Richmond School District Policy Statement **Policy #: 363.2**
Internet Safety and Acceptable Use

The District provides students with access to information technology and communication resources to accomplish the District's vision of teaching, learning, and public service operations. Uses shall be related to educational programs or other operations of the District.

The district administrator or designee shall be responsible for the maintenance and enforcement of rules and procedures concerning the acceptable, safe, and responsible use of the District's Internet access infrastructure and other technology-related District resources by any person who is authorized to use the District's systems and equipment, including any student, District employee, District official, or other authorized user. To the extent appropriate to various groups of users, and with such additions as the administration deems necessary or appropriate, those rules and procedures shall:

1. Provide notice regarding the District's retention of ownership, control, and oversight of the District's technology and network equipment and resources. Specifically, to the extent not prohibited by law, and at all times and without further notice:

    a. Individual users are subject to direct and regular District oversight of, and District access to, any and all data, files, communications, or other material that they create, store, send, delete, receive or display on or over the District's Internet connection, network resources, file servers, computers or other equipment.

    b. All aspects of any individual's use of the District's technology-related equipment and resources, including any online activities that make use of District-provided Internet access, are subject to monitoring and tracking by District officials.

    c. Except as to any privacy rights that independently exist under state or federal law, no person who accesses and uses the District's electronic networks and other technology-related equipment and resources does so with an expectation that any privacy right exists that would prevent District officials from (1) monitoring the person's activities; or (2) accessing equipment, data, communications, and other materials as described above.

2. Provide notice to users that their use of District technology resources is solely at their own risk regarding possible damage to, or any other potential loss of, data, content, software, or equipment. The District makes no promises or warranties to users regarding potential damage or other loss.

3. Prohibit the use of the District's technology-related resources by any person who has not been authorized as a user by school officials.

4. Establish rules and expectations related to maintaining a safe, appropriate and effective learning environment.

5. Confirm that all District policies prohibiting bullying, harassment, and discrimination apply with full force to an individual's online and other technology-based activities and communications.

6. Address and prohibit the unauthorized collection, disclosure, use and dissemination of personal and personally-identifiable information regarding students and minors, as applicable to technology-based resources.

7. Address employees' obligations regarding the proper retention of District records, maintaining the confidentiality of student records, and avoiding inappropriate disclosures of District records.

8. Establish rules and expectations related to accessing and using systems, networks, and data appropriately, including rules (a) prohibiting the use of District resources to access and/or transmit inappropriate material via the Internet, electronic mail, or other forms of electronic communications; and (b) prohibiting unauthorized access to systems, networks, and data.

9. Establish rules and expectations related to academic integrity.

10. Establish rules and expectations related to copyright law, licensing agreements, and related issues.

11. Establish rules and procedures related to maintaining and securing District property and resources.

12. Establish rules and procedures related to requests to temporarily adjust levels of Internet filtering/blocking where there is a demonstrated educational purpose and the request is otherwise consistent with District policies and applicable law.

13. Provide direction and processes for the reporting of violations of the policies, rules and procedures that govern the acceptable, safe, and responsible use of the District's technology-related resources.

14. Provide notice to users regarding possible consequences for violations of the policies, rules and procedures that govern the acceptable, safe, and responsible use of the District's technology-related resources. Consequences may include the suspension, restriction or revocation of the privilege of use or access, the imposition of other disciplinary action by the District, and/or referral to law enforcement.

15. Provide a means for documenting each user's receipt and acceptance of the terms and conditions under which they may be authorized to use the District's technology-related resources.

The administration shall take steps to ensure that instruction or training activities and reasonable structural and systemic supports are in place to facilitate and enforce individual users' compliance with the District's policies, rules, and procedures that govern the acceptable, safe, and responsible use of the District's technology-related resources. Appropriately limiting a user's access rights to be consistent with the individual's role and authority, and running up-to-date anti-virus and other protective software are examples of structural and systemic supports that can facilitate the acceptable, safe, and responsible use of the District's technology-related resources. Ultimately, however, a cornerstone of the District's expectations for individual users is that use of District technology resources is a privilege that requires each user to take an appropriate degree of personal responsibility for following District rules and procedures and for using sound judgment in his/her communications and other technology-related personal conduct and activities.

Additional Provisions Regarding Internet Safety

Internet access is an essential component of the District's technology program and technology infrastructure for the advancement and promotion of high-quality operations, instruction, and student learning. Internet access provides students and staff with statewide, national and global communications opportunities; rich sources of data, information, and research; as well as a wealth of adaptable instructional tools that build and enhance skills. The ability to appropriately locate, navigate and utilize Internet-based resources is itself an essential skill for all students and instructional staff.

Further, from an instructional point of view, students need to be capable of critically reviewing and analyzing Internet-based resources to determine their accuracy, credibility, and weight as a sound authority on the subject matter that is being addressed.

However, Internet access is neither inherently nor exclusively a beneficial educational resource. Internet access can be used—inadvertently or, in some cases, purposefully—to facilitate inappropriate, harmful, deceptive, and even illegal activities and communications. Further, notwithstanding reasonable efforts at prevention, there is still a risk that a student may, at some time, be exposed to particular content or participate in particular activities or communications that the District would consider harmful, deceptive, or otherwise inappropriate, or that a parent or guardian may find objectionable.

Consistent with applicable federal laws, the Board of Education believes that the best approach to student Internet safety involves a combination of technology protection measures, monitoring, and instruction. The District's comprehensive approach to student Internet safety shall take into account the differing ages and instructional levels of the students in the District.

It shall be the responsibility of the district administrator in consultation with such designees as they deem appropriate, to:

1. Ensure that the District's systems and equipment that provide access to the Internet make active use of technology protection measures designed to block or filter Internet access to visual depictions that are: (a) obscene; (b) pornographic; or (c) as to computers and other devices that may be accessed by students or other minors, otherwise harmful to minors. Filtering, blocking or other protective technologies will also be used to decrease the likelihood that student users of the District systems and equipment might access materials or communications, other than visual depictions, that are inappropriate for students.

2. Develop and implement procedures that provide for the monitoring of students' and other authorized users' activities when using District-provided equipment or District-provided network access or Internet access. Such monitoring may sometimes take the form of direct supervision of students' and minors' online activity by school personnel. To the extent consistent with applicable law, other examples of such monitoring activities may include the use of applications, services, equipment, or other methods by which school personnel can:

    a. track and review users' Internet histories, online communications, uploaded, downloaded, saved or deleted data, files, applications, programs or other content, or other online activities;

    b. track and log network access and use by any person or under any account; or

    c. monitor fileserver space utilization by District users by, for example, file size, file type, file content and/or file function.

3. Develop and implement an instructional program that is designed to educate students about acceptable and responsible use of technology and safe and appropriate online behavior, including (a) safety and security issues that arise in connection with various forms of electronic communication; (b) information about interacting with other individuals on social networking sites and in chat rooms; and (c) cyberbullying awareness and response. Such educational activities shall vary by the instructional level of the students and shall include (but shall not consist exclusively of)

reinforcement of the provisions of the District's specific rules regarding student's acceptable and responsible use of technology while at school.

Building principals and their designees shall have responsibility, within their respective schools, for overseeing the day-to-day implementation of the District's policies, rules and guidelines regarding the acceptable, safe, and responsible use of technology resources.

Legal References:

Wisconsin Statutes

Section 120.12(1) [Board of Education duty; care, control and management of school property and affairs of district]
Section 120.13(1) [Board of Education power to adopt conduct rules and discipline students]
Section 120.18(1)(i) [report on technology used in the district]
Section 943.70 [computer crimes]
Section 947.0125 [unlawful use of computerized communication systems]
Section 995.55 [access to personal Internet accounts]

Wisconsin Administrative Code

Section PI 8.01(2)(k) [integration of technology literacy and skills in curriculum]

Federal Laws and Regulations

Children's Internet Protection Act (CIPA) and Neighborhood Children's Internet Protection Act (NCIPA) [policy and other requirements related to Internet safety]
Protecting Children in the 21st Century Act [Internet safety policy requirement; education of students regarding appropriate online behavior]
Children's Online Privacy Protection Act (COPPA) [parent control over personal information collected by websites from their children]
E-rate funding requirements [technology plan and other requirements]

Cross References: Student Handbook

Adopted: 11/10/08
Reviewed: 1/10/11, 3/12/18