## Administrative Procedure EHB-AP(1): TECHNOLOGY USAGE - (Technology Safety)

**Status:** ADOPTED

**Original Adopted Date:** 08/15/2001 **| Last Revised Date:** 11/15/2017

**Student Users**

All student users and their parents/guardians must sign or electronically consent to the district's User Agreement prior to accessing or using district technology resources, unless otherwise excused by this policy or the superintendent or designee. Students who are 18 or who are otherwise able to enter into an enforceable contract may sign or consent to the User Agreement without additional signatures. Students who do not have a User Agreement on file with the district may be granted permission to use the district's technology resources by the superintendent or designee.

**Employee Users**

No employee will be given access to the district's technology resources unless the employee agrees to follow the district's User Agreement prior to accessing or using the district's technology resources. 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 or procedures, hinder the use of the district's technology resources for the benefit of its students or waste district resources. Any use that jeopardizes the safety, security or usefulness of the district's technology resources or interferes with the effective and professional performance of the employee's job is considered unreasonable. Unless authorized by the employee's supervisor in advance, employees may not access, view, display, store, print or disseminate information using district technology resources that students or other users could not access, view, display, store, print or disseminate.

**External Users**

Consultants, legal counsel, independent contractors and other persons having business with the district may be granted user privileges at the discretion of the superintendent or designee after consenting to the district's User Agreement and for the sole, limited purpose of conducting business with the school. External users must abide by all laws, district policies and procedures.

**General Rules and Responsibilities**

The following rules and responsibilities will apply to all users of the district's technology resources:

1. Applying for a user ID under false pretenses or using another person's ID or password is prohibited.

2. Sharing user IDs or passwords with others is prohibited except when shared with the district's technology department for the purpose of support. Individuals who share IDs or passwords may be disciplined and will be held responsible for any actions taken by those using the ID or password. A user will not be responsible for theft of passwords and IDs, but may be responsible if the theft was the result of user negligence.

3. Deleting, examining, copying or modifying district files or data without authorization is prohibited.

4. Deleting, examining, copying or modifying files 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. Use of district technology for soliciting, advertising, fundraising, commercial purposes or financial gain is prohibited, unless authorized by the district or in accordance with policy KI. Use of district technology

resources to advocate, support or oppose any ballot measure or candidate for public office is prohibited.

7. 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.

8. Users are required to obey all laws, including criminal, copyright, privacy, defamation and obscenity laws. The 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.

9. The district prohibits the use of district technology resources to access, view or disseminate information that is pornographic, obscene, child pornography, harmful to minors, obscene to minors, libelous, or pervasively indecent or vulgar.

10. 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.

11. The district prohibits the use of district technology resources to access, view or disseminate information 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 district policies and procedures.

12. The district prohibits any use that violates any person's rights under applicable laws, and specifically prohibits any use that has the purpose or effect of discriminating against or harassing any person on the basis of race, color, religion, sex, national origin, ancestry, disability, age, genetic information, pregnancy or use of leave protected by the Family and Medical Leave Act (FMLA).

13. The district prohibits any unauthorized intentional or negligent action that damages or disrupts technology, alters its normal performance or causes it to malfunction. The district will hold users responsible for such damage and will seek both criminal and civil remedies, as necessary.

14. Users may install and use only properly licensed software and audio or video media purchased by the district or 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.

15. At no time will district technology or software be removed from district premises, unless authorized by the district.

16. All users will use the district's property as it was intended. Technology resources will not be moved or relocated without permission from a building administrator. All users will be held accountable for any damage they cause to district technology resources.

**Technology Security and Unauthorized Access**

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

2. Use of district technology resources in attempting to gain or gaining unauthorized access to any technology system or the files of another is prohibited.

3. Use of district technology to connect to other systems, in evasion of the physical limitations of the remote system, is prohibited.

4. The unauthorized copying of system files is prohibited.

5. Intentional or negligent attempts, whether successful or unsuccessful, to interfere with the ability of others to utilize any district technology are prohibited.

6. Users will be granted access privileges to district technology resources as determined appropriate by the superintendent or designee. Any attempt to secure a higher level of privilege without authorization is prohibited.

7. The introduction of computer viruses, hacking tools or other disruptive or destructive programs into a district computer, network or any external networks is prohibited.

**Online Safety and Confidentiality**

Curricular or noncurricular publications distributed using district technology will comply with the law and Board policies on confidentiality.

All district employees will abide by state and federal law, Board policies and district rules when using district technology resources to communicate information about personally identifiable students. Employees will take precautions to prevent negligent disclosure of student information or student records.

All students will be instructed on the dangers of sharing personal information about themselves or others over the Internet and are prohibited from sharing such information unless authorized by the district. Student users shall not agree to meet with someone they have met online without parental approval and must promptly disclose to a teacher or another district employee any message the user receives that is inappropriate or makes the user feel uncomfortable.

**Electronic Mail and Messaging**

A user is generally responsible for all e-mail and other electronic messages originating from the user's accounts; however, users will not be held responsible when the messages originating from their accounts are the result of the account being hacked.

1. Forgery or attempted forgery of electronic messages is illegal and prohibited.

2. Unauthorized attempts to read, delete, copy or modify electronic messages of other users are prohibited.

3. Users are prohibited from sending unsolicited mass e-mail or other electronic messages, unless the communication is a necessary, employment-related function or an authorized publication.

4. When communicating electronically, all users must comply with district policies, regulations and procedures and adhere to the same standards expected in the classroom.

5. Users must obtain permission from the superintendent or designee before sending any districtwide electronic messages.

**Communication Devices**

Employees and others to whom the district provides mobile phones or other electronic communication devices must use them professionally and in accordance with district policies, regulations and procedures. These devices shall not be used in a manner that would distract the employee or other user from adequate supervision of students or other job duties.

**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 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 educational purpose for using the district's technology in a manner that may violate any of the district's policies, regulations or 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 student's purpose, age, maturity and level of supervision involved.

* * * * * * *

***Note: The reader is encouraged to review policies and/or forms for related information in this administrative area.***