Fayetteville-Manlius Acceptable Use Guidelines

Staff

The District believes that computer technology is an integral component of instruction and support services. The fundamental characteristics of computer technology in our school environment are instructional efficacy, operational efficiency, appropriate student and personnel access and confidentiality, accountability, and effective supervision.

This Acceptable Use Guideline governs the usage of all technology that is purchased or brought to any school or office in the Fayetteville-Manlius District. This includes all phones, laptops, audio devices, external drives, cameras, interactive whiteboards, and any device that has the capability to connect to the internet. All technology brought from outside the district must adhere to the District's internet policy, and is subject to administrative regulations. All student use of computers will be supervised by classroom teachers, teaching assistants, aides and lab assistants working in the computer labs, classrooms and with mobile labs.

The above is the splash page. The user will then click next to go to the information below.

Reservation of Rights

The district has the right to set the priority of the use of technology as it sees fit. It is understood that the priority of technology is for the instruction of students. There are times when instruction is interrupted for emergency repair or processing by network technicians.

The district reserves the right to limit the amount of data transmitted over the network and internet. The district has the right to cancel or suspend accounts in response to any violations to the District policy, and cooperate with legal authorities in investigations of illegal activity.

The District will monitor all communications into, and out of, its network facilities to prevent the introduction of viruses or other hostile code, to prevent intrusions and otherwise to enforce this Policy.

Enforcement

Depending on the nature and severity of a violation, an administrator may take disciplinary action ranging from verbal or written warning, to access denial, to suspension for students or discipline with employees with accordance to contract and law. If warranted, the administrator shall refer the case to an appropriate school, local, state, or federal authority for disposition. Restitution for willful property damage will be required.

Evidence of attempted or actual system security, integrity, or performance-related incidents shall be cause for immediate access denial. The purpose of access denial in these cases is to prevent further damage to the system or data while an investigation is conducted. If there is evidence that a user took actions to violate a policy, but was unsuccessful, it will be considered a violation.

Personal Use

The District permits staff incidental personal use of computers as long as the personal use does not:

- occur during instructional time (planning time is included as instructional time)
- interfere with the employee's job performance
- violate district policy or regulations
- damage district property
- use more than a trivial amount of resources
- interfere with education
- interfere with office productivity
- interfere with network speed
-

Privacy

Anyone using technology in the District should not expect any privacy with regard to District technology resources especially with email or other files maintained on the District's computer system or individual computers. The District monitors the use of all computer technology including but not limited to individual keystrokes, use of internet sites, the District's computer system and email.

Acceptable Use Guidelines

All users must avoid the following inappropriate uses of the District's network and computer resources. The following is a list of some but not limited to appropriate uses of the District's network and computer resources.

- Using resources for personal gain or profit
- Degrading or disrupting equipment, software or system performance
- Violating security including the spread of computer viruses, trojans, worms, or any program designed to violate security, interfere with the proper operation of any computer, or destroy data
- Using information and/or data obtained through network and computer resources without giving proper credit to the source (plagiarism)

- Interfering with the work of others
- Vandalizing the data of another user
- Using resources in any manner that violates Board policy, federal, state, or local law, including unauthorized copying or transmission of software, music, and video (i.e. Torrent, but not exclusive of peer to peer sharing)
- Evading the internet filter (Using proxies)
- Gaining unauthorized access to systems and networks
- Invading the privacy of individuals
- Using an account owned by another user, or allowing another user to use your account
- Misleading staff about the nature of "work" for which one is using the network
- Posting personal communications without the original author's consent
- Posting anonymous or falsely identified messages
- Initiating or forwarding "chain" e-mails or mass emails not approved by the administration.
- Downloading, storing, printing or distributing files or messages that are profane, obscene, threatening, or that use offensive, lude or indecent language that degrades others
- Downloading, storing, printing or distributing files or messages that contain information considered dangerous to the public at large
  Unauthorized advertising and soliciting on school computers, including sending messages from a home or other outside computer to school district email users

Harassment

School policies, administrative regulations, and procedures against sexual harassment and other forms of discriminatory harassment apply equally to communications through any technology including but not limited to school computer systems and cell phones.

Security

The district is not an insurer of computer technology security. Security is the responsibility of every user. Security guidelines and recommendations are stated in the Staff Handbook for Technology. Users are restricted to only the applications used. Records kept by staff members will not share any information except authorized by Federal and State law.

Security is the responsibility of every user to:

- check computers for key loggers,
- keep passwords private,
- use passwords when students are away from the computer,

- lock the computer when leaving the immediate area of the computer (control, alternate, delete).

Security measures that are maintained include:

- offsite/secure storage of backup data,
- internet firewalls and filtering software,
- remote monitoring,
- network password protection
- workstation password protection.

Security audits are performed on a regular basis.

Application Copyrights and Licensing

Software may not be used in violation of licensing or copyright laws.

Individuals must obtain written permission from the copyright owner before duplicating information for which that individual or the District does not hold the copyright or as otherwise premitted by the District's copyright policy. Any user who learns of the misuse of software-related documentation shall notify an administrator.

Copying District Application Software

Computer users within the District shall not copy software provided by the District to any storage medium such as a USB drive, hard disk drive, tape, or CD-ROM. District users are not allowed to change the software configurations of computers or make copies or transfers that may violate licensing agreements with software vendors.

Software Installation and Configuration

All software for staff and student use shall be installed, configured, and tested by authorized staff.

COMPUTER ELECTRONIC MAIL

The District’s educational and office environments are enhanced when electronic mail (email) is used appropriately. The District will provide email resources to staff and students on an authorized basis. While it does not seek to interfere with the use of these resources, the District will take reasonable actions to ensure the appropriate use.

All users are to be accountable for their conduct as it relates to use of the email system. The District does not accept responsibility for information shared or opinions expressed by individuals or groups using its email system. The District may restrict an email privilege to any user whose conduct is not consistent with this Administrative Regulation or any associated rule.

Neither students nor staff should have any expectation of privacy when using email on district owned networks. The District retains the right to monitor or print any data found on its email sent.

User Accountability

Users of the District's email system are accountable for all actions they take either individually, or as part of a group. Any email sent from a school computer contains a return address identifying the school district. Accordingly, staff shall take steps to insure their own statements are not mistakenly attributed to the District.

In addition to email, all electronic communications such as Information posted by staff or students to email systems, electronic bulletin boards, or other information sharing systems is not necessarily a formal statement by, or an official position of, the District.

Student Use of email

Student access to email accounts is intended for school related purposes only.

Privileges

Email privileges will be restricted for any user who knowingly abuses the purpose for which the email system was implemented.

Inappropriate Uses of Email

Use of the District email system is prohibited if it involves:

- harassing, insulting, threatening, or attacking others electronically
- downloading, storing, displaying, sending or printing files or messages considered obscene, profane, threatening, or language that is offensive, lude or degrades others initiating or forwarding a "chain" letter
- posting personal communication without the original author's consent downloading, storing, printing, or distributing files or messages that contain information considered dangerous to the public at large
- posting anonymous or falsely-identified messages
- permitting a third party to send a message from the user's email account
- posting contact information about anyone without their permission

Purging email

The district is not responsible to the user for backing up and archiving data. All student data is deleted at the end of the school year. Other user data may be deleted by the district at any time as the district deems necessary.

Security

Email and/or email attachments received from the Internet to District email accounts shall be screened for viruses or other destructive programs or macros before entering the District network. Any email that fails the virus examination shall be rejected.

Email Communication Between Home and School

All users of school email should be aware that it is not confidential and is stored electronically. Teacher-student email is at the discretion of the individual teacher. Teachers choosing to use email as a communication tool with their students must use the district provided email accounts.

COMPUTER INTERNET USE AND SAFETY

When used appropriately, the Internet is an important resource for students and staff. It provides a connection to a variety of information sources, educational institutions, and Internet users throughout the world. The Internet fosters research and encourages resource sharing, innovation, and communication.

Despite district safeguards, including firewall and filtering/blocking software, a determined user may be able to gain access to inappropriate or unauthorized services on the Internet. Therefore, it is recognized that students may gain access to information and communications that they (or their parents) find inappropriate, offensive, or controversial. Parents and guardians assume an inherent risk in using this technology.

The District does not sanction any unauthorized use of the Internet. Users granted access to the Internet through the District's resources assume personal responsibility, both civil and criminal, for uses of the Internet not authorized by Policy or administrative regulation.

Appropriate Uses of the Internet

The District provides Internet access for appropriate uses only. The following are some appropriate uses of the Internet:

- Completing an assignment, conducting research, and contacting individuals as directed by a teacher.

- Using electronic mail or other digital communication methods to communicate with people inside and outside the District.
- Exploring the Internet to learn more about how to use computers, networks and the Internet.
- Gaining access to information.

Inappropriate Uses of the Internet

The following are examples of inappropriate uses of the Internet:

- Using or disseminating information obtained from the Internet without verifying the integrity and authenticity thereof
- Using information and/or data obtained through network and computer resources without giving proper credit to the source (plagiarism)
- Violating copyright law
- Using the Internet for financial or commercial purposes
- Violating Policy or administrative regulations
- Downloading unauthorized programs and using proxies (allows user to bypass security or filters)

Computer Internet Safety

School policies, administrative regulations, and procedures against sexual harassment and other forms of discriminatory harassment apply equally to communications through any technology including but not limited to school computer systems and cell phones.

The District provides Internet access for appropriate uses only. Supervision and technology will be used to restrict Internet access to authorized users for appropriate purposes. The District filters the internet as defined by the Children's Internet Protection Act (CIPA). The following technology protection measures are used to prevent inappropriate use of the Internet:

The District will employ passwords at all grade levels to limit Internet access to authorized users only.
The District will employ commercially available Internet filtering/blocking software to protect against access through their computers to visual depictions that are obscene, pornographic or harmful to minors.

The District will instruct students on internet safety and best practices.

Only groups of users that receive permission granted by the Computer Committee and the Coordinator of Technology for bona fide research or other lawful purpose will be allowed to bypass the filtering/blocking software.

Internet access and use will be screened and logged. Inappropriate use as defined by this regulation shall be immediately reported to the building administrator and the Coordinator of Technology.

Internet access through District resources requires that all student users read, acknowledge and sign the Student Acceptable Use Agreement. This agreement requires the user to abide by the District's "Internet Use" Policy and this Regulation.
At the discretion of an administrator, teacher, and/or lab assistant, further limits to Internet access may be imposed.

Social Networking

Any personal web pages, blogs, or social sites cannot link to District web pages. Photographs of students cannot be included in personal pages.

I ACKNOWLEDGE AND UNDERSTAND MY OBLIGATIONS (staff member selects submit button)

For District policy and regulations go to
http://www.fmschools.org/departments.cfm?subpage=9896