

NETWORK AND INTERNET

ACCEPTABLE USE POLICY

1. Authorization to Use Computer Network

A. General Provisions

To use District 113 computers, which includes: the district's local and/or wide area network and access to the Internet through District computers or the District's local and/or wide area network, students must obey the provisions of this Policy that governs their use. The provisions of the policy regarding use and unacceptable use will also apply to student's use of computers outside of the District 113 network, where those computers are used to access or communicate with the District 113 network, or to store, display or otherwise make materials available in such a way that they may be accessed from the District 113 network.

B. Student Authorization

To be authorized to use District 113 computers, students must:

- submit properly signed copies of the Computer Network Access forms when signing for the handbook;
- obtain computer validation on their Student ID Cards prior to using school computers (valid for school year);
- if asked, display their validated Student ID Cards when using any part of the District's Computer Network.

Upon entering District 113, all students will be required to submit a properly signed copy of the Student Authorization for Computer Network Access form. Once the completed form is submitted, students are held responsible to the terms of the policy throughout their entire high school career.

2. Use of Computer Network

A. Acceptable Use

The District computer network is to be used for educational or research purposes consistent with the District's educational mission. The Superintendent, Building Principals, or their designees will determine regulations for appropriate access rules and policies and will disseminate such regulations to those subject Policy.

B. Unacceptable Use

1. Unacceptable use is generally defined as any action that is inconsistent with the District's educational mission.

3. Violation of Terms

Violation of the terms of the Student Authorization Forms or of the Student Computer Use Policy may result in the suspension or revocation of computer network privileges, disciplinary action, and/or legal action. Disciplinary measures, if any, will be imposed consistent with District discipline policies. Disciplinary action can result in 20/40/60 day restriction from open computer labs, revocation on internet privileges, all computerized privileges, Saturday detentions, in-school suspensions and/or expulsion. If a student's computer network privileges are suspended or revoked, newly signed copies of the student and parental authorizations must be submitted before the student's access privileges can be restored.

4. Privacy

Users do not have a right of privacy with respect to any electronic communications or files created on, stored on, or sent to, from or via the computer network, subject to applicable law governing the privacy of certain student records and information. The Superintendent, Building Principal, and/or their designees may access, retrieve, review and copy any such electronic communications or files and use them as they deem appropriate in connection with the protection of the network or the implementation or enforcement of school policies or suspected violations of the law.

5. Security

The security and integrity of the District's computer network is a high priority. Users are to keep their account and password secure and confidential at all times. Users will neither exploit nor enable others to exploit any security gap, weakness, or breach on the District's computer network or on the Internet using the District computer network and will immediately report to a supervisory teacher or administrator any such gap, weakness or breach.

6. No Warranties

- a. The District will not be responsible for any damages users suffer, including loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by users' errors, omissions, or negligence. The District specifically denies any responsibility for the accuracy or quality of information obtained through the computer network.
- b. The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs, relating to, or arising out of, an individual user's use of the computer network.
- c. The District has acted in good faith and in a reasonable manner in selecting and implementing filtering software, blocking software, and other technology protection measures to prevent access to material, which is obscene or pornographic. The District assumes no responsibility for access gained or denied by the technology protection measures that have been implemented.

7. Cooperation with Investigations

The Principal or Principal's designee will notify legal authorities of all evidence and reports of all illegal activity if warranted.