

STAFF ACCEPTABLE USE POLICY

Sycamore CUSD #427

The following form must be read by each member of the District staff as a condition to using the District's Computer Network. The Computer Network shall include all computer hardware and software, all information accessed by Internet sites, E-Mail, the District's web site, on-line services and bulletin board systems.

Access to the Computer Network exists to support the District's educational responsibilities and mission and is provided as a privilege by the District. The specific conditions and services that are offered will change from time to time. In addition, the District makes no warranties with respect to the Computer Network, and it specifically assumes no responsibilities for:

1. Any costs, liability, or damages caused by the way the personnel misuses his/her Computer Network access;
2. Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the District;
3. The privacy of electronic mail; or
4. Any retrieval of or access to illegal, obscene or indecent material or information.

Acceptable Use

The use of on-line network computer services must at all times be in support of education and research consistent with the educational objectives of Sycamore CUSD #427. All users of the computer network and computers (the "Computer Network") at the District must comply with all rules and regulations, guidelines, terms and conditions.

Prohibited Use

Unethical and unacceptable behavior as defined below is prohibited and shall result in disciplinary action which may include all discipline available under the District's policies, suspension or denial of Computer Network privileges or appropriate legal action.

Unethical and unacceptable use of the Computer Network shall include, but not be limited to:

1. Use of the Computer Network to access, retrieve, or view obscene or indecent materials. Obscene or indecent materials are those materials which, in context, depict or describe in terms patently offensive, as measured by contemporary community standards and do not have any serious literary, artistic, political or scientific value.
2. Use of the Computer Network to access, retrieve or view or disseminate any material in violation of any U.S. or state regulation or school policy. This includes, but is not limited to, improper use of copyrighted material, improper use of passwords or access codes, disclosing any user's full name, home address, or phone number or that of another student or teacher.
3. Use of the Computer Network to transfer software program files to or from the school computer.
4. Use of the Computer Network for profit from commercial activities including advertising or sales.
5. Use of the Computer Network in a manner that is directed toward or intended to harass, threaten, intimidate or demean an individual or group of individuals because of sex, color, race, religion, handicap, national origin or sexual orientation.

6. Use of the Computer Network to substantially threaten or actually disrupt the educational process or interfere with the rights of others at any time either during school days or after school hours.
7. Use of the Computer Network in any manner, which intentionally disrupts the information network traffic or interferes with the network and/or connected systems.
8. Use of personal equipment attached, connected, and/or installed to any district equipment.
Exceptions: Flash or jump drives
9. Use of the Computer Network to gain unauthorized access to the files of others or vandalize the data or files of another user.
10. Use of the Computer Network to gain access to unauthorized areas.
11. Use of the Computer Network to improperly forge or alter electronic mail messages or to use an account owned by another user.
12. Use of the Computer Network to invade the privacy of any individual.
13. Use of the Computer Network to download, copy, print or otherwise store or possess any data, which might be considered in violation of these rules.

Personal Use

School computers, networks, Internet access and e-mail are provided to support the educational mission of the district. They are to be used primarily for school-related purposes. Incidental personal use of school computers must not interfere with the employee's job performance, must not violate any of the rules contained in this policy and must not damage the District's Computer Network or Equipment. Personal privacy does not apply on district-owned computers as the District has the right to track network, e-mail and Internet usage.

Confidentiality

District employees are not to transmit confidential information concerning students or others. An e-mail message may constitute an "education record" which is protected under the law.

Advertising

Advertising and solicitation on district computers is prohibited. This includes district employees sending advertising messages from a home or outside computer to school district e-mail users.

Fund-raising, non-profit or charitable solicitation

The use of the Computer Network for transmitting announcements of non-profit or charitable events other than those of the District is prohibited.

Representing personal view(s) as those of the school district

Any e-mail sent from a district computer contains a return address which identifies the school district. Therefore, sending an e-mail is the same as using school letterhead and should be used with caution.

Installing software programs without permission

The cumulative effect of software program installation, including downloading of software programs from the Internet for installation on district computers, in terms of degradation of performance, virus transfer, maintenance, and copyright/licensing issues can be significant. Therefore, no software installation on District computers is allowed without pre-approval from a building technology coordinator.

E-mail usage

District employees are asked to follow these procedures when utilizing e-mail:

- a. Be polite and nonabusive in messages to others.
- b. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
- c. Do not reveal the personal addresses or telephone numbers of students or colleagues.
- d. Do not use another person's e-mail account.
- e. Recognize that electronic mail is not guaranteed to be private.
- f. Do not type in all caps as this is recognized as shouting.
- g. Proofread your message before sending it.
- h. Perform regular e-mail maintenance. Check e-mail daily. After reading e-mail, decide what action to take – delete, reply, print or archive.
- i. Delete messages from the mailbox as well as from the sent box regularly. Fair utilization of file server space is necessary from all staff.
- j. The district e-mail system is provided for efficiency in the operation of school business and educational goals. Therefore, forwarding chain letters, jokes, movie files and graphics is discouraged.
- k. Use care in opening attachments. If an attachment file extension is not recognized (like .ppt or .doc) or if the sender is unknown or not recognized, it is best not to open the attachment. Delete it as it might be a virus. It is normal procedure to tell a person in advance that an attachment is being sent to them, so he/she expects its arrival.

Disclaimer

The District makes no warranties of any kind whether expressed or implied for the Computer Network. The District will not be responsible for any damages suffered including the loss of data resulting from delays, non-deliveries, misdeliveries or service interruptions. Use of any information obtained via the Computer Network is at the user's own risk. The District denies any responsibility for the accuracy or quality of information obtained through the Computer Network.

Security

Security in any network is a high priority and must be a priority for all users. If any user of the Computer Network is aware of any security risk or abuse of the Computer Network, the personnel member must notify an administrator immediately. Students and personnel are prohibited from sharing their log-in ID or password with any other individual. Any attempt to log onto the Computer Network as another individual will result in immediate cancellation of system privileges.

Vandalism

Any vandalism or attempted vandalism (physical or electronic) to District computers, the District network, files of others or to the Computer Network in any way is prohibited and will result in immediate cancellation of Computer Network privileges, disciplinary action and potential legal action. Vandalism includes, but is not limited to, the downloading, uploading or creation of computer viruses.