

# F. Policies and Procedures

District policies and procedures protect not only the user, but also the integrity of the network and data. While some policies remain static, others need to be revisited to determine their utility in the face of changing technologies and changing information literacy needs.

- Increased Access for All Students and Teachers.
- Data and Network Security.
- Internet Safety and Children's Internet Protection Act Compliance (CIPA).
- Student and Staff Acceptable Use Policies.
- District Policies Regarding Student Use of Personal Technologies

CIPA requires a school to have an Internet Safety Policy that protects minors from pornography or activities that could harm them. CIPA compliance is required for E-Rate and Title II Part D of No Child Left Behind programs. Under CIPA, the Internet Safety Policy must also contain a "technology protection measure" that prohibits access to graphic images considered pornography or harmful to minors.

## Guiding Questions:

1. Describe the policies/procedures in place for the areas required/recommended. What are some of their key components?
2. Describe the district's filtering and security measures.
3. Describe the district's procedure for renewal of acceptable use policies.
4. How are school staff, parents and students kept updated on these policies?
5. Have you conducted a security audit of your network? What type of security is used to secure your network and safeguard the privacy of data?
6. Describe your district's compliance with the Safe Schools Act and how it includes technology related infractions.
7. Explain the district's policy on ensuring equitable access to all students and teachers.

## FEDERAL REQUIREMENTS

*E-Rate and NCLB Requirements: School district's who wish to be eligible for funding from E-Rate and NCLB Title II D must be in compliance with the Children's Internet Protection Act.*

## STATE REQUIREMENTS

*4.03 (1) (c) Evidence of compliance with the safe schools requirements pursuant to § 22-32-109.1, C.R.S. and evidence of compliance with the Gun Free Schools Act of 1994, 20 U.S.C. 70 and Pub. L. 107-110, Sec. 4141.*

*2.01 (4) (m) Assurance that the District or the Institute has adequate policies and that these policies are being implemented and in compliance with state statutes, rules and regulations;*

*2.01 (4) (r) Assurance of a plan for technology and information literacy that is integrated into the district's standards-based educational plan and includes the assessment of all students in the eighth grade. The technology plan shall include policies and procedures to prevent students from accessing inappropriate material on the Internet;*

1, 2, 3, 4, 6) The district has board approved policies regarding Internet access. We have acceptable use policies for both staff and students which are signed annually. The acceptable use policies are evaluated every other year to make sure they are in compliance with CIPA and No Child Left Behind. We filter through a Smart filter all content that might be considered inappropriate for a K-12 environment, with an override that can be utilized for an educational purpose. Security concerns, such as the sharing of passwords, are covered in the acceptable use policy. Students and staff must sign this agreement annually. Failure to do so results in no computer privileges on school grounds. The policies are posted on the district website. These policies and procedures are in compliance with the Safe Schools Act. All of these policies are posted on the district website under Board Policies at [http://www.brushschools.org/jm/index.php?option=com\\_remository&Itemid=68&func=stardown&id=951](http://www.brushschools.org/jm/index.php?option=com_remository&Itemid=68&func=stardown&id=951).

5) A security audit is done occasionally by an outside firm. However, we would like to be able to do this more consistently. We have a mail foundry in place, a pix firewall, a N2H2 Bess filtering appliance in place and ISA firewall to assure data security. Technology related infractions result in the cancellation of privileges or use of the computer via a due process procedure.

There is currently a procedure in place regarding student use of cell phones in all buildings. Inappropriate use of cell phones results in the loss of cell phone privileges. Other personal technologies have not been addressed at this time.

6) All students and teachers have access to computers in the district. Procedures are in place to insure student privacy on all computers. Violations of policy and procedures result in a withdrawal of access from district computers.