BRUNEAU/GRAND VIEW TECHNOLOGY POLICIES

Acceptable Use Policy

TECHNOLOGY USEAGE (ACCEPTABLE USE POLICY)

Student Users

No student will be given access to the district's technology resources until the district receives a *User Agreement* signed by the student and the student's parent(s), guardian(s) or person(s) standing in the place of a parent. Students who are 18 or who are otherwise able to enter into an enforceable contract may sign the *User Agreement* without additional signatures.

Employee Users

No employee will be given access to the district's technology resources until the district has a signed *User Agreement* on file. Authorized employees may use the district's technology resources for reasonable, incidental personal purposes as long as the use does not violate any provision of district policies, regulations or procedures, hinder the use of the district's technology for the benefit of its students or waste district resources. Any use that jeopardizes the safety, security or usefulness of the district's technology is considered unreasonable. Any use that interferes with the effective and professional performance of the employee's job is considered unreasonable.

Because computers are shared resources, it is not appropriate for an employee to access, view, display, store, print or disseminate information via district resources, including email or internet access that students or other users could not access, view, display, store, print or disseminate without authorization by the district. Student teachers, interns, volunteers, substitutes, etc. are considered employees for the purposes of network access.

Board Member Users

Members of the School Board may be granted user privileges, including an email address, upon completion of a *User Agreement*. Board members will set an example of responsible use and will abide by district policies, regulations and procedures. Board members will abide by all pertinent state statutes regulating Public Records and Public Meetings.

External Users

Consultants, counsel, independent contractors and other persons having professional business with this school district may also be granted user privileges at the discretion of the superintendent or designee, subject to completion of a *User Agreement* and for the sole, limited purpose of conducting business with the school. External users must abide by all laws, district policies, regulations or procedures.

Privacy

A user does not have a legal expectation of privacy in the user's electronic communications or other activities involving the district's technology resources.

All district technology resources are considered district property. The district may maintain or improve technology resources at any time. The district may remove, change or exchange hardware or other between buildings, classrooms, employees, students or any other user at any time without prior notice. Authorized district personnel may load or delete programs or information, install new equipment, upgrade any system or enter any system to correct problems at any time.

The district may examine all information stored on district technology resources at any time. The district may monitor employee and student technology usage. Electronic communications, all data stored on the district's

technology resources and downloaded material, including files deleted from a user's account, may be intercepted, accessed or searched by district administrators or designees at any time.

Violations of Technology Usage Policies and Procedures
Use of the district's technology resources is a privilege, not a right. A user's privileges may be suspended pending an investigation concerning the use of the district's technology resources. Any violation or district policies, regulations or procedures regarding technology may result in temporary, long-term or permanent suspension of user privileges.

The administration may use discretionary measures to enforce district policies, regulations and procedures. Employees may be disciplined or terminated, and students suspended or expelled for violating the district's policies, regulations and procedures. Any attempted violation of district policies, regulations or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation.

Sanctions:
1) Violations may result in loss of access.
2) Additional disciplinary action may be determined at the building level in line with existing district and/or building discipline policies and/or procedures.
3) When appropriate, law enforcement agencies may be involved.

Damages:
All damages uncured by the district due to the misuse of the district's technology resources, including the loss of property and staff time, will be charged to the user. District administrators have the authority to sign any criminal complaint regarding damage to district technology.

General Rules and Responsibilities:
The following rules and regulations will be followed by all users of the district technology resources:
1. Applying for a user ID under false pretenses is prohibited.
2. Using another person's user ID and/or password is prohibited.
3. Sharing one's user ID and or password with any other person is prohibited. A user will be responsible for actions taken by any person using the ID and/or password assigned to the user.
4. Deleting, examining, copying or modifying files and/or data belonging to other users without their prior consent is prohibited.
5. Mass consumption of technology resources that inhibits use by others is prohibited.
6. Non-educational Internet usage is prohibited except for reasonable, incidental personal purposes.
7. Use of district technology for soliciting, advertising, fundraising, commercial purposes or for financial gain is prohibited, unless authorized by the district.
8. Use of district technology for political lobbying as defined under federal or state law is prohibited; however, users may use the system to communicate with elected representatives and to express their opinion on political issues.
9. Accessing fee services without permission from an administrator is prohibited. A user who accesses such services without permission is solely responsible for all charges incurred.
10. Users are required to obey all laws, including criminal, copyright, privacy, defamation and obscenity laws. The school district will render all reasonable assistance to local, state or federal officials for the investigation and prosecution of persons using district technology in violation of any law.

11. Accessing, viewing or disseminating information using district resources, including e-mail or Internet access, that is pornographic, obscene, child pornography, harmful to minors, obscene to minors, libelous, pervasively indecent or vulgar, or advertising any product or service not permitted to minors is prohibited.
12. Accessing, viewing or disseminating information on any product or service not permitted to minors is prohibited unless under the direction and supervision of district staff for curriculum-related purposes.
13. Accessing, viewing or disseminating information using school or district resources, including e-mail or Internet access, that constitutes insulting or fighting words, the very expression of which injures or harasses other people (e.g., threats of violence, defamation of character or of a person's race, religion or ethnic origin); presents a clear and present likelihood that, because of their content or their manner of distribution, they will cause a material and substantial disruption of the proper and orderly operation and discipline of the school or school activities; or will cause the commission of unlawful acts or the violation of lawful school regulations is prohibited.
14. Any use that has the purpose or effect of discriminating or harassing any person or persons on the basis of race, color, religion, sex, national origin, ancestry, disability, age, pregnancy or use of leave protected by the Family and Medical Leave Act or the violation of any person's rights under applicable laws is prohibited.
15. Any unauthorized, deliberate or negligent action that damages or disrupts technology, alters its normal performance or causes it to malfunction is prohibited, regardless of the location or the duration of the disruption.
16. Users may only install and use properly licensed software, audio or video media approved for use by the district. All users will adhere to the limitations of the district's technology licenses. Copying for home use is prohibited unless permitted by the district's license and approved by the district.
17. At no time will district technology or software be removed from the district premises, unless authorized by the district.
18. Software that interferes with the reliable operation of the network and its systems or that attempts to bypass security and capture data is not allowed. Examples of such software include, but are not limited to, viruses that cause denial of service attacks and keystroke capture applications installed without the user's knowledge.
19. All users will use the district's property as it was intended. Technology or technology hardware will not be lifted, moved or relocated without permission from an administrator or designee. All users will be held accountable for any damage they cause to district technology resources.
20. All damages incurred due to the misuse of the district's technology will be charged to the user. The district will hold all users accountable for the damage incurred and will seek both criminal and civil remedies, as necessary.
21. Electronic resources provided for home access are for the exclusive use of Bruneau/Grand View School District #365 students, staff and Board of Education members.
22. WebPages by teachers shall be hosted on servers maintained by the district or on an approved site. Content of webpage hosted on school websites needs to be education/focused.

Technology Security and Unauthorized Access

All users shall immediately report any security problems or misuse of the district's technology resources to a teacher or administrator.

No person will be given access to district technology if he or she is considered a security risk by the superintendent or designee.

1. Use of district technology resources in attempting to gain or gaining unauthorized access to any technology system or the files of another is prohibited.
2. Use of district technology to connect to other systems, in evasion of the physical limitations of the remote system, is prohibited.
3. The unauthorized copying of system files is prohibited.
4. Intentional or negligent attempts, whether successful or unsuccessful, to interfere with the ability of others to utilize any district technology are prohibited.
5. Any attempts to secure a higher level of privilege on the technology resources without authorization are prohibited.
6. The introduction of computer "viruses," "hacking" tools or other disruptive/destructive programs into a school or district computer, network or any external networks is prohibited.

Online Safety -- Disclosure, Use and Dissemination of Personal Information

1. All students will be instructed on the dangers of sharing personal information about themselves or others over the Internet.
2. Student users are prohibited from sharing personal information about themselves or others over the Internet, unless authorized by the district.
3. Student users shall not agree to meet with someone they have met online without parental approval.
4. A student user shall promptly disclose to his or her teacher or another school employee any message the user receives that is inappropriate or makes the user feel uncomfortable.
5. Users shall receive or transmit communications using only district-approved and district-managed communication systems. For example, users may not use messaging, videoconferencing or chat services, except in special cases where arrangements have been made in advance and approved by the district.
6. All district employees will abide by state and federal law, Board policies and district rules including, but not limited to, the Federal Educational Rights and Privacy Act (FERPA) when communicating information about personally identifiable students.
7. Employees shall not transmit confidential student information using district technology, unless designated for that use. Employees will take precautions to prevent negligent disclosure of student information or student records.
8. No curricular or non-curricular publication distributed using district technology will include the address, phone number or e-mail address of any student.

Electronic Mail

A user is responsible for all e-mail originating from the user's ID or password.

1. Forgery or attempted forgery of e-mail messages is illegal and is prohibited.
2. Unauthorized attempts to read, delete, copy or modify e-mail of other users are prohibited.
3. Users are prohibited from sending unreasonable amounts of unsolicited electronic mail unless the communication is a necessary, employment-related function or an authorized publication.
4. All users must adhere to the same standards for communicating online that are expected in the classroom and that are consistent with district policies, regulations and procedures.

Exceptions

Exceptions to district rules will be made for district employees or agents conducting an investigation of a use that potentially violates the law, district policies, regulations or procedures. Exceptions will also be made for

technology administrators who need access to district technology resources to maintain the district's resources or examine and delete data stored on district computers as allowed by the district's retention policy.

Waiver

Any user who believes he or she has a legitimate reason for using the district's technology in a manner that may violate any of the district's adopted policies, regulations and procedures may request a waiver from the building principal, superintendent or their designees. In making the decision to grant a waiver to a student, the administrator shall consider the purpose, age, maturity and level of supervision involved.

No Warranty/No Endorsement

The district makes no warranties of any kind, whether expressed or implied, for the services, products or access it provides. The district's technology resources are available on an "as is, as available" basis.

The district makes no guarantee that the functions or the services provided by or through the district technology system will be error-free or without defect. The district will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information obtained through or stored on the system. Bruneau/Grand View School District #365 will not be responsible for financial obligations arising through the unauthorized use of the system.

All opinions, advice, services and all other information expressed by students, staff, information providers, service providers, or other third party personnel on the district technology system are those of the individual and do not represent the views or position of Bruneau/Grand View School District #365 unless these parties are acting in an official capacity, within the limits of their authority. Users will hold Bruneau/Grand View School District #365 harmless against any claim, lawsuit, or cause of action arising out of the use of the district's technology systems or connection to the Internet. Bruneau/Grand View School District #365 is not liable for any defamatory, offensive, infringing or illegal materials or conduct on the part of, or attributable to, any third party, and reserves the right to remove such materials from its web site without liability.

Technology Usage Policy

TECHNOLOGY USAGE

Bruneau/Grand View School District recognizes the educational and professional value of electronics-based information technology, both as a means of access to enriching information and as a tool to develop skills that students need.

The district's technology exists for the purpose of maximizing the educational opportunities and achievement of district students. The network is considered a limited purpose device. The professional enrichment of our staff and Board, and increased engagement of the student's families and other patrons of the district are assisted by technology, but are secondary to the ultimate goal of student achievement.

Use of technology resources in a disruptive, manifestly inappropriate or illegal manner impairs the district's mission, squanders resources and shall not be tolerated. Therefore, a consistently high level of personal responsibility is expected of all users granted access to the district's technology resources. Development of student's personal responsibility is itself an expected benefit of the district technology program.

Definitions

For the purpose of this policy and related regulation, procedures and forms, the following terms are defined:

User --any person who is permitted to by the district to utilize any portion of the district's technology resources including, but not limited to, students, employees, school Board members, and agents of the school district.

User Identification (ID) --any identifier that would allow a user access to the district's technology resources or to any program including, but not limited to, e-mail, and Internet access.

Password – a unique word, phrase, or combination of alphabetic, numeric, and non-numeric characters used to authenticate a user ID as belonging to a user.

Technology Administration

The superintendent or designee shall create rules and procedures governing technology usage in the district to support the district's policy, as needed.

The superintendent or designee shall assign trained personnel to maintain the district's technology in a manner that will protect the district from liability and will protect confidential student and employee information retained or accessible through district technology resources.

Trained personnel shall establish a retention schedule for the regular archiving and deletion of data stored on district technology resources in accordance with applicable law. Administrators of computer resources may suspend access to and/or availability of the district's technology resources to diagnose and investigate network problems or potential violations of the law or district policies, regulations, and procedures.

User Identification and Network Security

The district's technology resources may be used by authorized students, employees, school Board members, and other persons such as consultants, legal counsel, and independent contractors. Use of the district's technology resources is a privilege, not a right. No student, employee, or other potential user will be given an ID, password, or other access to district technology if he/she is considered a security risk by the superintendent or designee.

Users must adhere to district policies, regulations, procedures, and other district guidelines. All users shall immediately report any security problems or misuse of the district's technology resources to an administrator or teacher.

User Agreement and Privacy

All users must have and appropriately signed *User Agreement* on file with the district before they are allowed access to district technology resources. All users must agree to follow the district's policies, regulations, and procedures.

In addition, all users must recognize that they do not have a legal expectation of privacy in any electronic communication or other activities involving the district's technology. A user ID with e-mail access, if granted, is provided to users of this district's network and technology resources only on condition that the user consents in his or her *User Agreement* to interception of or access to all communications accessed, sent, received, or stored using district technology.

Content Filtering and Monitoring

The district will monitor the on-line activities of minors and operate a technology protection measure ("filtering/blocking device") on the network and/or all computers with Internet access, as required by law. The filtering/blocking device will attempt to protect against access to visual depictions that are obscene, harmful to minors and child pornography, as required by law. Because the district's technology is a shared resource, the filtering/blocking device will apply to all computers with Internet access in the district. Filtering/Blocking devices are not foolproof, and the district cannot guarantee that users will never be able to access offensive materials using district equipment. Evasion or disabling, or attempting to evade or disable, a filtering/blocking device installed by the district is prohibited.

The superintendent, designee or the district's technology administrator may disable the district's filtering/blocking device to enable an adult user access for bona fide research or for other lawful purposes. In making decisions to disable the district's filtering/blocking device, the administrator shall consider whether the use will serve a legitimate educational purpose or otherwise benefit the district.

Closed Forum

The district's technology resources are not a public forum for expression of any kind and are to be considered a closed forum to the extent allowed by law.

The district's webpage will provide information about the school district, but will not be used as an open forum. The district's webpage may include the district's address, telephone number and an e-mail address where members of the public may easily communicate concerns to the administration and the Board.

All expressive activities involving district technology resources that students, parents and members of the public might reasonably perceive to bear the imprimatur of the school and that are designed to impart particular knowledge or skills to student participants and audiences are considered curricular publications. All curricular publications are subject to reasonable prior restraint, editing and deletion on behalf of the school district for legitimate pedagogical reasons. All other expressive activities involving the district's technology are subject to reasonable prior restraint and subject matter restrictions as allowed by law and Board policies.