

### **363.2                STUDENT INFORMATION & COMMUNICATION TECHNOLOGIES ACCEPTABLE USE POLICY**

The Williams Bay Public School District is providing access to the Internet to enhance the curriculum and provide learning opportunities for all students. The district has established the Information & Communication Technologies Acceptable Use Policy to ensure appropriate use of this resource.

**Rationale:** The reasons for using the Internet as an instructional resource are:

- accessing global resources
- entering partnerships to enhance learning options
- broadening problem-solving and decision-making abilities
- broadening research capabilities by using appropriate materials
- developing higher level thinking skills
- gaining employability skills needed for the 21st century
- utilizing electronic communication for educational purposes.

Internet access will be provided for students and staff for the purpose of conducting research and communicating with others. Independent student access to the Internet will be provided only to students who have agreed to abide by this policy and its accompanying guidelines and to act in a considerate and responsible manner.

As a part of its internet safety policy, the Williams Bay Public School District will educate minors about cyber bullying awareness and response, and appropriate online behavior, including interacting with others on social networking websites and in chat rooms.

Communication on the Internet is often very public in nature. Students are responsible for good behavior in the use of computers and the Internet, just as they are in a classroom or on school property. The Board does not sanction any use of the Internet that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines. Users who disregard this policy and accompanying guidelines may have their privileges suspended or revoked, and disciplinary action taken against them. Users granted access to the Internet through the district computers assume personal responsibility and liability, both civil and criminal, for uses of the Internet not authorized by this Board policy and accompanying guidelines. When using the district's access to the Internet, users are expected to abide by the policies established by the district, which include generally accepted rules of network etiquette. These include, but are not limited to the following:

**Acceptable Use-Responsible users:**

- will follow rules of common sense or etiquette
- may use the Internet to research classroom projects and electronic mail for educational purposes only
- may use the Internet to explore other computer systems
- will respect and uphold copyright laws and all other applicable laws or regulations
- will respect the rights and privacy of others by not accessing private files
- will use the Internet in accordance with district policies relating to harassment
- may download or use streaming video or audio, or any software program only with permission of the computer director to avoid overtaxing the network
- shall use the network in such a way that would not disrupt the use of the network by others
- will follow the regulations posted in the computer lab or other areas where computers are in use
- will follow the directions of the adult in charge of the computer lab or other areas where computers are in use
- will use their school assigned email for educational purposes only

**Unacceptable Use-Responsible users shall not**

- use the Internet for any illegal purpose
- bypass or attempt to bypass the filter
- use profane, impolite, or abusive language
- access or use gambling websites
- access any computer files that do not belong to the user or use another person's password
- use the system for commercial or profitable purposes
- use the network to access, transmit, or download pornographic, offensive, harassing, or other inappropriate material
- use computers to access or lead to unauthorized access into accounts or other computer networks.
- use computers to pursue "hacking" internal or external to the district or attempt to access information that is protected by privacy laws.
- create and/or distribute a computer virus over the network
- use the network in such a way that would disrupt the use of the network by others
- deliberately or willfully cause damage to computer equipment, system, or network or assist others in doing the same
- deliberately access materials that are inconsistent with the school's code of conduct or the district's educational goals or show others how to do the same
- violate copyright or otherwise use another person's intellectual property without his or her prior approval and proper citation
- use the Internet to harass, bully, insult, or threaten others
- use an account other than their own or misrepresent their identity.
- reveal addresses, phone numbers, images, or any other personal information about self or others when using the Internet or communicating electronically.

## **Use of Online Collaboration Tools including Web Pages and Social Networking**

Certain educational Web 2.0 services (e.g., Moodle, blogs, podcasts, vodcasts, wikis) that emphasize online educational collaboration and sharing are permitted only in controlled, staff supervised settings and for valid school-related purposes. All other uses are prohibited.

Use of social networking services (e.g., Facebook, Instagram, Twitter, Tick Tok) is not permitted for students using District Systems, unless under the direct supervision of a staff member.

## **Use of Personal Electronic Devices**

During class time, students may use Personal Devices only with permission from staff members. Use of personal devices during non-instructional times (e.g. lunch and passing periods) is permitted by high school students so long as it does not interfere with educational responsibilities and so long as it does not hinder, disrupt, or consume an unreasonable amount of network or staff resources, or violate school rules, state law, federal law or Board policies. Each Building Principal, in working with their staff, may implement administrative guidelines that restrict or permit personal electronic device usage. Students are expected to follow the directives of staff members regarding the use of Personal Devices during the school day or while attending a school-sponsored activity.

The use of a Personal Devices to access the district systems will be allowed for the use of filtered internet access only. Filtered access will be consistent with that available when using a district-owned device. Bypassing or attempting to bypass this network through proxies, tethering, or other means is not allowed and will be disciplined.

File, print, and application services will not be available on the wireless public network. With staff permission, Personal Devices may be connected with a district-owned piece of equipment (i.e., LCD projector or SMART Board) for instructional purposes only and under the direction of a district staff member.

Users connecting to district systems, even those with a Personal Device, should have no expectation of privacy. The district may review and monitor accounts, without notice, to ensure responsible technology use and maintain system integrity.

The district reserves the right to confiscate and search Personal Devices if reasonable suspicion exists that district policies have been violated. The Personal Device may be turned over to law enforcement if the Personal Device has been used for an illegal purpose. Upon request, users must surrender the Personal Device in its entirety.

Users found to be in violation of district policies using a Personal Device will be subject to consequences, including disciplinary action, exclusion of the device from the district, or criminal prosecution.

In accordance with state law (§175.22, §942.08, §942.09, board policy (731.2)), under no circumstances shall any Personal Device with photographic capabilities be used in locker rooms, bathrooms, or other areas where privacy is expected. Personal Devices shall not be used to photograph students or others without their permission and shall not be used to photograph any items that are confidential (e.g., testing materials). A student who violates this section of the policy shall be subject to discipline, which may include consequences up to and including expulsion for students.

Responsibility for the care of Personal Devices and behavior while using the device belongs solely to the owner. The district is not liable for loss, damage, or misuse of any personal device including while on District property, connected to District systems, or while attending school-sponsored activities. Technical support for Personal Devices will not be available. Any assistance provided by the district to access the wireless public network shall be done in good faith and does not render the district liable for the function of any Personal Device.

#### **Use of Student Likenesses. Student Work. Student Voice on Websites**

Student Likeness: A student's likeness (photograph or video image) may be posted on a teacher, school, or district website for educational purposes unless a parent/guardian denies permission to do so through the opt-out procedure listed in this policy.

All content shall be age appropriate to safeguard students by shielding the students' identification and locations. Content may include names of individuals; however, identifying information, such as names of family members, e-mail addresses, addresses and phone numbers will remain private.

#### **Security and Safety**

In compliance with the Children's Internet Protection Act (CIPA) and other applicable laws, the district has implemented filtering/and or blocking software to restrict access to Internet sites containing child pornography, obscene depictions, or other objectionable materials harmful to minors. Nevertheless, parents/guardians are advised that a determined user may be able to gain access to services on the Internet that the Board has not authorized for educational purposes and are responsible for setting and conveying the standards that their children should follow when using the Internet. In fact, it is impossible to guarantee students will not gain access through the Internet to information and communications that they and/or their parents/guardians may find offensive, inappropriate, objectionable, or controversial. The School District of Williams Bay does not condone the use of such material. Students must have a specific information objective in mind before they will be allowed to use Internet resources.

In order to ensure the systems are being used for educational purposes, the School District of Williams Bay reserves the right to inspect all data stored in public or private areas of networked or individual storage systems of any kind, without notice or warning, and at any time or for any reason. No District user should have any expectation of privacy as to his or her Internet usage, or the privacy of any electronic mail message, file, download, note or other data stored on or transmitted or received through any District computing facility.

Access to the Internet via the Williams Bay School District is a privilege, not a right. This privilege may be restricted at any time for use not consistent with the educational goals of the district.

Students who commit any of the above listed acts of misconduct will be disciplined in one or more of the following ways:

- the device will be confiscated
- the student's parents will be contacted
- the student will be given limited access to school telecommunications equipment, networks, and service
- the student will be denied access to school telecommunications equipment, networks, and services
- the student will be required to pay for all property damage
- the student will receive an in-school suspension
- the student will receive an out-of-school suspension
- the student will be denied access to all district owned computer equipment, networks, and services
- the appropriate law enforcement agencies will be notified
- the student will be recommended for expulsion

### **Notification to Users**

Reference to the District's acceptable use policy and rules shall be included in every student ~~and staff~~ handbook. If a parent/guardian chooses to deny Internet access or access to the wireless public network, or permission for the student's work, voice, likeness, or name posted on a website, they must opt Out within Skyward.

APPROVED: June 10, 2002

REVISED: January 13, 2003, November 8, 2010, July 16, 2012, July 10, 2017

REVIEW: February 22, 2021

REVISED: July 26, 2021

## Opt-Out: Student Likeness, Work, or Voice on District Websites

From time to time the Williams Bay School District posts student likeness (e.g. photographs, video clips), work (e.g. written work, art work) and voice (e.g. podcasts, performances) on its district, school, and teacher websites.

A parent/guardian who chooses to deny permission to post their child's likeness, work, or voice on any website owned and operated by the Williams Bay School District under the domain

**\*.williamsbayschools.org** must complete the Opt-Out form below and return it to the District Administrator's Office at 500 West Geneva Street, Williams Bay, WI 53191.

---

(Please Print) Student's Last Name First Name M.I.

---

Address City Zip Code

---

Current Grade Level School

I, the undersigned, understand the information above and deny permission for my child's likeness, work, voice to be posted on any website owned and operated by the Williams Bay School District under the domain **\*.williamsbayschools.org**

---

Authorized Signature for Minor Student / Print Your Name

---

Relationship to Student / Daytime Phone / Date (Required)