

- Revealing personal information (addresses, phone numbers, etc.) regarding oneself or another to an unknown party.
- Using the Internet without authorization.
- Attempting to impersonate or to gain unauthorized access as a system administrator or as any other user.
- Attempting to harm or destroy data of the district network, another user on the network, or any other agency connected to the Internet.
- Encouraging or supporting the prohibited activities of others.
- Spamming (sending massive, inappropriate and unsolicited information) or flooding (transferring data without intent of meaningful communication).

### **District Response to Infractions**

Deliberate attempts to degrade or disrupt system performance may be viewed as violations of district policy and/or criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism will result in the cancellation of system privileges and will require restitution for costs associated with hardware, software, and system restoration.

The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district's network.

A user who violates district policy or administrative procedures or uses the district network inappropriately will be subject to suspension or termination of district privileges and will be subject to appropriate district/school disciplinary action and/or prosecution.