The Cinema School
Computer and Internet
Acceptable Use Policy

Access to computer systems and networks owned or operated by The Cinema School (TCS) of The New York City Department of Education (DOE) imposes responsibilities and obligations and is granted subject to Department of Education and school policies, and local, state, and federal laws.

Appropriate Use should always reflect academic honesty, high ethical and moral responsibility and show restraint in the consumption of shared resources. Appropriate use demonstrates respect for intellectual property, ownership of data, system security mechanisms, and for individuals' rights to privacy and rights to freedom from intimidation, harassment and unwarranted annoyance.

1. Appropriate Use of the System

- Given TCS educational mission and the need to provide all users fair and reasonably equitable access to the system resources, the following statements describe both appropriate and inappropriate use of computer resources: IMPORTANT - If you have question or need clarification concerning any of the policy, you should contact the Mr. Ojeda in Room 118 BEFORE ATTEMPTING TO USE THE SYSTEM.
- Files owned by individual users are to be considered private, whether or not they are accessible by other users. The ability to read a file does not imply the permission to read or use that file.
- Files owned by individual users are to be considered private, whether or not they are accessible by other users. The ability to read a file does not imply the permission to read or use that file. Files created in public directories are subject to deletion without prior notice to the user.
- Do use the system resources ONLY for valid educational purposes.
- Do refrain from deliberately engaging in activities that are intended to hinder another user's ability to do their work. You have the right not to be harassed while using the computer facilities. Harassment in the form of physical, verbal, electronic or any other form of abuse will not be tolerated. Harassment should be reported to a teacher or the systems administrator immediately.
- DO NOT transmit or store any information, which contains obscene, indecent, lewd or lascivious material, or other material, which explicitly or implicitly refers to sexual conduct.
- DO NOT transmit information which contains profane language or panders to bigotry, sexism, or other forms of discrimination; this includes files in any and all directories that are group or world-readable.

- DO NOT use computer programs to decode passwords or access control information.
- DO NOT attempt to circumvent or subvert system security measures.
- DO NOT engage in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files.
- DO NOT develop or use programs that attempt to consume all of available system resources (memory, swap space, disk space, network bandwidth, etc.)
- DO NOT use mail or messaging services to harass, intimidate, or otherwise annoy another person, for example, by broadcasting unsolicited messages or sending unwanted mail.
- DO NOT use the school's systems for financial gain and/or for profit. If in doubt, ask the systems administrator first.
- DO NOT create, modify, execute or retransmit any computer program or instructions intended to obscure the true identity of the sender of electronic mail or electronic messages including, but not limited to, forgery of messages and/or alteration of system and/or user data used to identify the sender of messages. Deliberate alteration of system files is vandalism or malicious destruction DOE property.
- Do abide by the Internet policies, TCS school policies, and local, state, or federal statutes and regulations concerning the use of computing facilities.
- DO NOT engage in any other activities that fail to comply with the general principles presented above.
- Do use ONLY use your own user name and password to access the log in. You may not allow other users to use you user name and password to log in. This is for you own protection as well as the protection of the system in general. You are responsible for any and all activity initiated in or on any Bronx Science TCS system by your account.
- Do keep you password confidential. Our security software will require that you change it at regular intervals. It should not be a dictionary word or common phrase.
- Do manage your use of system resources so as to minimize the impact of you activities on other users. Use only the resources that you need to complete your activity. Learn how to use the resources efficiently.
- Do modify only files belonging to you and files to which you have group write access to. Create them only in you own directories unless given explicit permission to use other directories. Merely having write or execute capability enabled on a file or directory does not constitute explicit permission. Users are responsible for protecting their own files and data from reading and/or written by other users.
- Individuals who use computers and/or the network inappropriately

are subject to disciplinary action by TCS, DOE, City, State and Federal authorities.
- Misuse of computer resources is not limited to incidents involving only TCS equipment. Inappropriate use of computing facilities external to our network, but accessed through or by our network will be considered an inappropriate use of our network.

2. Work Priorities:

The network is an intensively used resource. Network users must abide by the following priority system:

Priority Type of Work

1.System Maintenance by Sys Admins

2.Completion of student's course assignments, including film editing

3.Faculty use

4.E-mail

5.All other work

If you have work of higher priority than a user occupying a seat, you have the right to ask that user vacate the seat. The activity of the user occupying the seat should be used to determine relative priorities of you and their activity. This means that if you mix activities of differing priorities, you run the risk of losing your seat and not being able to complete you higher priority work because you may be asked to vacate your seat while you are engaged in a lower priority activity.

3. Games

Playing games is prohibited.

4. E-Mail

The systems administrator may regulate the content of private, electronic mail communication between users when necessary.

5. Privacy

The systems administrator, in order to preserve the integrity or operational state of the network, may look at data or files on the system.
You should be aware that no computer security system, no matter how elaborate, can absolutely prevent a determined person from accessing stored information that they are not authorized to access. Thus, we cannot guarantee the privacy of confidentiality of any information stored on it. Information that must remain confidential, you should not store it on the

network. This policy exists to make you aware of the inherent limitations on your ability to maintain you desired level of privacy or confidentiality of information stored on the network.

The Cinema School reserves the right to read and/or remove any files on the system without prior notification to system users.

Preventing Access by Others

Leaving your workstation unattended is dangerous to you personal files, reputation, and to system security. Log off or lock your workstation to protect your account.

Network Policy Enforcement Guidelines

Depending on the nature and severity of the policy violation, the systems administrator may take one or more of the following disciplinary actions:

a. Verbal, written, or electronic mail warning.

b. Disciplinary probation.

c. Temporary access denial (lockout).

d. Permanent access revocation.

e. Alternative punishment not involving access or usage restrictions.

If warranted, the systems administrator will refer the case to an appropriate school, Local, State, or Federal authority for further disposition.

Evidence of attempted or actual system security, integrity, or performance related incidents will be cause of 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. The user or users involved will be required to meet with the school administration. Demonstrated intent to violate policy will be considered the same as an actual policy violation. Demonstrated intent means evidence of actions, which, if successful or if carried out as intended, would result in a policy violation.

Disclaimer: The Cinema School will make every effort to maintain the network so that each user has equal and fair access. It is our primary concern to make this network a friendly, and cohesive virtual user community; we take no responsibility for the accuracy or security of information contained in any user or public file or directory. We will make every effort to maintain the security and integrity of our system. We cannot guarantee the security and ultimate privacy of any material stored on the network. We take no responsibility for the loss of data, files, or information on the network.