

MESA UNIFIED SCHOOL DISTRICT	TOPIC: Student Computer and Internet Use
GOVERNING BOARD POLICY	DISTRICT CODE: JFCH

## **STUDENT COMPUTER AND INTERNET USE**

Mesa Public Schools provides computers and Internet access to support the educational mission of its schools and to enhance the curriculum and learning opportunities for students and staff. The resources available through the Internet are of significant value in the learning process and in preparing students for future success. At the same time, the unregulated availability of information and communication on the Internet requires that schools establish reasonable controls for lawful, efficient and appropriate use of this technology.

Student use of school computers, networks and Internet services is a privilege, not a right. Students are required to comply with this policy and the rules outlined in administrative regulation JFCH-R. Students who violate the policy and/or rules may have their computer privileges revoked and may also be subject to further disciplinary and/or legal action.

All Mesa Public Schools computers remain under the control, custody and supervision of the school. The school reserves the right to monitor all computer and Internet activity by students. Students have no reasonable expectation of privacy in their use of school computers.

Students and parents will be informed of this policy on an annual basis through handbooks and/or other means selected by the Superintendent.

The Superintendent may adopt administrative procedures, as necessary, to implement this policy.

Adopted: March 23, 2004

Cross Reference: [GBSA – Employee Computer and Internet Use](#)  
[EGAA – Copyright](#)

MESA UNIFIED SCHOOL DISTRICT	TOPIC: Student Computer and Internet Use
GOVERNING BOARD POLICY	DISTRICT CODE: JFCH-R

## STUDENT COMPUTER AND INTERNET USE RULES

These rules implement Governing Board Policy JFCH, Student Computer and Internet Use. The rules are intended to provide general guidelines and examples of prohibited uses but do not attempt to state all required or prohibited activities by users. Failure to comply with Governing Board Policy JFCH and these rules may result in loss of computer and Internet access privileges, disciplinary action and/or legal action.

### A. Computer Use is a Privilege, Not a Right

Student use of a school's computers, networks and Internet services is a privilege, not a right. Unacceptable use/activity may result in suspension or cancellation of privileges as well as additional disciplinary and/or legal action. The principal will have final authority to decide whether a student's privileges will be denied, revoked and/or reinstated.

### B. Acceptable Use

Student access to the school's computers, networks and Internet services are provided for educational purposes and research consistent with the school's educational mission, curriculum and instructional goals. The same rules and expectations that govern student conduct and communications will apply to student use of computers and the Internet. Students are further expected to comply with these rules and all specific instructions from the teacher or other supervising staff member/volunteer when accessing the school's computers, networks and Internet services.

### C. Prohibited Use

The user is responsible for his/her own actions involving school computers, networks and Internet services and for his/her computer files, passwords and accounts. Examples of unacceptable uses that are expressly prohibited include, but are not limited to, the following:

1. Accessing Inappropriate Materials: Accessing, submitting, transmitting, posting, publishing, forwarding, downloading, scanning or displaying materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal.
2. Illegal Activities: Using the school's computers, networks and Internet services for any illegal activity or activity that violates other Board policies, procedures and/or school rules.
3. Violating Copyrights: Copying or downloading copyrighted materials without the express authorization of the student's teacher or principal.
4. Plagiarism: Representing as one's own work any materials obtained on the Internet (such as term papers, articles, etc.). When Internet sources are used in student work, the author, publisher and Web site must be identified.
5. Copying Software: Copying or downloading software without the express authorization of the student's teacher or principal.
6. Nonschool-Related Uses: Using the school's computers, networks and Internet services for non-school-related purposes such as private financial gain, commercial, advertising or solicitation purposes.
7. Misuse of Passwords/Unauthorized Access: Sharing passwords, using other users' passwords without permission and/or accessing other users' accounts.

8. Malicious Use/Vandalism: Any malicious use, disruption or harm to the school's computers, networks and Internet services, including, but not limited to, hacking activities and creating/uploading computer viruses.
9. Unauthorized Access to Chat Rooms/News Groups: Accessing chat rooms or news groups without specific authorization from the supervising teacher.
10. Misuse of School Name or Logo. Misuse of a school name or logo on a personal Web site that gives the reader the impression that the Web site is an official Web site of the school or district.

#### **D. No Expectation of Privacy**

The school retains control, custody and supervision of all computers, networks and Internet services owned or leased by the school. The school reserves the right to monitor all computer and Internet activity by students. Students have no expectations of privacy in their use of school computers, including e-mail and stored files.

#### **E. Compensation for Losses, Costs and/or Damages**

The student and/or the student's parent/guardian will be responsible for compensating the school for any losses, costs or damages incurred by the school related to violations of policy JFCH and/or these rules, including investigation of violations.

#### **F. School Assumes No Responsibility for Unauthorized Charges, Costs or Illegal Use**

The school assumes no responsibility for any unauthorized charges made by students including, but not limited to, credit card charges, long-distance telephone charges, equipment and line costs, or for any illegal use of its computers, such as copyright violations.

#### **G. Student Security**

A student will not reveal his/her full name, address or telephone number on the Internet without prior permission from a supervising teacher. Students should never meet people they have contacted through the Internet without parental permission. Students should inform their supervising teachers if they access information or messages that are dangerous, inappropriate or make them uncomfortable in any way.

#### **H. System Security**

The security of the school's computers, networks and Internet services is a high priority. Any user who identifies a security problem must notify a supervising teacher. The user will not demonstrate the problem to others. Any user who attempts or causes a breach of system security will have his/her privileges revoked and may be subject to additional disciplinary and/or legal action.

#### **I. Parent Opt-Out**

While reasonable precautions will be taken to supervise student use of the Internet, Mesa Public Schools cannot prevent all inappropriate uses, including access to objectionable materials and communication with persons outside of the school. The school also is not responsible for the accuracy or quality of information that students obtain through the Internet. The parent/guardian may opt to not allow his or her child to use computers or the Internet while at school. Parents will be informed of this right annually.

Adopted:        March 23, 2004

---

Debra Duvall  
Superintendent

MESA UNIFIED SCHOOL DISTRICT	TOPIC: Employee Computer and Internet Use
GOVERNING BOARD POLICY	DISTRICT CODE: GBSA

## **EMPLOYEE COMPUTER AND INTERNET USE**

Mesa Public Schools provides computers, networks and Internet access to support the educational mission of the schools and to enhance the curriculum and learning opportunities for students and school staff. Employees are to use district computers, networks and Internet services for school-related purposes and the performance of job duties. Incidental personal use of school computers is permitted as long as the use does not result in any additional cost to the district and does not interfere with the employee's job duties and performance, with system operations, or with other system users. "Incidental personal use" is defined as incidental, occasional and reasonable use by an individual employee for personal communications. Employees are reminded that such personal use must comply with this policy and all other applicable policies, procedures and rules. Any employee who violates this policy and/or rules governing use of district computers will be subject to disciplinary action, up to and including discharge. Illegal uses of district computers will also result in referral to law enforcement authorities.

All district computers remain under the control, custody and supervision of the school or department, which reserves the right to monitor all computer and Internet activity by employees. Employees have no expectation of privacy in their use of district computers.

The Superintendent may adopt administrative procedures, as necessary, to implement this policy.

Adopted: March 23, 2004

CROSS REF.: JFCH – Student Computer and Internet Use  
EGAA – Copyright

MESA UNIFIED SCHOOL DISTRICT	TOPIC: Employee Computer and Internet Use
GOVERNING BOARD POLICY	DISTRICT CODE: GBSA-R

## **EMPLOYEE COMPUTER AND INTERNET USE RULES**

The intent of these rules is to provide employees with general requirements for using district computers, networks and Internet services. These rules may be supplemented by more specific administrative procedures and rules governing day-to-day management and operation of the computer system. These rules provide general guidelines and examples of prohibited uses for illustrative purposes but do not attempt to state all required or prohibited activities by users. Employees who have questions regarding whether a particular activity or use is acceptable should seek further guidance from the appropriate administrator or from the system administrator. Failure to comply with Governing Board Policy GBSA, these rules, and/or other established procedures or rules governing computer use, may result in disciplinary action, up to and including discharge. Illegal uses of district computers will also result in referral to law enforcement authorities.

### **A. Access to School Computers, Networks and Internet Services**

The level of access that employees have to district computers, networks and Internet services is based upon specific employee job requirements and needs.

The Superintendent may authorize a certificated or exempt classified employee to have remote access to the district's computer systems while working at home.

### **B. Acceptable Use**

Employee access to district computers, networks and Internet services is provided for administrative, educational, communication and research purposes consistent with the district's educational mission, curriculum and instructional goals. General rules and expectations for professional behavior and communication apply to use of district computers, networks and Internet services. Employees are to use district computers, networks and Internet services for school-related purposes and performance of job duties. Incidental personal use of district computers is permitted as long as the use does not result in any additional cost to the district and does not interfere with the employee's job duties and performance, with system operations, or with other system users. "Incidental personal use" is defined as incidental, occasional and reasonable use by an individual employee for personal communications. Employees are reminded that such personal use must comply with this policy and all other applicable policies, procedures and rules.

### **C. Prohibited Use**

The employee is responsible for his/her actions and activities involving district computers, networks and Internet services and for his/her computer files, passwords and accounts. General examples of unacceptable uses which are expressly prohibited include, but are not limited to:

1. Any use that is illegal or in violation of other policies, including (a) Policy GBCX – Sexual Harassment - Employees, (b) Policy EGAA – Copyright, and (c) Policy GBG – Use of District Employees and Resources to Influence the Outcome of Elections.
2. Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive.

3. Any inappropriate communications with students or minors.
4. Any use for private financial gain or for commercial, advertising or solicitation purposes.
5. Any use as a forum for communicating by e-mail or any other medium with other district users or outside parties to solicit, proselytize, advocate or communicate the views of an individual or non-district-sponsored organization; or to raise funds for any non-district-sponsored purpose, whether for profit or not for profit. No employee will knowingly provide district e-mail addresses to outside parties whose intent is to communicate with district employees, students and/or families for non-school purposes. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the principal, other appropriate administrator or supervisor, or the system administrator.
6. Any communication that represents personal views as those of the district or that could be misinterpreted as such.
7. Downloading or loading software or applications that have not been approved for installation on a district computer or network. Employees who are uncertain as to whether a particular software or application may be downloaded should seek further guidance from the building principal or other appropriate administrator or supervisor or the system administrator.
8. Sending mass e-mails to district users or outside parties for district or non-district purposes without the permission of the building principal or other appropriate administrator or supervisor.
9. Any malicious use or disruption of district computers, networks and Internet services or breach of security features.
10. Any misuse resulting in damage to district computer equipment.
11. Misuse of computer passwords or accounts (employee or other users).
12. Any communications that are in violation of generally accepted rules of network etiquette and/or professional conduct.
13. Any attempt to access unauthorized sites or to circumvent the district's internet filter system.
14. Failing to report a known breach of computer security to the building principal, other appropriate administrator or supervisor, or the system administrator.
15. Using district computers, networks and Internet services after such access has been denied or revoked.
16. Any attempt to delete, erase or otherwise conceal any information stored on a district computer that violates these rules.
17. Accessing non-work related chat rooms or news groups.
18. Misuse of a school name or logo on a personal Web site that gives the reader the impression that the Web site is an official Web site of the school or district.

#### **D. No Expectation of Privacy**

The district retains control, custody and supervision of all computers, networks and Internet services owned or leased by the district. The district reserves the right to monitor all computer and Internet activity by employees and other system users. Employees have no reasonable expectation of privacy in their use of district computers, including e-mail messages and stored files.

**E. Confidentiality of Information**

Employees are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential.

**F. Staff Responsibilities to Students**

Teachers, staff members and volunteers who use district computers for instructional purposes with students are expected to provide reasonable supervision commensurate with the student's age, maturity and experience with computers. Teachers, staff members and volunteers are expected to be familiar with the district's policies and rules concerning student computer and Internet use and to enforce them. When, in the course of their duties, employees/volunteers become aware of student violations, they are expected to stop the activity and inform the building principal or other appropriate administrator or supervisor.

**G. Compensation for Losses, Costs and/or Damages**

The employee will be responsible for any losses, costs or damages incurred by the district related to violations of policy GBSA and/or these rules.

**H. District Assumes No Responsibility for Unauthorized Charges, Costs or Illegal Use**

The district assumes no responsibility for any unauthorized charges made by employees including, but not limited to, credit card charges, subscriptions, long-distance telephone charges, equipment and line costs, or for any illegal use of its computers, such as copyright violations.

Adopted:        March 23, 2004

---

Debra Duvall  
Superintendent

MESA UNIFIED SCHOOL DISTRICT	TOPIC: School-Sponsored Information & Web Sites
GOVERNING BOARD POLICY	DISTRICT CODE: KBB

### **SCHOOL-SPONSORED INFORMATION MEDIA & WEB SITES**

Publications issued by and in the name of the schools of this district will reflect a high quality of editorial content and format. The district will exercise appropriate economy in materials and production.

The Superintendent may request employees who are preparing articles for publication, that directly or indirectly mention the district, to submit a copy for review prior to publication. If implemented, this procedure will be used solely to ensure that the most current and valid information about the district is considered.

Schools and school staff may create school and class Web sites, subject to guidelines adopted by the Superintendent.

Adopted: March 23, 2004

MESA UNIFIED SCHOOL DISTRICT	TOPIC: School-Sponsored Information & Web Sites
GOVERNING BOARD POLICY	DISTRICT CODE: KBB-R

## HOME PAGE GUIDELINES FOR THE INTERNET

1. Each school's home page should include the following:
  - a. A statement identifying the school as a member of Mesa Public Schools.
  - b. The official MPS logo.
  - c. The last date on which the Web site was modified.
  - d. The school's phone number and fax number.
  - e. Content that is accurate and grammatically correct.
  - f. Content that observes copyright laws.
  - g. Content that observes the privacy of individuals who work at and attend school at the site.
  - h. Content that is appropriate for public access.
  - i. The school's home page contact's name and a link to that individual's e-mail address.
  - j. A link to the MPS home page.
  
2. Web pages should protect students and staff by:
  - a. Not including student photographs and other personal information without written parental permission. Use of students' last names is discouraged.
  - b. Not including staff photographs and other personal information without written permission. Use of staff last names is discouraged.
  - c. Not including personal phone numbers or addresses for students or staff.
  - d. Not including maps of the school facilities.
  
3. A Web site must have:
  - a. Approval by the site administrator for all content.
  - b. A facilitator who is responsible for updating the page regularly.
  - c. An available contact person who will respond to inquiries.
  - d. A technical liaison who can modify links or correct any technical problems that occur so that no dead-end links exist.
  
4. District departments will create and maintain their department Web sites in compliance with these guidelines.

Adopted: March 23, 2004

---

Debra Duvall  
Superintendent