MARANA
UNIFIED SCHOOL DISTRICT

Governing Board Agenda Item

Meeting Date: October 2, 2025

From: Kristin Reidy, Assistant Superintendent

Subject: Policy Revision

Priority: To provide rigorous, relevant, and innovative academics

Consent   []   Action   [X]   Discussion []

Background:

The following policy is being revised:

Policy IJNDB, Use of Technology Resources in Instruction

House Bill 2484 added A.R.S. 15-120.05 relating to student access to the internet, student use of wireless communication devices, policies and procedures, annual notice, and definitions for public schools. Policy IJNDB and IJNDB-R incorporate the new mandates and headings were added to improve clarity.

This Marana Unified School District specific policy and regulation have been approved by District legal counsel.

Recommended Motion:

I move that the Governing Board approve revisions to Policy IJNDB, Use of Technology Resources in Instruction, as presented.

Approved for transmittal to the Governing Board: _____
                                                                    Dr. Daniel Streeter, Superintendent

Questions should be directed to: Kristin Reidy, Assistant Superintendent
Phone: (520) 682-4757

IJNDB
USE OF TECHNOLOGY RESOURCES
IN INSTRUCTION

Appropriate use of Electronic
Information Services

Purpose

This policy defines the acceptable uses of technology and technological education efforts within the Marana Unified School District. The District may provide electronic information services (EIS) to qualifying students, teachers, and other personnel who attend, utilize, or are employed by the District. Every effort will be made to ensure that electronic information resources are used only in support of administrative, informational, instructional, communication, research, and educational objectives of the District.

General

The District may log the use of all systems and monitor all District-owned electronic information system utilization. Accounts may be closed and files may be deleted at any time. The District is not responsible for any service interruptions, changes, or consequences. *Good-faith efforts* will be made to maintain all systems in good operating condition, but systems will inevitably fail, with resulting inconvenience or loss to users. The District reserves the right to establish rules and regulations as necessary for the efficient operation of the electronic information services.

The District does not assume liability for information retrieved via EIS, nor does it assume any liability for any information lost, damaged, or unavailable due to technical or other difficulties.

The parent(s)/guardian(s) of each student user shall sign a use agreement annually before the student is granted access to District technological systems. This use agreement addresses issues of privacy, ethical use of information regarding intellectual property, and the prohibition against using the network for illegal or inappropriate activities. The smooth operation of the network relies upon the proper conduct of users, who must adhere to all rules.

The Superintendent will be responsible for establishing and enforcing the District's electronic information services rules and procedures for appropriate use.

Definition of District Electronic
Information Services

District electronic information services (EIS) include but are not limited to networks (e.g., LAN, WAN, Internet), computers (desktops, notebooks, laptops, netbooks, tablets, etc), databases, electronic mail, web services, and in general, any computer-accessible sources of information. These include but are not limited to hard drives, ~~tapes, floppy disks, optical discs (CDs, DVDs, Blu-ray),~~ flash drives, or any other electronic sources.

Scope

To assure that District EIS resources are used in an appropriate manner and for the educational purposes intended, the District will require anyone who uses the District EIS resources to follow its rules and procedures for appropriate use. Annually, each user will be required to sign a Use of Technology Resources in Instruction Agreement. Anyone who misuses, abuses, or chooses not to follow the EIS rules and procedures may be denied access to the District's EIS and may be subject to disciplinary action. This policy applies to qualifying students, teachers, and other personnel who attend, utilize, or are employed by the District, and its scope includes the following areas:

A. Computer access.

B. District network access.

C. Internet access.

D. Electronic mail.

E. Web services.

Personal equipment (flash drives, etc.) physically connected to the District's electronic information services, including the District's network, is also subject to this policy.

**Acceptable Use of District
EIS Resources**

In an effort to support the educational and research goals of the Marana Unified School District, while also complying with child protection laws, a network comprised of limited internet access has been designed and implemented. This network provides access to computing resources that support student management, business management, and educational research.

The District's network can be accessed via physical network connection, wireless network access (or WiFi), or remotely. These services are provided to support research and education. Uses for other purposes are not permitted.

Specifically acceptable uses:

A. For approved school/community communication and information activities, including but not limited to education-related web pages and bulletin boards.

B. Communication and exchange for professional development, to maintain currency, or to debate issues in a field or subfield of knowledge.

C. Use for professional society, university association, government advisory, or standards actively related to the user's research and education activities.

D. Use in applying for and administering grants or contracts for research or instruction, for District-related fund-raising, or for District-related public-relations activities.

E. Any other administrative communications or activities in direct support of research or education.

F. Use for student management and assessment.

G. Use for bookstores and activity accounting.

H. Communication incidental to otherwise acceptable use. Reasonable occasional personnel use of a casual nonbusiness nature by staff members and students will be permitted as long as such use is incidental in nature, violates no other principle of District EIS policies, regulations, rules, does not interfere with the efficient operation of the network, and does not detract from educational or job performance.

I. Student instructional and research activities.

J. Any other activity specifically approved by appropriate administrators.

K. Accessing any portion of the District's wireless network with personally-owned equipment (laptop, notebook, desktop, tablet, etc.) is permissible. End-users electing to do so should be vigilant in ensuring that their equipment is free of viruses, and in general, any malware.

Specifically unacceptable uses:

A. Submitting, publishing, displaying, storing or retrieving any material that the individual knows, or should know, is defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.

B. Use in for-profit activities or by for-profit organizations, unless specific permission is given by the Superintendent, such as for advertising that benefits the District and/or District students.

C.   Use of District EIS resources to engage in "hacking," and other unlawful activities or to engage in the unauthorized disclosure, use and dissemination of personal identification information regarding minors;

C D. Use of District EIS resources for personal or private reasons is prohibited. Reasonable occasional personnel use of a casual non-business nature by staff members and students will be permitted as long as such use is incidental in nature, violates no other principle of District EIS policies, regulations, rules, does not interfere with the efficient operation of the network, and does not detract from educational or job performance.

D E. Use of District EIS resources in a manner prohibited by the Use of Technology Resources in Instruction regulation.

E F. No one shall use Ethernet (or network) cables to physically connect any computer (laptop, notebook, desktop, tablet, etc.) to the District network or equipment without the knowledge and approval of the Information Technology Department. The Director of Information Technology may place restrictions on the use of personally-owned equipment to protect the Districts' network.

Generative Artificial Intelligence Programs

The proper use of Artificial Intelligence (AI) programs can be effective at enhancing student learning and can prepare students with the competencies and knowledge needed in the digital age. Its use should also be guided by responsible and ethical considerations, including mitigating bias, promoting transparency, and providing AI benefits to all students. Use of AI programs in the classroom should be approved by the site or District administrator, and teachers' instructions and expectations should guide the classroom use of AI. Teachers should include relevant lessons on correct and responsible use of AI, and students should be taught standards regarding plagiarism and source citation and should use these guidelines if AI is used for a school assignment. AI use should be guided and monitored by teachers and/or administrators and should align with the District's guidelines and policies, including any relevant student rules/responsibilities. AI resources should be available to all students, including those with disabilities and English language learners. Use of an AI system should comply with the Family Educational Rights and Privacy Act (FERPA) and should support data privacy and security.

Filtering and Internet Safety

The District shall provide for technology protection measures that are designed to protect against Internet access by both adults and minors to visual depictions that are obscene, pornographic, or, with respect to use of the computers by students, harmful to students. Such protective measures shall also include monitoring the online activities of staff and students alike.

Limits, controls, and prohibitions shall be placed on student:

A. Access to inappropriate matter.

B. Safety and security in direct electronic communications.

C. Unauthorized online access or activities.

D. Unauthorized disclosure, use and dissemination of personal information.

Wireless Communication Devices

It is the policy of the District to limit student use of wireless communication devices during the school day. All students may use wireless communication devices for the following purposes:

A. for educational purposes, as directed by the student's teacher.

B. during an emergency.

C. as needed for a medical condition.

Use is other circumstances is dependent upon the grade level of the student. See Regulation IJNDB-R.

Education, Supervision and Monitoring

It shall be the responsibility of all District employees to be knowledgeable of the Board's policies and administrative guidelines and procedures. Further, it shall be the responsibility of all employees, to the extent prudent to an individual's assignment to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, and the Protecting Children in the 21st Century Act and A.R.S. 15-120.05.

The Superintendent shall provide for appropriate training for District employees and for students who use the District's computer network and have access to the Internet. Training provided shall be designed to promote the District's commitment to:

A. the standards and acceptable use of the District's network and Internet services as set forth in District policy;

B. student safety in regards to use of the Internet, appropriate behavior while using, but not limited to, such things as social ~~networking Web sites~~ media platforms, online opportunities and chat rooms; and cyberbullying awareness and response; and compliance with E-rate requirements of the Children's Internet Protection Act.

While training will be subsequently provided to employees under this policy, the requirements of the policy are effective immediately. Employees will be held to strict compliance with the requirements of the policy and the accompanying regulation, regardless of whether training has been given.

The Superintendent is responsible for the implementation of this policy and for establishing and enforcing the District's electronic information services guidelines and procedures for appropriate technology protection measures (filters), monitoring, and use.

Parent Notification

~~Parents~~ At the beginning of each school year, parents will be notified of the policies regarding the use of technology and the Internet while at school. Parents will also be notified of their ability to prohibit the student from the use of technology and the Internet while at school in which covered information may be shared with an operator pursuant to A.R.S. 15-1046. This does not apply to software or technology that is used for the daily operations or administration of a local education agency or Arizona Online instruction programs authorized pursuant to A.R.S. 15-808.

Definitions

A. "School day" means periods of time when students are at school, including meals, passing periods and recess.

B. "Social media platform" means a website, computer application or other digital platform that is used for social networking and creating or exchanging virtual content.

C. "Wireless communication devices" includes personal devices and devices that are provided by the school.

Adopted: ~~September 12, 2024~~ October 2, 2025

LEGAL REF.:
A.R.S.
13-2316
13-3506.01
13-3509
15-341
15-808
15-1046
34-501
34-502
20 U.S.C. 1232g, the Family Educational Rights and Privacy Act
20 U.S.C. 1232h, the Protection of Pupil Rights Amendment
20 U.S.C. 1400 et seq., Individuals with Disabilities Education Act
20 U.S.C. 6301 et seq., Every Student Succeeds Act of 2015
20 U.S.C. 9134, The Children's Internet Protection Act
47 U.S.C. 254, Communications Act of 1934 (The Children's
    Internet Protection Act)
16 CFR Part 312, Children's Online Privacy Protection Rule (COPPA)

REGULATION

USE OF TECHNOLOGY RESOURCES
IN INSTRUCTION

**(Acceptable use of Technology
Resources in Instruction)**

**Administrative Regulation -
EIS and Web Services**

Use of the District's electronic information services (EIS) must be in accordance with the following rule and support the education, research, and educational goals of the District. Filtering, monitoring, and access controls shall be established to:

A. Limit and restrict access by minors to ~~inappropriate~~ content on the Internet and World Wide Web that is inappropriate for and/or harmful to minors.

B. Limit the use of wireless communication devices by students during the school day.

~~B~~ C. Monitor the safety and security of minors when using direct electronic communications.

~~C~~ D. Monitor for unauthorized access, including so-called "hacking," and other unlawful activities by minors online.

Content Filtering

A content filtering program or similar technology shall be used on the networked electronic information services (EIS). The technology shall, at a minimum, be designed to limit access to obscene, profane, sexually oriented, harmful, and illegal materials, and shall comply with the Children's Internet Protection Act (CIPA). Should a District adult employee have a legitimate need to obtain information from an access-limited site, the Superintendent may authorize, on a limited basis, access for the necessary purpose specified by the employee's request to be granted access.

Monitoring

As a means of providing safety and security in direct electronic communications and to prevent abuses to the appropriate use of electronic equipment, all computer access to the Internet through the District electronic information services (EIS) shall be monitored at a minimum periodically ~~or~~ and randomly through in-use monitoring or review of usage logs.

Access Control

Individual access to District EIS resources shall be by authorization only. Designated personnel may provide authorization to students and staff who have completed and returned an electronic information resource agreement annually. The Superintendent may give authorization to other persons to use the EIS.

A user who violates the EIS rules and procedures may be denied access to the District's EIS and may be subject to disciplinary action. Accounts may be closed and files may be deleted at any time.

Acceptable Use

Each user of District EIS shall:

A. Use the EIS to support educational objectives consistent with the educational goals and objectives of the District.

B. Agree not to submit, publish, display, store or retrieve any material that the individual knows, or should know, is defamatory, factually inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.

C. Abide by all copyright and trademark laws and regulations.

D. Agree not to let anyone use their District account or to give out their username and password.

E. Take responsibility for assigned personal and District accounts, including password protection. The Information Technology Director reserves the right to establish end-user security procedures to protect the network from unauthorized access. This includes but is not limited to strong password and workstation rules.

F. Follow all District EIS policies, regulations and rules, take all responsible precautions, including password maintenance and file and directory protection measures, to prevent the use of personal and District accounts and files by unauthorized persons.

G. Not reveal home addresses, personal phone numbers or personally identifiable data of any person unless authorized to do so by designated school authorities.

H. Understand and agree that electronic mail or direct electronic communication is not private and may be read and monitored by designated school authorities.

I. Not use the District's network in any way that would disrupt the use of the network by others, including but not limited to spamming, mass forwarding of e-mails, broadcasting, or file sharing.

J. Not use District EIS for personal or private reasons except as follows: Reasonable occasional personnel use of a casual nonbusiness nature by staff members and students will be permitted as long as such use is incidental in nature, violates no other principle of District EIS policies, regulations, or rules does not interfere with the efficient operation of the network and does not detract from educational or job performance.

K. Not use Ethernet (or network) cables to physically connect any computer (laptop, notebook, desktop, tablet, etc.) to the District network or equipment without the knowledge and approval of the Information Technology Department. The Director of Information Technology may place restrictions on the use of personally-owned equipment to protect the District's network.

L. Be vigilant to ensure that if any personally-owned equipment (laptop, notebook, desktop, tablet, etc.) is used to ~~A~~access the District's wireless network or equipment ~~with personally-owned equipment (laptop, notebook, desktop, tablet, etc.), and to the best of my ability, will be vigilant to ensure that~~ such equipment is free of viruses, and ~~in general, free of~~ any malware.

M. Not use District EIS for commercial purposes, unless specific permission is given by the Superintendent, such as for advertising that benefits the District and/or District students.

N.   Not attempt to harm, modify, add, or destroy software or hardware nor interfere with and/or circumvent any system security.

O. Understand that inappropriate use of District EIS may result in cancellation of permission to use District EIS and appropriate disciplinary action up to and including expulsion for a student and termination of employment for an employee.

In addition, acceptable use for District employees is extended to include the requirement to maintain supervision of students using District EIS.

Acceptable Use of Wireless Communication Devices by Students

Students may use wireless communication devices:

A.   for educational purposes, as directed by the student's teacher
B.   during an emergency;
C.   as needed for a medical condition.
D.   With permission from a teacher or staff member, a student may contact their parent/legal guardian using the student's cellular telephone.

In addition, students in grades K-8 may use wireless communication devices before and after school but must have their devices on silent and stored out of sight during the entirety of the school day unless the student is using the device as authorized above.

Students in high school may use their wireless communication devices before and after school, during their lunch break, and during passing periods. Students must have their devices on silent and stored out of sight during all instructional time unless the student is using the devices as authorized above.

No student may use a wireless communication device during instructional time to access a social media network except as expressly authorized by a teacher or staff member for educational purposes.

Web Services

The purpose of the District's website is to provide effective, timely and supportive educational information to District students, staff, and community. The District website provides easy access to a wide variety of rich media and educational resources which directly supports student learning, student achievement, staff recognition, professional development, and organizational effectiveness.

Material appropriate for placement on the District website includes information about the District, department activities or services, schools, teachers or classes, student projects, and student extracurricular organizations. Educational resources for staff, students, and the community may also be published online. Personal information, not related to education, will not be allowed on the District website.

Any use of defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material may result in loss of network privileges.

Marana Unified School District (MUSD) endeavors to ensure that all website links are operational. The District does not assume liability for information lost, damaged, or unavailable due to technical or other difficulties.

Website Creation: The following will be observed in the use of web servers:

A. The District's Information Technology Department will oversee the design, implementation and maintenance of all MUSD websites.

B. School principals or department directors will be responsible for all content and subject matter posted on their school or department website.

C. School principals will be responsible for all content and subject matter posted on their teacher/staff websites. Department directors will be responsible for all content and subject matter posted on their staff websites.

D. Web content must be in keeping with the District's Use of Technology Resources in Instruction policy.

E. Approved parent citizen organizations will work with their schools Web Team and with the school principal's approval to place content on their school's website in accordance with the Use of Technology Resources in Instruction policy.

Publication Expectations

The following will be observed in all District, school, and employee web publications by all website publishers:

A. All District and school web pages should meet goals of quality in both style and presentation. The design of all site pages will be consistent with the design and styles of the District web site. Modification of color, design, logo, mascot for school web sites is acceptable only with the approval of the school Web Team and the Information Technology Department.

B. All teacher websites should meet goals of quality in both style and presentation. The design of teacher site pages will be consistent with the approved design and styles established for the District. The style and design may vary depending on the product used.

C. All web pages must comply with the Use of Technology Resources in Instruction policy.

D. All web publishers must have read and agreed to abide by the established Use of Technology Resources in Instruction policy prior to having content published online.

E. All pages for publishing will be approved by the principal or department director to insure correct content and/or quality of published material.

F. Web pages not in keeping with District policy may be subject to removal without notice.

G. Inactive web pages may be removed without notice.

H. Personal web pages are not permitted on any District web page or sites.

I. Correct grammar and spelling are expected. All content must be current and verifiable.

J. All sites/pages should be checked regularly for quality content and designed for clarity and readability.

K. Relevant referencing and modification dates for each page must be able to be viewed from the administration side of the Web Content Management System.

L. No students are allowed to publish pages to the Web Content Management System. As part of the instructional process a teacher may sponsor the work of a student and present it to the school Web Team for content upload to the school website. Only MUSD staff members may act as student sponsors and all pages must reflect the connections to educational projects, activities or goals.

M. Publication of identifiable student photos or student work are not permitted without a current District Internet Website Release form on file with the school's Web Team or the department director.

N. A current District Internet Website Release form must be retained on file as long as the student's picture, work product, or name remains online. A group photograph may be published in the Web Content Management System without the use of a release form if the photograph is general in nature and does not include the names of specific students appearing in the photo.

O. All web pages must comply with all state, federal, and international laws concerning copyright, intellectual property rights, and legal uses of network computers. All web publishers

must clearly identify the sources of documents they post, and provide complete citations for documents, or sources, which are incorporated into the District/school website.

P. Copyrighted materials must be clearly identified, and prior written permission must be secured before using copyrighted work in electronic form. Copyrighted materials that do not meet these standards will not be placed on a web site and are subject to removal without notice.

Q. Publications must include a statement of copyright when appropriate and indicate that permission has been secured when including copyrighted materials.

R. Noneducational games and links to noneducational games are not to be published online. Educational games in the support of educational processes are acceptable. (Example: programming classes that instruct students in creation of computerized games.)

S. Commercial use for the pursuit of personal or financial gain is prohibited on District web pages, unless specific permission is given by the Superintendent, such as for advertising that benefits the District and/or District students. School Web Teams in coordination with the Information Technology Department can approve nonprofit club pages or other school related pages.

T. Website creation programs that have been purchased by the District or schools must meet all rules for web servers and publication and have the capability to be monitored for content. The Information Technology Department in collaboration with school Web Teams or department directors can approve use of external web servers that host specialized functions not available in the Web Content Management System.

U. All District web publishers will participate in District Web Content Management Training through Professional Development or through the Information Technology Department.

V. The Web Content Management System has been tested for use by most popular browsers and screen resolutions; there is no implied guarantee or warranty of usability to users of the website.

**District Electronic Collaboration
Systems - DECS**

Compliance with this Acceptable Use policy in its entirety is expected and will be observed by all network users while using District Electronic Collaboration Systems (DECS - currently known as Web 2.0 tools or Rich Internet Applications).

The District will allow the use of third party District Electronic Collaboration Systems, or Web 2.0 tools, by MUSD network users. These tools include but are not limited to: electronic mail (e-mail), file storage, blogs, wikis, podcasting, social networking, etc.

Such Web 2.0 tools have varying degrees of bandwidth requirements. Some online collaboration systems require short-term bandwidth needs (file storage, e-mail, blogs, wikis), while other require prolonged and sustained bandwidth (audio/visual streaming, etc.)

The availability of these resources to District staff and students is directly related to the amount of available Internet bandwidth, as well as available bandwidth per site. Every effort will be made to allow full access to such resources during school hours. In the event that Internet bandwidth has, or will, become compromised in its availability, the Information Technology Department reserves the right to limit access to various web resources.

The District reserves the right to control and/or monitor all electronic collaboration as it relates to MUSD employees, students, or other authorized network users. Efforts should be made to ensure that District Electronic Collaboration Systems are used only in support of administrative, instructional, research, and educational objectives of the District.

Individuals that decide to use a District Electronic Collaboration System are charged with monitoring and administering their site. For example, if a teacher creates a blog for use by students, the teacher becomes the responsible party and is accountable for all content displayed on that blog.

No MUSD website author/publisher will knowingly link to any material that the individual knows, or should know, is defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal from any District/school website.

District Electronic Collaboration Systems must take into account various children protection acts (COPPA, CIPA, etc.), possess the ability to administer users and groups of users, and allow for the monitoring and removal of inappropriate content or links to inappropriate content.

No District employee or student shall create a social networking page or account in an effort to, with or without malice, represent the District, a school within the District, a District department, or an area of interest within a school (student clubs, athletics, etc.), using, either in part or in whole, the name of the District, or any of its schools, without the consent of District administration.

Levels of Web Publication

All system training, accounts and administration will be provided by the Information Technology Department who also oversees the following levels of web publication.

District Level

Includes the main District website as well as all department websites.

A. The District website is maintained by the Information Technology Department.

B. Department websites are maintained by department directors and/or their designee.

School Level

Includes the school website as well as teacher websites.

A. School websites are the responsibility of the school principal who designates a school web team and a member of administration to be the team leader.

B. The school website is maintained by the school Web Team.

C. Team members shall be designated specific duties as determined by the Web Team Leader and the Information Technology Department.

D. All Web Team members will read and become familiar with the Use of Technology Resources in Instruction and will maintain the school website in accordance with the policy.

Staff, Teacher and Student Level

Includes staff, teacher and teacher-sponsored websites.

A. Staff or teachers who have completed appropriate training will be given access to create and maintain an authorized teacher website which may include any combination of on-line tools the District offers. Currently:

1. WCM Teacher Website (Web Content Management).

2. DECS.

3. Genesis Parent Portal.

B. Appropriate training may be provided through the Professional Development department.

C. The website must be maintained by the staff member or teacher.

D. All staff and teachers will read and become familiar with the Use of Technology Resources in Instruction and will maintain their websites in accordance with the policy.

E. Students are not allowed to publish to the Web Content Management system.

F. Teachers may sponsor student web pages and post them to the Web Content Management system provided the pages meet the requirements set forth in the Use of Technology Resources in Instruction policy.

Appendices:

A. District Internet Website Release form

B. Web Publishing Checklist

C. MUSD Electronic Acceptable Use Agreement - Staff (*note*: also used for student teacher)

D. MUSD Electronic Acceptable Use Agreement - Students