

GARFIELD COUNTY SCHOOL DISTRICT
Policy DMB
Employee Use of District-Owned Electronic Devices

DRAFT — for board review and legal counsel review

Purpose—

The District provides electronic devices to employees to support the educational and business requirements of the District. The purpose of this policy is to establish standards for the responsible use, care, and security of District-owned electronic devices; to define the limited personal use of such devices that the Board authorizes; and to give notice of the monitoring, records, and disciplinary provisions that apply to all use of District devices. Policy DMA contains additional standards relating to personally owned electronic devices, and Policy EEB governs use of the District’s internet and network resources.

Utah Admin. Rules R277-495-3(1) (October 8, 2025)

Definitions—

“Electronic device” means a device that is used for audio, video, or text communication or any other type of computer or computer-like instrument, including a smart phone, a smart or electronic watch, a tablet, a laptop or desktop computer, or a virtual reality device.

“District device” means an electronic device owned, leased, or issued by the District, including any District-provided accounts, software, storage, and connectivity associated with the device.

“Incidental personal use” means occasional, brief personal use of a District device by an employee that conforms to the conditions of this policy, occurs at no more than negligible cost to the District, and does not interfere with the employee’s duties or the operations of the District.

“Inappropriate matter” means pornographic or indecent material as defined in Utah Code § 76-5c-208 and Utah Code § 53G-10-103.

Utah Admin. Rules R277-495-2 (October 8, 2025)

General requirements for use of District devices—

District devices shall be used in compliance with all federal, state, and local laws and regulations and in a cost-effective and ethical manner. Employee use of District devices must comply with Policy DMA, Policy EEB (internet and network use), Policy DAI (employee code of conduct), Policy DKB (sexual harassment), Policy DKBA (interactions with students), Policies FE and FEA (privacy of student records and information), and any other applicable District policies. Certified employee use of District devices must also comply with the Utah Educator Standards (see Utah Admin. Rules R277-217-1 and following).

An employee who is issued or provided a District device is responsible for that device at all times. Misuse of a District device may have employment consequences regardless of when or where the misuse occurs.

Utah Admin. Rules R277-495-4(3)(b) (October 8, 2025)

Use of a District device to access inappropriate matter is prohibited at all times and in all locations, whether or not the employee is on school property or on duty. Such use is also illegal, may have criminal consequences, shall be reported to law enforcement, and may have adverse employment consequences including termination from employment.

Utah Admin. Rules R277-495-4(1)(c), (3)(a) (October 8, 2025); Utah Code § 76-5c-208 (2026)

District devices must not be used in hacking (obtaining unauthorized access to or disrupting in any way) any network or electronic device, and must not be used to invade others' reasonable expectations of privacy, consistent with the recording and privacy provisions of Policy DMA.

Utah Admin. Rules R277-495-4(1)(e), (5)(a) (October 8, 2025)

Incidental personal use authorized (local provision)—

The Board recognizes that District employees are members of homes and communities, and that occasional personal use of a District device—such as personal email, family communication, civic and community obligations, and routine personal business—can often be accomplished at no cost to the District and without any interference with District operations. The Board therefore expressly authorizes incidental personal use of District devices as a de minimis employee benefit, subject to all of the following conditions:

- Incidental personal use is subject to the same standards of conduct as work-related use, including every requirement of this policy and of Policies DMA, EEB, DAI, DKB, DKBA, FE, and FEA. Authorization of personal use does not lower any standard.
- Incidental personal use may not occur during instructional time, during time when the employee has direct supervisory responsibility for students or school activities, or at any other time where there is a reasonable expectation of quiet attentiveness (consistent with the duty-time provisions of Policy DMA). Appropriate times include break times, lunch times, preparation times, and outside of regular duty hours.
- Incidental personal use must not interfere with the employee's job performance or the work of others, and must not burden District systems, storage, or connectivity beyond a negligible degree.
- District devices may not be used for personal financial gain, an outside business or employment, commercial solicitation, political campaigning, or advocacy for or against a ballot proposition.
- Employees may not install personal software or applications on District devices, alter security or filtering configurations, or connect District devices to services that circumvent District content filtering.
- District devices should not be used as the storage location for substantial personal files, including personal photo or video libraries. Personal information stored on a District device may be lost without notice when a device is re-imaged, repaired, reassigned, or returned, and the District is not responsible for such loss.

- Personal use must not commingle personal accounts or personal files with student data or District records, and must not create confusion as to whether a communication is made in the employee's personal or official capacity.

Incidental personal use within these conditions is authorized use of District property. Personal use outside these conditions is unauthorized and may violate the Utah Public Officers' and Employees' Ethics Act in addition to this policy.

Utah Code § 67-16-4; Utah Admin. Rules R277-495-4 (October 8, 2025)

No expectation of privacy; monitoring and records—

District devices, accounts, networks, and all information created, stored, sent, or received on them remain the property of the District. Employees have no expectation of privacy in any use of a District device, including authorized incidental personal use. The District may access, monitor, filter, audit, and review any District device or account at any time, with or without notice, for any lawful purpose.

Records created or stored on District devices may be subject to the Government Records Access and Management Act (GRAMA), to litigation holds, and to District records-retention requirements, regardless of whether the content is personal in nature. Employees who do not wish personal communications to be subject to these provisions should conduct them on personally owned devices consistent with Policy DMA.

Utah Code § 63G-2-101 and following (GRAMA)

Care, security, and return of devices—

Employees shall exercise reasonable care to protect District devices from loss, theft, and damage, shall follow District requirements for passwords, authentication, updates, and security, and shall promptly report any lost, stolen, or damaged device to their supervisor and the District technology department. District devices and associated accounts shall be returned upon request or upon separation from employment. An employee may be held responsible for use or misuse of a device issued to the employee, including use by other individuals the employee permits to access the device.

Utah Admin. Rules R277-495-4(3)(b) (October 8, 2025)

Training and notice—

This policy shall be included in the employee training provided within the first 45 days of each school year under Policy DMA, and shall be available on the District's website in the same location as the District's data governance plan, at the District office, and at school administration offices.

Utah Admin. Rules R277-495-3(4), R277-495-5 (October 8, 2025)

Consequences for violating policy—

Violation of this policy or of Policies DMA or EEB may result in withdrawal of the incidental personal use privilege, restriction or revocation of device access, and disciplinary action against the employee up to and including termination of employment. Violations involving illegal conduct shall be reported to law enforcement.

Utah Admin. Rules R277-495-4(5)(c) (October 8, 2025)