activity carried out with their credentials.

Users shall NOT share their credentials with other users or borrow a credential from someone else.

All Users shall be responsible for choosing passwords that are difficult to guess. Passwords shall be kept secret and not revealed to anyone.

Consent to Monitoring

Users DO NOT have a right, nor should they have any expectation, of privacy while using any school computing system at any time, including accessing the Internet, and using email. To the extent that Users wish that their private activities remain private, they shall not use the school's computing systems such as their computer, the Internet, or email. By using the school's computing systems, Users consent to disclosing the contents of any files or information maintained or sent through the school's computing systems, including location based tracking of assets (e.g. GPS, A-GPS, 3G, or other location aware services). If computer equipment resides in a User's office, classroom, cubicle, or workstation, the User acknowledges and agrees that the school can enter that office/classroom/cubicle/workstation to remove the equipment.

By using the school's computing systems, Users consent to monitoring and recording of their activities, including, but not limited to, accessing the Internet and using email. Use of computing systems is collected through a variety of programs and/or applications. Many systems generate an audit trail. Any use of the school's communications resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

The school uses electronic auditing of Users' activities as deemed appropriate.

The school applies filters and monitors data processing activities as needed to secure and protect the availability of Bear Grass Charter School services for employees, students, contractors, third parties and other Users.

The school investigates reported incidents of suspected abusive and/or illegal activities. Investigations of specific individuals are performed in accordance with Bear Grass Charter School's policies and procedures. The investigations may include reviews of electronic data files and records.

The school employs monitoring tools to detect improper use. Electronic communications may be disclosed within the school to Users who have a need to know in the performance of their duties. Information concerning electronic activities by school users is subject to both internal and external audits. The Department will periodically audit, inspect, and/or monitor the Users' computer and Internet activities. The failure of the school to monitor use is not a waiver of its rights to monitor.

All users of Bear Grass Charter School computing systems are advised that their use of these systems may be subject to monitoring and filtering. By using the school's computing systems, Users consent to monitoring and recording. The school has the right to monitor – randomly and/or systematically – the use of Internet and the school computing system's connections and traffic. Any activity conducted using the school's computing systems (including but not limited to computers, networks, mobile devices, email, etc.) may be monitored, logged, recorded, filtered, archived, or used for any other purposes, pursuant to applicable school policies and State and Federal laws or rules. Bear Grass Charter School reserves the right to perform these actions without specific notice to the User.

Personal Use

Personal use is a privilege, not a right, and may be taken away at any time. This policy does not create the right to use school computing systems for non-educational purposes. Nor does the privilege extend to modifying such computing systems, including loading personal software or making configuration changes.

Enforcement

Failure of the school's Users to comply with this Internet Acceptable Use Policy may result in disciplinary actions up to and including termination of employment for staff and teachers or suspension for students. Any unauthorized disclosure of information shall constitute grossly inefficient job performance. A violation of the Internet Acceptable Use Policy that results in serious loss of or damage to school property or funds which adversely impacts the school constitutes grossly inefficient job performance.

Failure of the school's contractors to comply with Internet Acceptable Use Policy or other Security Policies and Standards may result in termination of their contract. Bear Grass Charter School may also pursue or may assist other parties in pursuing legal remedies for violations of law or for recovery of damages resulting from violation of information security policies and standards.

USER CERTIFICATION OF NOTIFICATION AND AGREEMENT OF INTERNET ACCEPTABLE USE POLICY

I certify that I am an employee, student, volunteer, guest, vendor or contractor working for or attending Bear Grass Charter School and that I have read this "Internet Acceptable Use Policy" and understand my obligations as described in the policy. I understand that this policy was approved by the Board of Directors of Bear Grass Charter School and these obligations are not specific to any individual, but are applicable to all employees, students, volunteers, and contractors of the school. I understand that failure to observe and abide by these obligations may result in disciplinary action, which may include termination of employment, suspension, expulsion and/or contract termination. I also understand that in some cases, failure to observe and abide by these obligations may result in criminal or other legal actions. Furthermore, I have been informed that the school will retain this signed agreement on file for future reference. A copy of this agreement shall be maintained in the personnel file, student file and/or in the contract administration file.

Print Name _____

User Signature (e.g. Employee, Student, Volunteer, Guest, Vendor or Contractor Signature)

_____ Date _____

Sign Appropriate Approval:

Supervisor's Signature _____ Date _____

Parent's Signature _____ Date _____

Sponsoring Teacher Signature _____ Date _____