

# Douglas County West Community Schools

## 1:1 iPad Program

### DC West Community Schools Mission Statement

At Douglas County West Community Schools we create passionate learners by maximizing achievement through dynamic learning experiences that inspire and provide a quality education for all students within a safe and community-supported learning environment.

---

DC West Community Schools uses Instructional Technology as one way of enhancing the mission to prepare and inspire all students for life-long success by teaching the skills, knowledge, and behaviors students will need as responsible citizens in the global community. Students learn collaboration, communication, creativity, and critical thinking in a variety of ways throughout the school day. Excellence in education requires that technology is seamlessly integrated throughout the educational program. In an effort to increase access to those 21st-century skills, DC West Elementary has made it a goal to offer students access to their learning through the DC West 1:1 iPad Program. The individual use of technology is a way to empower students to maximize their full potential and to prepare them for the future.

The policies, procedures, and information within this document apply to all iPads used at DC West Elementary School. Teachers may set additional requirements for use in their classrooms.

An important component of the 1:1 iPad Program will be education about digital citizenship and appropriate online behaviors. We will review cyber-safety rules with students frequently throughout the school year, and will offer reminders and reinforcement about safe online behaviors. We also encourage parents to be involved with helping their student(s) make good choices when it comes to being online and using school-issued technology.

DC West Community Schools is proud to offer our DC West Elementary School students Apple iPad devices for use in the classroom. The 1:1 iPad Program, which provides mobile computing and wireless technology to DC West Elementary students, has been designed to enhance the delivery and individualization of instruction.

## Table of Contents

[Section 1: iPad Specifications](#)

[Section 2: Taking Care of your iPad](#)

[Section 3: Using your iPad at School](#)

[Section 4: iPad Apps](#)

[Section 5: Protecting Your iPad](#)

[Section 6: iPad Acceptable Use Guidelines](#)

[Section 7: Precautions & Consequences](#)

[iPad Damages - Cost to Student](#)

[Appendix 1: Internet Safety and Acceptable Use of Computer/Network Policies](#)

## Section 1: iPad Specifications

**Grades pk-6** 9.7 inch iPad (6th Generation) 32 GB Capacity Wi-Fi

## Section 2: Taking Care of Your iPad

For students and parents/guardians, the following information is provided to help you understand the expectations and responsibilities to care for the iPad.

- Students will receive instruction from school district staff on the proper use of the iPad.
- The school will provide a protective case for iPads. Students may use their own case if approved by the Technology Department or Administrators.
- Students will not be able to take the iPad home.
- Students will keep their iPad in their possession inside of school.
- Students are expected to treat the iPad as a valuable piece of equipment.
- Students will clean and maintain their iPads per school procedures.
- Students must take precautions to prevent damage to the iPad.
- The iPad comes with preloaded school approved apps.
- Students are to use the iPad to access only socially and educationally appropriate materials and websites.
- Students should not use the iPad to purchase goods and services via the Internet.

(NOTE: Parents/students are charged with full responsibility for any financial obligations incurred from the inappropriate use of the iPad.)

- Students are to use the iPad in accordance with the DC West Community Schools 2021-22 Student Handbook, the Acceptable Use Regulations, and to maintain the iPad in accordance with the procedures and information provided.
- iPads are the property of DC West Community Schools and must be returned at the end of the academic year, upon withdrawal from DC West Community Schools, or at the request of a teacher or administrator. Willful failure to return the iPad in accordance with the stated conditions will result in criminal prosecution.
- Since the iPads are the property of DC West Community Schools, officials of the school have the right to review all material stored on or accessed by any iPad. School officials may revoke a student's iPad use and/or privileges for misuse or violation of policies.

## Section 3: Using Your iPad

### General

- iPads are intended for academic use at school every day. Students are responsible for making sure their iPad is plugged in and charging every day.

### iPads Undergoing Repair

- Older, loaner iPads may be issued to students when their iPads has been sent to Technology Support for repair.

### Screensavers and Backgrounds

- Only school appropriate backgrounds and screensavers may be used on the iPads.
- Presence of weapons-related materials, pornographic materials, inappropriate language, alcohol, drug, gang-related symbols, or pictures on the iPad or within its files will result in disciplinary action and, where appropriate, referral to law enforcement.
- The iPad is the property of the school district. Therefore, the school staff has the right to check any material stored on a student's iPad.
- Violation of this policy will result in disciplinary action.

### Sound

- Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.

### Printing

- Materials printed on school printers must be school-related. No personal printing is allowed.

## Section 4: iPad Apps

### Installed Apps

\*The apps originally installed or added during the school year by DC West Community Schools must remain on the iPad in usable condition and be easily accessible at all times. Students are not allowed to alter or remove school-installed apps. The Technology Department has the discretion to approve and install or delete additional apps and files. Distributing apps to unauthorized devices is prohibited.

### Security

The iPad may have Anti-virus protection software installed. This Anti-virus software may be updated from the Internet. Students are required to allow all updates to download uninterrupted.

### Inspection

Students will willingly provide their school-issued iPad for inspection by school staff without prior notice.

## Section 5: Protecting and Your iPad Device

### iPad Identification

Student iPads will be labeled in the manner specified by the school. Under no circumstances are students to modify, remove, or destroy these labels.

### Password Protection

Students are expected to set up a personal lock-code for their assigned iPad. Tampering with machine security measures is forbidden. Violations of this policy will result in disciplinary action. Do not share this password with other students.

### Apple ID

Students are to use their school-issued Apple ID. This will be provided by a teacher as needed.

## Section 6: iPad Acceptable Use Guidelines

### General Guidelines

- Students are responsible for their ethical, socially appropriate and educational use of the technology resources of the DC West Community Schools.
- Access to the DC West Community Schools technology resources is a privilege and not a right. Each employee, student and/or parent will be required to follow the DC West Community Schools Acceptable Use Policy.
- Transmission of any material that is in violation of any law is prohibited. This includes, but is not limited to the following: confidential information, copyrighted material, threatening or obscene material, and iPad viruses.
- Any attempt to alter data or profiles, the configuration of an iPad, or the files of another user, without the consent of the Principal/Administration or Technology Team, will be considered an act of vandalism and subject to disciplinary action in accordance with the district Acceptable Use Policies. Students who violate this may also be referred to law enforcement for criminal prosecution as appropriate.
- The Computer Network includes, but is not limited to, the use of local area networks, Internet, online commercial communications, and all other computer communications provided by the DC West Community School District.
- The DC West Community School District will take reasonable precautions to ensure the security and appropriate use of the iPad network. However, it accepts no responsibility for harm caused directly or indirectly through its use.

### Integrity and Civility

In addition to any standard/rules established by the school, the following behaviors are prohibited as they violate the standard of integrity and civility.

- Cheating
- Plagiarizing
- Falsifying Information
- Violating Copyright Law
- Hacking
- Gaining unauthorized access to any network or iPad
- Cyberbullying
- Always use appropriate language.
- Do not transmit language/material that is profane, obscene, abusive, or offensive to others.
- Do not send mass emails, chain letters, or spam.
- No private chatting during class without permission.
- Cyberbullying will not be tolerated.

## Section 7: Precautions and Consequences

### Technology Left in Unsupervised Areas

- Under no circumstances should iPads or other technology equipment be left in unsupervised areas. Unsupervised areas include, but are not limited to: the school grounds and campus, computer labs, unlocked classrooms or lockers, bathrooms, busses, and hallways. Any iPad left in these areas is in danger of being stolen.
- iPads carried in book bags may be damaged, **please handle the iPad with care.**
- Lockers are to be locked when storing any technology equipment. This includes, but is not limited to power cords and iPads.
- Unsupervised iPads will be confiscated by staff and taken to the administrative office. Disciplinary action will be taken for leaving your iPad in an unsupervised location. **Each student is responsible for his or her iPad & charging cord once it has been issued.**

**iPad Damage - \*Cost to Student**

Claims/Damage	Cost to Replace
Lost iPad	\$200
Stolen iPad (Police Report Required)	\$150
iPad Repairs - due to Physical Damage	\$20
Purposeful/Intentional Damage	\$300

**iPad Consequences for Inappropriate Use:**

Noncompliance with the policies of the DC West Community Schools 1:1 iPad Program Procedures, 2021-22 Student Handbook or Acceptable Use of Computers/Network Policies will result in loss of privileges, disciplinary action, and/or criminal prosecutions deemed appropriate. All inappropriate behaviors are subject to the 2021-22 Student Handbook. Additional consequences for inappropriate iPad behaviors may occur as described in the 1:1 iPad Program Procedures.

Device usage, network usage, and all files stored on a school-issued iPad is not to be considered confidential and may be monitored at any time by designated DC West Community Schools staff. The district will refer student misconduct to law enforcement and will cooperate fully with local, state, or federal officials in any criminal investigation, particularly those concerning or relating to violations of computer crime laws,

**Consequences:**

The consequences for students who abuse their iPad privileges can include anything from partial to total loss of iPad privileges to iPad suspensions.

**Example Violations:**

- Unattended iPad
- Inappropriate/unauthorized apps, games, chat, email, video chat, or music without permission.
- Voice and/or Video recording without staff permission.
- Abuse of iPad.
- Printing Inappropriately.
- Inappropriate Pictures (desktop, screensaver, saved files etc.)
- Inappropriate Internet Site.
- Inappropriately Accessing School Network (Hacking).
- Deleting profiles or the Student handbook.

The administration retains the right to suspend the student's iPad for any period of time if the offense warrants or for any offense not listed on this sheet. This includes suspending the iPad for the remainder of the semester or school year.

The DC West Community Schools District is not liable for and disclaims any liability arising from any injury or damage caused by or stemming from unauthorized access to the network or inappropriate use of authorized access to the network.

A student and the student's parents or guardians agree to release the School district from any liability for physical or emotional harm or damage resulting to the student that is caused by or related to the inappropriate use of the iPad network.

## Appendix 1: Internet Safety and Acceptable Use of Computer/Network Policies

### A. Internet Safety Policy

It is the policy of Douglas County West Community Schools to comply with the Children's Internet Protection Act (CIPA). With respect to the District's computer network, the District shall: (a) prevent user access to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) provide for the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) prevent unauthorized access, including so-called "hacking," and other unlawful activities online; (d) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (e) implement measures designed to restrict minors' access to materials (visual or non-visual) that are harmful to minors.

#### A1. Definitions

Key terms are as defined in CIPA. "Inappropriate material" for purposes of this policy includes material that is obscene, child pornography, or harmful to minors. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that: (1) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (2) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (3) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

#### A2. Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the CIPA, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

#### A3. Inappropriate Network Usage

To the extent practicable, steps shall be taken to promote the safety and security of users of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by CIPA, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

#### A4. Supervision and Monitoring

It shall be the responsibility of all members of the District staff to supervise and monitor the usage of the online computer network and access to the Internet in accordance with this policy and CIPA. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Superintendent and the Superintendent's designees.

#### A5. Social Networking

Students shall be educated about appropriate online behavior, including interacting with others on social networking websites and in chatrooms and cyberbullying awareness and response. The plan shall be for all students to be provided education on these subjects. The Superintendent or the Superintendent's designee shall be responsible for identifying educational materials, lessons, and/or programs suitable for the age and maturity level of the students and for ensuring the delivery of such materials, lessons, and/or programs to students.

#### A6. Adoption.

This Internet Safety Policy was adopted by the Board at a public meeting, following normal public notice.

### B. Computer Acceptable Use Policy.

This computer acceptable use policy is supplemental to the District's Internet Safety Policy.

#### B1. Technology Subject to this Policy

This Computer Acceptable Use Policy applies to all technology resources of the District or made available by the District. Technology resources include, without limitation, computers and related technology equipment, all forms of e-mail and electronic communications, and the internet.

#### B2. Access and User Agreements

Use of the District technology resources is a privilege and not a right. The Superintendent or designee shall develop appropriate user agreements and shall require that employees, students (and their parents/ guardians), and others sign such user agreements as a condition of access to the technology resources, as the Superintendent determines appropriate. Parents and guardians of students in programs operated by the District shall inform the Superintendent or designee in writing if they do not want their child to have access.

The Superintendent and designees are authorized and directed to establish and implement such other regulations, forms, procedures, guidelines, and standards to implement this Policy. The technology resources are not a public forum. The District reserves the right to restrict any communications and to remove communications that have been posted.

#### B3. Acceptable Uses

The technology resources are to be used for the limited purpose of advancing the District's mission. The technology resources are to be used, in general, for educational purposes, meaning activities that are integral, immediate, and proximate to the education of students as defined in the E-rate program regulations.

#### B4. Unacceptable Uses

The following are unacceptable uses of technology resources:

**B4a. Personal Gain:** Technology resources shall not be used, and no person shall authorize its use, for personal financial gain other than in accordance with prescribed constitutional, statutory, and regulatory procedures, other than compensation provided by law.

**B4b. Personal Matters:** Technology resources shall not be used, and no person shall authorize its use, for personal matters.

Occasional use that the Superintendent or designee determines to ultimately facilitate the mission of the District is not prohibited by this provision. Examples of occasional use that may be determined to ultimately facilitate the mission of the District: sending an email to a minor child or spouse; sending an e-mail related to a community group in which an employee is a member where the membership in the community group facilitates the District's mission.

This occasional use exception does not permit the use by employees contrary to the expectations of their position. For example, employees may not play games or surf the net for purposes not directly related to their job during duty time; nor may students do so during instructional time.

The occasional use exception also does not permit the use of the technology resources for private business, such as searching for or ordering items on the internet for non-school use; or sending an e-mail related to one's own private consulting business.

**B4c. Campaigning:** Technology resources shall not be used, and no person shall authorize its use, for the purpose of campaigning for or against the nomination or election of a candidate or the qualification, passage, or defeat of a ballot question.

**B4d. Technology-Related Limitations:** Technology resources shall not be used in any manner which impairs its effective operations or the rights of other technology users. Without limitation,

- i. Users shall not use another person's name, log-on, password, or files for any reason, or allow another to use their password (except for authorized staff members).
- ii. Users shall not erase, remake, or make unusable another person's computer, information, files, programs or disks.
- iii. Users shall not access resources not specifically granted to the user or engage in electronic trespassing.
- iv. Users shall not engage in "hacking" to gain unauthorized access to the operating system software or unauthorized access to the system of other users.
- v. Users shall not copy, change, or transfer any software without permission from the network administrators.
- vi. Users shall not write, produce, generate, copy, propagate, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software. Such software is often called a bug, virus, worm, Trojan horse, or similar name.
- vii. Users shall not engage in any form of vandalism of the technology resources.
- viii. Users shall follow the generally accepted rules of network etiquette. The Superintendent or designees may further define such rules.

**B4e. Other Policies and Laws:** Technology resources shall not be used for any purpose contrary to any District policy, any school rules to which a student user is a subject, or any applicable law. Without limitation, this means that technology resources may not be used:

- i. to access any material contrary to the Internet Safety Policy; or to create or generate any such material.
- ii. to engage in unlawful harassment or discrimination, such as sending emails that contain sexual jokes or images.
- iii. to engage in violations of employee ethical standards and employee standards of performance, such as sending emails that are threatening or offensive or which contain abusive language; use of end messages on emails that may imply that the District is supportive of a particular religion or religious belief system, a political candidate or issue, or a controversial issue; or sending emails that divulge protected confidential student information to unauthorized persons.
- iv. to engage in or promote violations of student conduct rules.
- v. to engage in illegal activity, such as gambling.
- vi. in a manner contrary to copyright laws.
- vii. in a manner contrary to software licenses.

**B5. Filter**

A technology protection measure is in place that blocks and/or filters access to prevent access to Internet sites that are not in accordance with policies and regulations. In addition to blocks and/or filters, the District may also use other technology protection measures or procedures as deemed appropriate.

Notwithstanding technology protection measures, some inappropriate material may be accessible by the Internet, including material that is illegal, defamatory, inaccurate, or potentially offensive to some people. Users accept the risk of access to such material and responsibility for promptly exiting any such material.

The technology protection measure that blocks and/or filters Internet access may be disabled only by an authorized staff member for bona fide research or educational purposes: (a) who has successfully completed District training on proper disabling circumstances and procedures, (b) with permission of the immediate supervisor of the staff member requesting said disabling, or (c) with the permission of the Superintendent. An authorized staff member may override the technology protection measure that blocks and/or filters Internet access for a minor to access a site for bona fide research or other lawful purposes provided the minor is monitored directly by an authorized staff member.

**B6. Monitoring**

Use of the technology resources, including but not limited to internet sites visited and e-mail transmitted or received is subject to monitoring by the administration and network administrators at any time to maintain the system and ensure that users are using the system responsibly, without notice to the users. Users have no privacy rights or expectations of privacy with regard to the use of the District's computers or Internet system. All technology equipment shall be used under the supervision of the Superintendent and the Superintendent's designees.

**B7. Sanctions**

Violation of the policies and procedures concerning the use of the District technology resources may result in suspension or cancellation of the privilege to use the technology resources and disciplinary action, up to and including expulsion of students and termination of employees. Use that is unethical may be reported to the Commissioner of Education. Use that is unlawful may be reported to the law enforcement authorities. Users shall be responsible for damages caused and injuries sustained by improper or non-permitted use.

Legal Reference: Children's Internet Protection Act, 47 USC § 254

FCC Order adopted August 10, 2011

47 USC § 254(h)(1)(b); 47 CFR 54.500(b) and 68 FR 36932 (2003) (E-rate restrictions)

Neb. Rev. Stat. § 49-14,101.01 (Political Accountability and Disclosure Act) Date of Adoption: June 11, 2012