

USER AGREEMENT

Use of school and district networks must be in support of education, research, and the educational goals and objectives of the Sierra Vista High School and the Clark County School District. Students are personally responsible for this provision at all times when using building and district networks.

- Students will need to be in compliance with the guidelines outlined in the *Acceptable Use Policy* provided by the Technology Development Services of the Clark County School District. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade secret.
- The use of another organization's networks or computing resources must comply with rules appropriate to that network (i.e. e-mail services, internet download facilities, etc.)
- Students will be working on **assigned tasks** at all times. Any unauthorized "web-surfing" will result in disciplinary action according to the Sierra Vista High School Discipline Policy.

SUMMARY OF RULES:

- NO email, chat, blogs, or instant messaging, or bypassing CCSD filters.
- NO game sites or game cheat sites; school-related sites only.
- NO installation of software or change of computer desktops or configurations.
- NO sharing of student accounts, copying other students' files, plagiarism.
- DO NOT save files that are not school related, i.e., MP3, movies, personal photos, etc.

Students should be familiar with these rules and how to use the Internet before getting on-line. If they have any questions about these rules, they should ask their teacher. Be aware that the inappropriate use of electronic information resources can be a violation of school rules, local, state, and federal laws and that students can be prosecuted for violating those laws.

If any unauthorized files are found on the computer by any student, he/she must inform the instructor immediately or it will be assumed by the school's staff that he/she put it there. Under no circumstances are students to use unauthorized files, add icons, or alter the standard icons on their computer.

NETWORK ETIQUETTE AND PRIVACY

Students are expected to abide by the generally accepted rules of network etiquette. These rules include but are not limited to:

- **BE POLITE:** Never send, or encourage others to send, abusive messages.
- **USE APPROPRIATE LANGUAGE:** You are a representative of your school and your school district on a public system. Never swear, use vulgarities, or any other inappropriate language.
- **PRIVACY:** Do not reveal your home address, phone number, names or addresses of family members, or the addresses or phone numbers of other students or colleagues.
- **DISRUPTIONS:** Do not use the network in any way that would disrupt the use of the network by others.
- **REPRESENTATION:** Do not send anonymous messages or represent a message as to have been written by another. The originator of all correspondence must be clearly identifiable.

SECURITY & VANDALISM

If students identify a security problem in the building or school district networks, they must notify their teacher or the system administrator immediately. Students should never demonstrate the problem to another user, use another individual's account, or tell anyone else their password. Any user identified as a security risk will be denied access to the network and may be liable for disciplinary action or prosecution.

Vandalism is defined as any malicious attempt to physically deface, disable, or destroy computers, peripherals, or other network hardware or to harm or destroy data of another user or any other agencies or networks that are connected to the system. This includes, but is not limited to, the creation or transmission of computer viruses. Any vandalism will result in loss of network privileges, disciplinary action, or possible legal referral.