

Infinity Charter School

SECTION: STUDENT POLICIES

**TITLE: TECHNOLOGY USE,
CONDUCT & DISCIPLINE**

**APPROVED: December 12, 2004
January 16, 2005**

REVISED: April 16, 2012

314: TECHNOLOGY USE, CONDUCT & DISCIPLINE

PURPOSE:

These policies shall apply to all users of computers and telecommunications systems which are entered via equipment and access lines located at Infinity Charter School. The purpose of this policy is to insure compliance with policies and guidelines at the local, state, national, and international levels. The use of equipment and related software is a privilege, not a right, and should be treated as such.

Any user who does not comply with policies and procedures may face appropriate disciplinary actions, including all student discipline management techniques, and denial of continued computer access.

Outside software may not be used without written authorization from the Chief Executive Officer or designee.

Users are responsible for the security of their network accounts. Passwords should not be shared or used carelessly.

System setup and maintenance may only be performed by authorized personnel. Computer equipment must be left in good condition for the next user.

If there is a problem with a piece of equipment, it should be reported by a teacher or staff member, in writing, to the Chief Executive Officer or designee.

PARENTAL RIGHTS TO LIMIT ACCESS TO THE INTERNET:

As required by CIPA, the school utilizes a technology protection measure ("filter") that blocks access to material that is potentially harmful to minors. It is very effective, but is not a foolproof solution. Parents wishing not to allow their child access to the Internet must notify the school Chief Executive Officer in writing.

ACCEPTABLE USE REGULATIONS:

Users are expected to abide by the generally-accepted rules of online etiquette.

These include, but are not limited to, the following:

1. Be polite.
2. Do not reveal any personal information.
3. Illegal activities should not occur over a network.
4. Use the computer network in a way that will not disrupt the use of the network by other users.

5. All communications and information accessible via the computer network should be assumed to be private property.

Only students who have been authorized by the school and who are under direct supervision of designated employees are permitted to use a school computer or to access any local network or outside telecommunications services. Prior to such authorization, the student and the student's parent must sign and return the School Acceptable Use Form acknowledging their responsibilities and the consequences of violation.

Electronic communications access is available to students and personnel at Infinity. This system includes all computer hardware, software, networks, and related peripherals that a user may encounter within the school.

Infinity believes the valuable information and interaction available on the Internet far outweighs the possibility that users may procure material that is inconsistent with the educational goals of Infinity.

The Chief Executive Officer or designee will oversee the school's Electronic Communications System.

The school's system will be used only for administrative and educational purposes consistent with the school's goals and mission. Commercial use of the school's system is strictly prohibited.

The school will provide training to all users in proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the school's system will emphasize the ethical use of this resource. Infinity Charter School also provides instruction to minors on the topics of Internet Safety and appropriate online behavior. Internet Safety education topics include, but are not limited to: online behavior and ethics, social networking safety, chat room safety, cyberbullying awareness and response to other online privacy and security issues.

Copyrighted software or data may not be placed on any system connected to the school's system without written permission from the holder of the copyright. Only the owner(s) or individual(s) the owner specifically authorizes may upload copyrighted material to the system.

SYSTEM ACCESS:

Access to the school's Electronic Communications System will be governed as follows:

1. With the approval of the Chief Executive Officer or designee, school employees, and/or students will be granted access to the school's system; and
1. Any system user identified as a security risk or as having violated the school computer use guidelines may be denied access to the school's system.

INSTRUCTIONAL TECHNOLOGY COORDINATOR RESPONSIBILITIES:

As the school's coordinator for the Electronic Communications System, the Chief Executive Officer and/or designee will:

1. Be responsible for disseminating and enforcing applicable school policies and guidelines for the school;
2. Ensure that all users of the school's system complete and sign an agreement to abide by school policies and administrative regulations regarding such use. All such

agreements will be maintained on file in the Chief Executive Officer's or designee's office;

3. Ensure that employees supervising students who use the school's system provide training emphasizing the appropriate use of this resource;
4. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed necessary to ensure appropriate use of the system;
5. Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate;
6. Set limits for disk utilization on the system as deemed necessary; and
7. Revoke use of the system by individuals as deemed necessary.

INDIVIDUAL USER RESPONSIBILITIES:

The following standards will apply to all users of the school's Electronic Communications System:

Online Conduct:

1. The system may not be used for illegal purposes, in support of illegal Activities, or for any other activity prohibited by school policy; and
2. System users may redistribute copyrighted programs or data only with the written permission of the copyrighted holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, school policy, and administrative regulations.

Vandalism Prohibited:

Any malicious attempt to harm or destroy school equipment or materials, data of another user of the school's system, or any of the agencies or networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of school policy and administrative regulations and possibly as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses. Any interference with the work of others, with or without malicious intent, will be construed as vandalism. Vandalism, as defined above, may result in the permanent cancellation of Electronic Communications System use privileges and will require restitution for costs associated with system restoration and/or network, hardware, or software repair or replacement.

Forgery Prohibited:

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.

Information Content/Third Party Supplied Information:

System users and parents of students with access to the school's system will be aware that use of the system may provide access to other Electronic Communications Systems in the global network that may contain inaccurate and/or objectionable material. The school will provide written notification to parents of potential objectionable material access.

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension and/or revocation of privileges on the school's system and will

be subject to other disciplinary action in accordance with the Code of Conduct.

An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with school policies.

Network Etiquette

System users are expected to observe the following network etiquette:

1. All use must be in support of education and research and no use shall serve to disrupt the use of the network;
2. Be polite. Use appropriate language.
3. Pretending to be someone else when sending/receiving electronic messages is considered inappropriate;
4. Transmitting obscene messages or pictures is prohibited;
5. Revealing personal information of the users or others is prohibited; and
6. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

CONSEQUENCES OF MISUSE OF ELECTRONIC COMMUNICATIONS SYSTEM OR RESOURCES:

Any attempt to violate the provisions of these guidelines may result in revocation of a user's account, regardless of the success or failure of the attempt. Any user who does not comply with school policies and procedures may face additional disciplinary actions and/or appropriate legal action.

TERMINATION /REVOCATION OF SYSTEM USER ACCOUNT:

The school may suspend or revoke a system user's access to the school's system upon suspected violation of school policy and/or administrative regulations regarding acceptable use.

Termination of an employee's account or of a student's access will be effective on the date the Chief Executive Officer, or designee receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

DISCLAIMER:

The school's system is provided on an "as is, as available" basis. The school does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein.

The school does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not the school.

The school will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the school's Electronic Communications System.