



Book	Fort Plain CSD Policy Manual
Section	6000: Personnel
Title	Staff Use of Computerized Information Resources
Code	6470
Status	Active
Adopted	July 7, 2005
Last Revised	November 19, 2025

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES

The Board of Education will provide staff with access to various computerized information resources through the District's computer system (DCS hereafter) consisting of software, hardware, computer networks, wireless networks/access and electronic communication systems. This may include access to electronic mail, so-called "on-line services" and the "Internet." It may also include the opportunity for staff to have independent access to the DCS from their home or other remote locations, and/or to access the DCS from their personal devices. All use of the DCS and the wireless network, including independent use off school premises and use on personal devices, shall be subject to this policy and accompanying regulations.

The Board encourages staff to make use of the DCS to explore educational topics, conduct research and contact others in the educational world. The Board anticipates that staff access to various computerized information resources will both expedite and enhance the performance of tasks associated with their positions and assignments. Toward that end, the Board directs the Superintendent or his/her designee(s) to provide staff with training in the proper and effective use of the DCS.

Staff use of the DCS is conditioned upon written agreement by the staff member that use of the DCS will conform to the requirements of this policy and any regulations adopted to insure acceptable use of the DCS. All such agreements shall be kept on file in the District office.

Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance shall apply to use of the DCS. Employees are expected to communicate in a professional manner consistent with applicable District policies and regulations governing the behavior of school staff. Electronic mail and telecommunications are not to be utilized to share confidential information about students or other employees.

Access to confidential data is a privilege afforded to District employees in the performance of their duties. Safeguarding this data is a District responsibility that the Board of Education takes very seriously. Consequently, District employment does not automatically guarantee the initial or ongoing ability to use mobile/personal devices to access the DCS and the information it may contain.

This policy does not attempt to articulate all required and/or acceptable uses of the DCS; nor is it the intention of this policy to define all inappropriate usage. Administrative regulations will further define general guidelines of appropriate staff conduct and use as well as proscribed behavior.

District staff shall also adhere to the laws, policies and rules governing computers including, but not limited to, copyright laws, rights of software publishers, license agreements, and rights of privacy protected by federal and state law.

Staff members who engage in unacceptable use may lose access to the DCS and may be subject to further discipline under the law and in accordance with applicable collective bargaining agreements. Legal action may be initiated against a staff member who willfully, maliciously or unlawfully damages or destroys property of the District.

Confidentiality, Private Information and Privacy Rights

Confidential and/or private data, including but not limited to, protected student records, employee personally identifying information, and District assessment data, shall only be loaded, stored or transferred to District-owned devices equipped with encryption and/or password protection. This restriction, designed to ensure data security, applies to devices within the District Computing Systems (DCS), any mobile devices, and any systems accessing the DCS from remote locations. Staff are strictly prohibited from using personal cloud-based storage accounts (such as Dropbox, Google Drive, OneDrive, iCloud, Box, etc.) files to store any District-related data. Staff must only use the District-provided cloud-based storage (Google-Drive), collaboration, and file-sharing needs.

The use of personal external USB storage devices (including flash, portable hard devices, or any other removable media) for storing or transferring District data is strictly prohibited. Only District-issued and encrypted storage devices may be used with prior authorization.

Staff will not use email to transmit confidential files in order to work at home or another location. Confidential files will not be stored or transferred through any non-District-approved platforms or devices.

Staff will not leave any devices unattended with confidential information visible. All devices are required to be locked down while the staff member steps away from the device, and settings enabled to freeze and lock after a set period of inactivity.

Staff data files and electronic storage areas shall remain District property, subject to District control and inspection. The computer coordinator may access all such files and communications to insure system integrity and that users are complying with requirements of this policy and accompanying regulations. Staff should **NOT** expect that information stored on the DCS will be private.

Electronic Transmission of Student PII

All staff members are required to exercise the highest degree of diligence when transmitting student Personally Identifiable Information electronically. In order to ensure the secure handling of such information:

1. Any electronic communication that contains multiple forms of student PII (e.g., a student's name combined with date of birth, address, Social Security number, or other unique identifiers) shall be transmitted only through the District's designated secure encryption system (e.g., Serv-U).
2. Electronic communications that contain a single form of student PII only (e.g., a student identification number without any additional identifiers) may be transmitted through the District's internal systems imbedded with standard encryption safeguards.

When determining the appropriate method of transmission, staff must exercise professional judgment and, in cases of uncertainty, utilize the District's more robust encryption system to ensure maximum data protection.

Implementation

Administrative regulations will be developed to implement the terms of this policy, addressing general parameters of acceptable staff conduct as well as prohibited activities so as to provide appropriate guidelines for employee use of the DCS.

NOTE: Refer also to Policies #5672 -- Information Security Breach and Notification
#5676 -- Data Privacy and Security Policy
#6471 -- Use of Email in the District
#7317 -- Student Use of Personal Technology
#8271 -- Internet Safety/Internet Content Filtering Policy

Adopted: 7/7/05
Revised: 1/8/14