ROUND TOP – CARMINE ISD

STUDENT INTERNET USE POLICY

The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. Students and teachers have access to electronic mail communication with people all over the world, information and news, discussion groups, university library catalogs, etc.

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. On a global network, it is impossible to control all materials (even though a filter may be in place) and the user may discover controversial (and sometimes offensive) information. Round Top-Carmine ISD firmly believes that the valuable information and interaction available on this worldwide network far outweigh the possibility that users may procure material that is not consistent with the educational goals of the District.

The smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided here so that you are aware of the responsibilities you are about to acquire. In general this requires efficient, ethical and legal utilization of the network resources. All students, faculty, and staff are responsible for seeing that the system is used in an effective, efficient, ethical, and lawful manner.

INTERNET TERMS AND CONDITIONS

1. The purpose of the Internet is to support research and education in and among academic institutions in the U.S. by providing access to unique resources and the opportunity for collaborative work. The use of the Internet must be in support of education and research and consistent with the educational objectives of Round Top-Carmine ISD.

2. The use of the Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrators will maintain an Internet user's log and if inappropriate sites for educational use are accessed, the building principal may require the system administrator to deny, revoke, or suspend, specific user privileges.

3. Users may be monitored through electronic means, computer user sign-up logs, or through teacher/staff observation. If violations are discovered, the matter will be immediately referred to the building principal.

4. Users are expected to abide by the generally accepted rules of network etiquette. These are (but are not limited to) the following:

    a) Be polite. Do not get abusive in your messages to others.

    b) Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Illegal activities are strictly forbidden.

c) Do not reveal personal addresses or phone numbers of students or colleagues.

d) Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to proper authorities.

e) Do not use the network in such a way that would disrupt the use of the network by other users.

f) All communications and information accessible via the network should be assumed to be private property.

5. Vandalism may result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, agency, or network connected to the Internet. This includes, but is not limited to, the uploading or creation of computer viruses. Loopholes in information security, or knowledge of a special password are not to be used to damage information systems, take resources from another user, gain access to systems, or use systems for which the proper authorization has not been given.

6. Users will not play games on the computers, will not waste supplies such as paper, printer cartridges, and will not take CD-ROMS from the room. Users may store their personal data files in the special storage area designated on the server (the folder with their user name). Students should not save data to the hard drives on the computers. Understand that network managers may need to view the contents of personal files to diagnose or correct problems and that teachers may need to access student files in the course of educational instruction.

7. Users are not to customize any of the computers in the district. This includes but is not limited to changing the mouse pointer, downloading any fields such as instant message services or music files, adding wall paper, changing any system settings, etc.

8. As per local policy, students will only access personal email at times as designated by the administration. All internet access will only be with permission and supervision.