

Policy IIBF – Use of District Technology Resources

Fremont Co School District #1 strongly believes in the value of instructional technology, the Internet, and other online information resources. Such resources can increase the power of curriculum content standards, enable exciting collaborations, increase productivity, and improve student learning. Access to a wide variety of software, multimedia content, instructional applications, and Internet resources is an integral part of education at Fremont #1. These services are provided to promote educational excellence in schools, support our curriculum, and support individual academic needs.

The use of electronic information resources is a privilege, not a right. Use of resources and levels of access are determined by job requirements. Inappropriate use of these resources may result in disciplinary action (including the possibility of termination) and/or referral to legal authorities. The superintendent or her/his designees may monitor, limit, suspend, or revoke access to electronic resources at any time for any reason.

Scope of policy

This policy includes any and all District-owned technology resources, including smartphones, cellular phones, computers, tablets, desk phones, servers, any other hardware, wired and wireless networks, the Internet, the District Intranet, electronic mail systems, purchased software and subscriptions, and any other elements of the District's computer, telecommunications, or electronic communication / information systems.

General Statement: Network usage

The Fremont #1 district network has a limited educational purpose which includes the use of its system for classroom activities, district administration, professional development, and other job-related activities. Users are expected to use Internet access through the Fremont #1 network to advance educational and professional goals consistent with the mission of Fremont County School District #1 and its policies; other use may be permitted so long as the use does not unduly burden District resources and does not interfere with job function or performance. However, some uses which may be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose system which the District provides.

General Statement: No expectation of privacy

Network and Internet access is provided as a tool for education. The District reserves the right to monitor, inspect, copy, review, and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted, received, or stored in connection with such usage. All such information files shall be and remain the property of the District, and no staff or student shall have any expectation of privacy regarding such materials. The District may share such transmissions with administration, law enforcement, and other entities that the District deems important. All digital storage is considered to be District property, and designated administrators will review files and communications to maintain system integrity and ensure that technology is used responsibly. Staff members should not expect that files stored on District servers or computers will be private. Electronic communications systems are potentially subject to the Public Records law which means that any e-mail or other content sent, received, or stored on the school district's technology systems could become public information (i.e., appear in a newspaper) or be subpoenaed for court purposes.

Security and confidentiality

Network and information security is a critical component for the operation and safety of the school district and its patrons. Network and applications user accounts and passwords are considered confidential and private information. At no time will staff share their network and/or application passwords with any student, volunteer, parent, or other staff, unless with the express prior approval of administration.

Student use of staff computers

Students are not to use a computer that a staff member has logged into, unless in a situation where a staff member is providing constant guidance and direct supervision of the student. At no time will staff allow

students to access a protected application (such as Infinite Campus) that contains confidential or private information.

Protecting data and access to network applications

The Technology Office, in conjunction with other appropriate departments, will develop, implement, and monitor procedures and protocols for the handling of confidential and secure information.

FERPA - Family Educational Rights and Privacy Act

Privacy of student information and adherence to the Family Educational Rights and Privacy Act is required. District employees shall not transmit or electronically publish material regarding students, parents/guardians, or employees that is protected by confidentiality laws, except as legally permitted. If material is not legally protected but is of a confidential or sensitive nature, great care shall be taken to ensure that only those with a “need to know” are allowed access to the material. Staff members shall handle all employee and student records in accordance with all relevant District policies.

Use of third-party or non-district applications or subscriptions to store District work

The District has the expectation that any confidential District work is to be stored within District-owned applications or within District-sanctioned services and subscriptions. By doing this, appropriate security and confidentiality can be maintained, and content can be recovered if necessary in the case of error or staff departure.

Ownership and copyright of content and materials

Content and materials created on District equipment by District staff during work time are the property of the Fremont #1 school district and may be altered, used, or transferred as the District deems appropriate.

Electronic communications usage and expectations

The primary purpose of email, web posting, and other collaborative and communication applications are provided to District staff in order to facilitate information exchange and classroom collaboration consistent with the educational mission of the District. Incidental personal use of resources is allowed as long as such use falls within policy guidelines and building and supervisor expectations. In any case, staff may not use these communication methods in ways inconsistent with the mission and expectations of the District.

Content posting standards

It is expected that any Internet posting or communication made by staff exhibits professionalism, uses good grammar and writing style, and positively reflects their classroom, their school, and the District. This includes but is not limited to email, website posting, blog comments, and Twitter usage. Personal politics, beliefs, and non-educational content should not appear on District-sanctioned web properties. Pages should be kept professional and current. Pages should also follow school and district expectations regarding content and communications.

Teacher-student communications

The District recognizes the value of 21st century communications and endeavors to incorporate these new methods of communication and collaboration into daily instruction. For security and safety for both employees and students, all students in grades 6-12 are provided with a district-managed email address. Likewise, all staff are provided with district-managed email accounts for communication with parents, students, peers, and others. These sanctioned accounts are managed and can be monitored if necessary to ensure District regulations are being followed. Except in special situations approved by administration, employees are strongly discouraged from communicating directly with students via private email addresses. Communication from a staff email address to a district-sanctioned student email address is part of normal communications and does not require approval; however, the communication must be school-related and should not be of a personal nature. Texting (using mobile phones for quick communications) between teachers and students is only permissible as long as such communication is school-related (for instance, coordinating a field trip schedule).

Use of social networking applications and communication methods

The District also recognizes the value and role of social networking technologies in today's world. However, "friending" students and using non-public communications can lead to misunderstandings and potentially unprofessional contact. Staff members are encouraged to use district-approved applications and subscriptions (such as our district Edmodo subscription) for classroom collaboration and social networking applications, as these provide a managed and safe environment for all. Using other social networking sites, "friending" students, and allowing non-professional contact via third-party sites is strongly discouraged.

Use of personal devices

In today's world, many staff choose to supplement or augment District resources by using personal equipment (smartphones, mobile computers, etc.) to connect to Internet resources and content. The use of personal devices in the workplace is acceptable, but limited to "guest" resources made available to District visitors. Personal equipment should not be connected to the general wired or secure wireless networks, except in extraordinary situations and only with the approval of administration and the technology director. Under no circumstances are District personnel obligated to provide support, maintenance, repair, or goods in response to the use or misuse of personal technology.

Accessing inappropriate material

Internet users may encounter material that is controversial which the user or District may consider inappropriate or offensive in an educational setting. The district has taken precautions to restrict access to inappropriate materials through several different layers of filtering and monitoring systems. However, it is impossible for any filtering device or regimen to control access to all content that a user may purposefully pursue or inadvertently discover on the global Internet. It is the user's responsibility not to purposefully initiate access to such material. Any site or material inadvertently accessed that is deemed controversial should be reported immediately to the appropriate administrator. The District expressly disclaims any obligation to discover all violations of inappropriate Internet access.

Employee equipment usage and checkout

The District may provide mobile technology (mobile computers, tablets, smartphones, etc.) to employees whose job descriptions require mobile access to District resources. Equipment needs and placements are determined by building administrators and the Technology Office. The use of mobile equipment outside of District boundaries is subject to the same expectations and limitations outlined in this policy (including privacy expectations) and staff may not use these devices in ways inconsistent with the mission and expectations of the District. Employees are expected to take reasonable steps to care for and secure equipment in their possession. Employees will immediately return any District equipment upon their resignation or departure, or when requested by District administration.

Contracted staff

The District may, at the approval of the Superintendent or his/her designee, grant limited access to District resources to non-District staff. Such access will be granted for specific applications and tasks related to the contract staff's appointment and job requirements. Contracted staff may be required to sign their acceptance of Policy IIBF before access is granted.

Applicability of other District policies

Other District policies and regulations (such as bullying and harassment) also apply to any District electronic communications or user-created content, even if they are not explicitly detailed in this policy.

Notification

The District annually notifies students and parents by a student-specific usage agreement which is included in the student handbook for each of our secondary schools. Also, students are reminded annually via fall orientation about expectations regarding technology usage. The District notifies staff by way of a signature

form that all District staff are required to sign stating they will abide by all district policies related to nondiscrimination, sexual harassment, and technology usage.

Disclaimer

Fremont County School District #1 makes no warranties of any kind, whether expressed or implied, for the technology and Internet services it is providing. The District will not be responsible for any damages suffered by users, including loss of data resulting from delays, non-deliveries, incorrect deliveries, or service interruptions caused by its own negligence, user errors, omissions, or factors beyond the control of the District. Use of any information obtained via the Internet is at the user's own risk for the user's own purpose. The District specifically denies any responsibility for the accuracy or quality of information obtained through its Internet access. The district does not warrant that the functions of the system will meet any specific requirements or that it will be error-free or uninterrupted. The District shall not be liable for any direct or indirect, incidental, or consequential damages (including lost data, information, effort, or monetary loss) sustained or incurred in connection with the use, operation, or inability to use any aspect of the system or service.

Adopted: April 17, 2012