Student

USE OF TECHNOLOGICAL DEVICES 5131.81(a)

The Fairfield Board of Education (the "Board") recognizes the need to maintain an effective educational environment. This policy establishes guidelines for the possession and use of devices to balance educational value with appropriate regulation.

I. DEFINITIONS

A. **District Technology Resources**

For the purposes of this policy, "District Technology Resources" refers to the District's owned, operated, managed, or offered:

- Computers and instructional technologies
- Communications and data management systems
- Networks and access to the Internet
- Software, hardware, and programs
- Electronic media information, devices, and systems
- Cell phones, smartphones, tablets, laptops, and desktop computers
- Storage devices including memory sticks and external drives
- Any other technological resources that can receive, transmit, and/or store digital information
- Any other technological resources owned and/or used by the District and accessible by students

B. **Privately-Owned Technological Devices**

For the purposes of this policy, "Privately-Owned Technological Devices" refers to privately-owned wireless, portable electronic hand-held equipment used for word processing, wireless internet access, image capture and recording, sound recording, information transmission and receiving, data storage, and more. These devices include but are not limited to:

- Desktop computers
- Personal computing devices
- Cellular phones
- Smartphones
- Smartwatches and other wearables
- Network access devices
- Tablets
- Laptops
- Personal gaming systems

Student

USE OF TECHNOLOGICAL DEVICES **5131.81(b)**

- Bluetooth speakers
- Wired and wireless earbuds
- Wired and wireless headphones
- E-readers
- Other electronic signaling device

This broad category encompasses all privately-owned devices, including Cellular-Capable Devices as defined in Section C below.

C. Cellular-Capable Devices

For the purposes of this policy, "Cellular-Capable Devices" refers to a specific subset of Privately-Owned Technological Devices that are capable of making voice calls, sending text messages, or accessing data through a cellular network connection. These devices include but are not limited to:

- Traditional cell phones and smartphones
- Tablets with cellular capability (devices with SIM card capability)
- Smartwatches and wearable devices with cellular/LTE capability
- Laptops or computers with embedded cellular modems
- Mobile hotspot devices
- Any device equipped with a SIM card slot or eSIM functionality
- Any device capable of connecting to cellular networks (3G, 4G, 5G, or future generations)
- Gaming devices with cellular capability
- E-readers with cellular data capability
- Any other device that can function independently as a communication device through cellular networks without requiring Wi-Fi or other network connections

These devices are distinguished by their capability to connect to cellular towers and function as independent communication tools, regardless of whether cellular service is currently active or a SIM card is presently installed. Cellular-Capable Devices are a subset of Privately-Owned Technological Devices and are subject to all provisions that apply to Privately-Owned Technological Devices, as well as additional specific restrictions outlined in Section III of this policy.

D. **Generative Artificial Intelligence**

For the purposes of this policy, "Generative Artificial Intelligence" refers to a technology system, including but not limited to ChatGPT, capable of learning patterns and relationships from data, enabling it to create content, including but not limited to text, images, audio, or video, when prompted by a user.

Student

USE OF TECHNOLOGICAL DEVICES **5131.81(c)**

II. GENERAL PROVISIONS

A. Privilege

The use of technological devices at school is a privilege, not a right. This privilege may be revoked for violations of this policy or other school rules.

B. Responsibility and Liability

1. Students are solely responsible for the safety, security, and maintenance of their privately-owned technological devices.
2. The Board assumes no responsibility for:
    a. Theft, loss, or damage to devices;
    b. Data plan charges or other costs; or
    c. Technical support or maintenance.
3. Students must take privately-owned technological devices home at the end of each school day unless specific permission is granted otherwise.

III. GUIDELINES FOR CELLULAR-CAPABLE DEVICES BY GRADE LEVEL

The following grade-level restrictions apply specifically to Cellular-Capable Devices as defined in Section I, C. Other Privately-Owned Technological Devices may be subject to different guidelines as determined by classroom teachers and school administration.

A. Elementary School Level

1. Prohibited during school hours and while using school-provided transportation.
2. Exceptions:
    a. Medical purposes (with administrative approval)

B. Middle School Level

1. Use prohibited during school hours.
2. Devices must be both:
    a. Turned off; and
    b. Stored.
3. Exceptions:
    a. Medical purposes (with administrative approval); and
    b. Special events (with administrative approval).

Student

USE OF TECHNOLOGICAL DEVICES **5131.81(d)**

C. **High School Level**

1. Use prohibited during school hours.
2. Devices must be both:
    a. Turned off; and
    b. Stored.
3. Exceptions:
    a. Medical purposes (with administrative approval); and
    b. Special events (with administrative approval).

IV. ACCESS TO DISTRICT TECHNOLOGY RESOURCES

A. **Network Access**

Students accessing district technology resources through private devices must:

1. Follow the administrative regulation for student internet policy for 6141.321.
2. Use only authorized network access methods.
3. Comply with security protocols.

B. **Network and Data Security**

1. Device recommendations:
    a. Maintain current security software and system updates
    b. Use password protection that meets district standards
    c. Store data using secure methods
    d. Log out when leaving devices unattended

2. Security Incidents:
    a. Report suspected data breaches immediately
    b. Report lost or stolen devices that accessed school networks
    c. Report unauthorized account access
    d. Change compromised passwords immediately

C. **Monitoring and Privacy**

1. The District's network administrators can:
    a. Identify users
    b. Monitor all privately-owned devices while on the network
    c. Bypass passwords for monitoring purposes
2. No expectation of privacy exists when using privately-owned technological devices on school networks.

Student

USE OF TECHNOLOGICAL DEVICES **5131.81(e)**

V. PROHIBITED USES

A. Elementary staff shall maintain screen-free settings during recess, snack time, and undirected time (e.g. transition time, play-based learning).

B. **Network Security Violations**

1. Using VPNs or proxy servers to bypass security
2. Attempting to bypass network filters
3. Sharing network credentials
4. Using another student's login information
5. Connecting to unauthorized wireless networks
6. Downloading unauthorized software

C. **Privacy Violations**

1. Sharing personal identifying information about self or others, except when required for assignment submission or educational purposes
2. Taking/creating unauthorized photos or videos of others
3. Recording in private spaces (restrooms, locker rooms)
4. Sharing photos/videos without consent
5. Photographing test materials or confidential documents

D. **Behavioral Violations**

1. Harassment, threats, or intimidation
2. Cyberbullying
3. Accessing obscene or inappropriate material
4. Unauthorized recordings, real or created (photo, video, audio)
5. Unauthorized use of generative AI
6. Use during emergency procedures without staff direction

E. **System Violations**

1. Damaging district technology resources
2. Unauthorized access to district technology resources
3. Installing unauthorized software
4. Intentionally opening suspicious attachments or links
5. Any violation of federal or state law

Student

USE OF TECHNOLOGICAL DEVICES **5131.81(f)**

VI. ENFORCEMENT AND DISCIPLINE

A. **Disciplinary Actions**

Misuse of the district technology resources and/or privately-owned technological devices to access or utilize the district's technology resources in an inappropriate manner or the use of such privately-owned technological devices in any manner inconsistent with this policy will not be tolerated and will result in progressive disciplinary action(s). The Superintendent or designee will collect all disciplinary action data to ensure the policy and administrative regulations are being enforced consistently and with fidelity.

B. **Search of Devices**

1. Devices may be searched if reasonable suspicion exists of policy violation.
2. Searches must be:
    a. Reasonable in scope
    b. Related to suspected violation
    c. Conducted by appropriate administrators
3. Criminal evidence will be referred to law enforcement

C**. Data Collection**

1. **Network Connection Data**
   When students connect Privately-Owned Technological Devices to district networks, the District may collect and monitor:

   a. Network traffic data including:

   - Websites visited while on district network
   - Time and duration of network usage
   - Bandwidth consumption
   - Attempted access to blocked or filtered content
   - Network protocols and ports used

   b. Device identification information including:

   - MAC (Media Access Control) addresses
   - IP addresses assigned by district network
   - Device type and operating system
   - Device hostname/name
   - Network access points used

Student

USE OF TECHNOLOGICAL DEVICES **5131.81(g)**

c. Authentication data including:

- Login credentials used to access district network
- Time and date of network connections
- Duration of network sessions
- Failed login attempts

2. Scope and Limitations

a. The District does NOT have access to:

- Files stored on privately-owned devices
- Personal applications not accessing the network
- Device content when not connected to district network
- Personal accounts not accessed through district network
- Device location outside of school property

b. Data collection occurs ONLY when:

- Device is connected to district Wi-Fi or network
- Device accesses district technology resources
- Device attempts to access internet through district network

3. Data Use and Protection

a. Collected network data will be used only for:

- Ensuring network security and preventing cyberattacks
- Monitoring compliance with acceptable use policies
- Troubleshooting network connectivity issues
- Maintaining Children's Internet Protection Act (CIPA) compliance
- Investigating policy violations or security incidents
- Managing network capacity and performance

b. The District will:

- Implement reasonable security measures to protect collected data
- Limit access to authorized IT and administrative personnel
- Not monitor personal accounts accessed through encrypted connections (HTTPS)
- Not sell or share network usage data with third parties except as required by law

Student

USE OF TECHNOLOGICAL DEVICES **5131.81(h)**

VII. EMERGENCY PROTOCOLS

A. Emergency Communications

1. Parents may contact the school for emergency messages.
2. Students may use office phones for emergency calls.

B. Medical Necessity

1. Medical exceptions must be documented with an approved party (e.g. 504 plan).
2. Individual medical plans may include device accommodations.

Adopted: 10/28/2025