Employee Use of Electronic Communications Devices

1. Purpose Statement

The Board recognizes that employees may carry electronic communications devices, either District-issued or personally owned. This policy governs employee use of District-issued and personally owned electronic communications devices when used for District business, during work time, on District property, or in communication with students.

2. Definitions

A. District-approved platform means an electronic communication, instructional, messaging, storage, or records platform approved by the Superintendent/designee for District business, school-related communication, or communication with students.

B. District-issued device means any electronic communication device, computing device, or network-connected device issued, assigned, owned, leased, managed, or otherwise provided by the District for employee use.

C. Electronic communication includes, but is not limited to, email, text messages, direct messages, messaging applications, learning management system messages, social media messages, video or audio messages, shared documents, posts, comments, photographs, videos, audio recordings, or other digital communications.

D. Electronic communication device means any device capable of creating, sending, receiving, storing, recording, transmitting, displaying, or accessing electronic communications, data, images, video, audio, or digital content.

E. Personally owned device means any electronic communication device owned, leased, or primarily controlled by an employee and not issued by the District.

3. District-Issued Communications Devices

A. District-issued communication devices may include, but are not limited to, cellular phones, smartphones, tablets, laptop computers, desktop computers, radios, hotspots, or other electronic communication, computing, or network-connected devices issued or authorized by the District.

B. Employees who receive District-issued equipment are responsible for the safekeeping of the equipment and shall exercise reasonable care to prevent the equipment from being lost, stolen, or damaged. Reckless or irresponsible use of District-issued equipment resulting in loss or damage may result in the employee being required to reimburse the District for associated repair or replacement costs.

C. District-issued equipment shall be returned immediately upon request, reassignment, separation from employment, termination of employment, or at any other time directed by the Superintendent/designee.

D. The Superintendent/designee may authorize a school principal, immediate supervisor, or District technology personnel to require the return of any District-issued device at any time for inspection, copying, review, reassignment, security, or other appropriate District purpose.

E. District technology personnel may require the return or submission of a District-issued device for routine maintenance, repair, replacement, or technical support.

F. Files, histories, saved data, metadata, applications, and other information on District-issued devices may be inspected, copied, or reviewed by designated District personnel when authorized by the Superintendent/designee. Failure to return District-issued equipment upon request may result in disciplinary action, up to and including termination.

4. Software, Security, Filtering, and Remote Management

A. Software, applications, extensions, operating systems, security settings, and management controls originally installed or authorized by the District shall remain on District-issued devices in usable condition.

B. District-issued devices may be configured with filtering, monitoring, anti-virus, endpoint protection, mobile device management, security, and other technology controls approved by the District.

C. Employees shall ensure that only licensed software, applications, or extensions authorized by the District Technology Department are installed on District-issued laptops, desktop computers, or other District-issued devices where administrative installation rights are restricted.

D. Employees may install applications on District-issued phones or tablets for limited personal use, provided the applications do not interfere with the function, security, filtering, management, storage capacity, or appropriate use of the device and are not prohibited by law, District policy, or District technology controls.

E. Employees may not install unauthorized software, applications, extensions, operating systems, upgrades, security controls, or safety controls that interfere with District technology controls or the District’s ability to manage, monitor, secure, update, or recover the device. Employees may not change the operating system, bypass District technology controls, or interfere with District-installed software, filtering, monitoring, management, or security features.

F. District-issued devices may be equipped with remote access, remote management, location, security, filtering, monitoring, or data-protection features. These features may be used for technical support, software maintenance, cybersecurity, recovery of missing or stolen devices, compliance with District policy, or other appropriate District purposes.

   i. Employee permission is not required before the District conducts remote software maintenance or uses District-installed management or security features for an appropriate District purpose.

   ii. Employees may not disable, remove, alter, or interfere with District-installed remote access, management, filtering, monitoring, or security features.

G. TikTok Use Prohibited

   i. Employees shall not download, install, access, or use TikTok on any District-issued device.

   ii. If TikTok has already been downloaded or installed on a District-issued device, the employee shall delete the application or seek assistance from District technology personnel.

   iii. The District shall take reasonable measures to prevent the downloading, installation, or use of TikTok on District-issued devices and to block access to TikTok through the District's electronic network.

H. Filtering software and other technology controls may be used to prevent access to material considered inappropriate, harmful to minors, unsafe, unlawful, or inconsistent with District policy. If technical difficulties occur, or if unauthorized software, a security concern, or a violation of District policy is discovered, District technology personnel may remove files, uninstall programs, reset, reformat, or reimage the device. The District is not responsible for loss of personal software, files, applications, or materials stored on a District-issued device.

I. Employees have no expectation of privacy in District-issued devices, District accounts, District networks, District systems, or data stored, transmitted, received, or accessed through District technology resources. Content stored, created, sent, received, or accessed on District-issued devices or District systems may be reviewed by the District and may be subject to disclosure under the Idaho Public Records Act unless an exemption or other legal protection applies.

5. Personally-Owned Communication Devices

A. Employees may carry and use personally owned electronic communication devices during the school day on school property, subject to this policy and other applicable District policies.

B. Personally owned hand-held citizens band radios, portable police scanners, and long- or short-range walkie-talkies shall not be used or carried by employees on school property during the school day unless specifically approved by the employee's immediate supervisor based on a personal health or safety need or District operational need.

C. Personally owned devices may be used during duty time when used for school-related job duties and in accordance with this policy.

D. Personally owned electronic communication devices should not be used during the employee's normal duty time to send or receive messages of a personal nature, except during normal break times, lunch times, preparation times, or in circumstances involving personal health or safety.

E. Use of personally owned electronic communication devices should be limited during instructional time, student supervision, school-sponsored programs, meetings, in-services, parent/guardian conferences, or any other time when there is a reasonable expectation of quiet attentiveness, unless use is necessary for District business, personal health or safety, or an emergency.

6. Electronic Communications with Students

A. Electronic communications between District employees and District students shall be professional, school-related, and consistent with the Code of Ethics for Idaho Professional Educators, applicable law, and District policy.

B. Electronic communications between a District employee and a District student shall be conducted through District-approved devices and District-approved platforms. Approved devices and platforms are identified in Exhibit 5335E.

C. Employees who use a personally owned device for school-related electronic communication with students shall do so only in accordance with this policy and the District's approved device and platform guidance.

D. The Superintendent/designee may approve additional platforms or devices when needed for instruction, student activities, athletics, safety, or District operations.

7. Photographs, Video, and Audio Recordings of Students

A. Employees shall not secretly photograph, video record, or audio record students. Employees may photograph, video record, or audio record students without the student's knowledge only when necessary to document or report an emergency,

safety concern, student injury, disciplinary incident, suspected abuse or neglect, or other urgent school-related matter.

B. Employees may photograph, video record, or audio record students only for a specific, authorized, school-related purpose and only in accordance with applicable law, District policy, parent/guardian media permissions or restrictions, and student confidentiality requirements.

C. Before photographing, video recording, or audio recording students, employees shall ensure that the recording is necessary for the authorized school-related purpose and that the use is permitted under applicable parent/guardian media permissions, student confidentiality requirements, and District procedures. Employees shall not knowingly photograph, video record, audio record, post, publish, or externally share images or recordings of a student in violation of a parent/guardian restriction or applicable confidentiality requirement.

D. When practicable, employees shall use District-issued devices or District-approved platforms to photograph, video record, or audio record students for authorized school-related purposes.

    i. If a personally owned device is used for an authorized school-related purpose, the employee shall transfer the image, video, or audio recording to a District-approved storage location or platform as soon as reasonably practicable and delete it from the personally owned device.

E. Employees shall not retain student photographs, videos, or audio recordings in personal files, personal devices, personal cloud storage accounts, personal messaging applications, personal social media accounts, or other non-District-approved locations. Student photographs, videos, or audio recordings shall not be retained in District files or District-approved platforms unless retention is necessary for the authorized school-related purpose and complies with applicable District records, student confidentiality, and data-retention requirements.

F. Recordings made to document or report an emergency, safety concern, student injury, disciplinary incident, suspected abuse or neglect, or other urgent school-related matter shall be provided to the appropriate District administrator as soon as reasonably practicable and shall not be retained, posted, or shared by the employee except as authorized by the Superintendent/designee or required by law.

8. Violations / Discipline

A. Any employee who violates this policy may be subject to disciplinary action, up to and including termination.

B. When appropriate, the District may restrict, suspend, or revoke an employee's access to District-issued devices, District networks, District accounts, District-approved platforms, or other District technology resources.

C. Violations involving student safety, student privacy, harassment, discrimination, abuse, neglect, unlawful conduct, misuse of District resources, or unauthorized access to or disclosure of confidential information may be referred to the Superintendent/designee, law enforcement, the Professional Standards Commission, or other appropriate authorities.

9. Cross References:

A. Internet Publishing #2172 / #3279 / #5355

B. Digital Citizenship and Safety Education #2175

C. Student Owned Electronic Communication Devices #3265

D. Network and Device Responsible Use Agreement #3270 / #5330

E. Computer Use Agreement Signature Page #3270F / #5330F

F. Wireless Internet Access #3275 / #5335

G. Searches and Seizure #3370

H. Personal Conduct #5240

I. Abuse of School Property #5327 / #3325 / #4360

10. Legal References:

A. Idaho Code § 18-6726 — TikTok Use by State Employees on a State-Issued Device Prohibited

B. Idaho Code § 33-512 — Governance of Schools

C. Idaho Code § 33-513 — Professional Personnel

D. Idaho Code § 74-101 et.seq. Public Records Act

E. IDAPA 08.02.02.076 — Code of Ethics for Idaho Professional Educators

F. Idaho Executive Order 2022-06

11. Adoption and Review

A. Adopted: 01-10-2007

B. Reviewed:

C. Revised: 09-09-2026