Availability of Access

Systems and electronic equipment.

Access to the District’s technology resources, including the Internet, shall be made available to students and employees, primarily for instructional and administrative purposes and in accordance with administrative regulations.

Limited Personal Use

Limited personal use of the District’s technology resources shall be permitted if the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden the District’s technology resources;
3. Has no adverse effect on an employee’s job performance or on a student’s academic performance; and
4. Is not used for commercial or political purposes.

Use by Members of the Public

Access to the District’s technology resources, including the Internet, shall be available to members of the public, in accordance with administrative regulations. Such use shall be permitted so long as the use:

1. Imposes no tangible cost on the District; and
2. Does not unduly burden the District’s technology resources.
   
   Access shall be primarily for instructional and administrative purposes.

Acceptable Use

Note: For Board member use of District technology resources, see BBI. For student use of personal electronic devices, see FNCE.

The Superintendent of Schools or designee shall develop and implement administrative regulations, including administrative procedures, guidelines, and user agreements, consistent with the purposes and mission of the District and with law.

Noncompliance with applicable regulations may result in disciplinary action consistent with District policies. Violations of law may result in criminal prosecution.

For purposes of this policy, “technology resources” means electronic communication.
Internet Safety

The Superintendent of Schools or designee shall develop and implement an Internet safety plan to:

1. Control students’ access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities;
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; and
5. Educate students about cyberbullying awareness and response and about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms.

Filtering

The District’s network systems shall be filtered to block access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children’s Internet Protection Act and as determined by the Superintendent of Schools or designee.

The Superintendent of Schools or designee shall enforce the use of such filtering devices. Upon approval from the Superintendent of Schools or designee, an administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose.

Monitored Use

Electronic mail transmissions and other use of the District’s technology resources by students, employees, and members of the public shall not be considered private. Designated District staff shall be authorized to monitor the use of the District’s technology resources at any time to ensure appropriate use.

Disclaimer of Liability

The District shall not be liable for users’ inappropriate use of the District’s technology resources, violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on electronic resources, including the Internet.

Record Retention

A District employee shall retain electronic records, whether created or maintained using the District’s technology resources or using personal technology resources, in accordance with the District’s record management program. [See CPC]
Security Breach Notification

Upon discovering or receiving notification of a breach of system security, the District shall disclose the breach to affected persons or entities in accordance with the time frames established by law. The District shall give notice by using one or more of the following methods:

1. Written notice.
2. Electronic mail, if the District has electronic mail addresses for the affected persons.
3. Conspicuous posting on the District’s website.
4. Publication through broadcast media.

Allocations

Technology resources shall be allocated to meet the minimum standards requirements of state mandates in accordance with the needs of schools as defined in the school improvement plans and as reflected in the goals of the Long-Range Plan for Technology.

Acquisitions

All acquisitions of technology resources, both hardware and software, must be authorized and coordinated with the Information Technology Division and shall meet the requirements of the Procurement Services department.

Donations

Technology donations must be coordinated through the Department of Volunteer and Partnership Services and the Information Technology Division. Donations must meet the minimum approved standards as defined by the Information Technology Division.

Although donated technology resources may be configured to operate in the District’s environment, the Information Technology Division cannot guarantee compatibility with all District applications and resources.

Adoption or Last Amended Date

This policy was last amended on August 23, 2018.

ADOPTED:
NETIQUETTE ON THE INTERNET

All users of the District’s computers and networks are expected to abide by the generally accepted rules of network etiquette (netiquette). Informal rules of behavior have evolved for the use of communication on the Internet and other online services. Breaches may result in restricted use or loss of privileges on the Internet. These rules of behavior include, but are not limited to, the following:

1. Be polite. Do not become abusive in your messages to others.

2. Use appropriate language. Do not swear, use vulgarities, or any other inappropriate language.

3. Do not reveal your personal home address or home phone number or that of other students or colleagues.

4. Do not place unlawful information on any network system. Electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to mail. Messages relating to or in support of illegal activities may be reported to the authorities.

5. Keep paragraphs and messages short and to the point. Focus on one subject per message.

6. Abbreviate when possible. Some examples are: IMHO (in my humble opinion), FYI (for your information), and :-) (happy face for humor).

7. Include your signature at the bottom of e-mail messages. Your signature footer should include your name, position, affiliation, and Internet address.

8. Capitalize words only to highlight an important point or to distinguish a title or heading. “Asterisks” surrounding a word can also be used to make a stronger point.
EXHIBIT E

MINIMUM SECURITY STANDARDS FOR USE OF PERSONAL EQUIPMENT

Use of personal technology equipment or other non-District-owned equipment connecting to the District’s network is a privilege not a right. Before providing access to the District’s network, users must be responsible, note disclaimers, and adhere to the standards listed below.

Users not adhering to those responsibilities, regulations, and disclaimers may be disconnected from the District’s network.

User Responsibilities

- Users are responsible for the purchase of all software and hardware for their personal equipment.
- Users are responsible for installing and maintaining any and all software and hardware to comply with these guidelines.
- The District reserves the right to inspect all devices connecting to the network.
- Users connecting to the District’s network have no expectation of privacy.
- The District is not responsible for supporting and/or troubleshooting problems with personal devices attaching to the network.

Security Standards

- Must “accept” the information security online agreement before being given access to the District’s network.
- Maintain current industry-supported operating system with all critical patches applied.
- Keep up-to-date commercial antivirus, spyware, and malware protection on all devices where available.
- Ensure that devices are password protected. If a device cannot be password protected, the device is not allowed onto the network.
- Do not upload, download, or share data on the device unless authorized.
- Do not use devices that act as a network or proxy, which is strictly prohibited.
- Adhere to all regulations herein (including Acceptable Use).
- See the Information and Technology Services department’s Web site for additional guidelines and controls, which will be reviewed and updated as required.
PASSWORD MANAGEMENT

The following password restrictions apply to all employees, teachers, students (grades 6–12), vendors, contractors, and other third parties:

**Passwords Must Contain:**
- At least eight characters in length.
- Characters from three of the following four categories:
  - English uppercase characters (A through Z).
  - English lowercase characters (a through z).
  - Base ten digits (0 through 9).
  - Non-alphabetic characters (e.g., ~!#$%^&*()_-+=).

**Passwords Cannot:**
- Spell a word or series of words that can be found in a standard dictionary.
- Spell a word in any language, slang, dialect, jargon, and the like.
- Spell a word that is a common usage word such as:
  - Names of family members, pets, friends, coworkers, fantasy characters, and the like.
  - Computer terms and names, commands, sites, companies, hardware, and software.
  - The words "Dallas ISD", "staff", "District", "DISD" or any derivation.
  - Birthdays and other personal information such as user ids, addresses, and phone numbers.
  - Word or number patterns such as aaabbb, qwerty, zyxwvuts, 123321, and the like.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

**Additional Password Restrictions:**
The following additional parameters have been established for all employees, teachers, students (grades 6–12), vendors, contractors, and other third parties:
- Password expires every 90 days or when admin staff resets your password.
- Last four passwords cannot be used.
• Account locked after six failed attempts.
• Six grace logins before you are forced to change password.

**Password Exceptions – Oracle**

Oracle passwords may not contain special characters as they interfere with system functionality. Therefore, the following does not apply in Oracle:

• Non-alphabetic characters (e.g., ~!@#$%^&*()-+=).

**Password Exceptions – Prekindergarten–Grade 5 Students**

Prekindergarten–grade 5 students are not at the same level of risk as older students, employees, teachers, and the like. Therefore, the following parameters have been established for students in prekindergarten–grade 5:

• Password set to four digit birth year.
• Password never expires.
• Students cannot change passwords.
• Admin staff can change student passwords.

**Password Resets**

To reset passwords, go to the Dallas ISD intranet Web site (authorized users only).

Go to http://inet/techresources/index.html.

OR

Contact your campus technician or department password administrator.

Employees, teachers, students, vendors, contractors, and other third parties may contact their campus technician or department’s password administrator and have that person request a password reset. If you do not know your department’s password administrator, contact your executive director or principal.

---

**Note:** You will need to provide a valid photo ID. Acceptable forms of ID include your Dallas ISD Employee or Student ID badge, state-issued driver’s license, or identification card or passport (U.S. or foreign). Once your identity is verified, your password will be reset.