

## SECTION 9000

### ADMINISTRATIVE DIRECTIVES

REVISED 2002

KAY DAVIS

#### Mission

To establish guidelines, policies, and goals for the use of the district Internet and electronic mail; and to provide students and staff educational and instructional enhancement through access to the global electronic community.

#### Enforcement of Policy

1. The use of the computer/information systems is a privilege, not a right. Unethical and unacceptable usage by any user will be just cause for taking disciplinary action. Such action can include suspending or revoking access to the computer/information systems and/or initiating legal action for any activity described in this policy where legal proceedings are deemed appropriate by the administration.
2. The district reserves the right to restrict, terminate, and/or deny access to any user who has been identified a security risk, has a history of problems with the computer/information systems, or demonstrates an interest not to comply with the district acceptable use policy. The district further reserves the right to monitor network activity in any form that it sees fit to maintain the integrity of the network system.
3. Access to technology including systems and networks owned or operated by Hickman Mills C-1 imposes certain responsibilities and obligations; and, therefore, use is granted subject to Board of Education policies, local, state, and federal laws.
4. Acceptable use should always reflect academic honesty, high ethical and moral responsibility and restraint in the consumption of shared resources. Acceptable use demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individual's rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance.

5. Demonstrated intent to violate this policy will be considered the same as an actual policy violation. Demonstrated intent means evidence of actions that, if successful, or if carried out as intended, would result in a policy violation.

#### Disclaimer

Worldwide access can provide access to material that is not considered to be of educational value in the school setting. Material that is not considered acceptable for school-aged children must not be accessed. It is impossible to control all materials on the global network. The district cannot prevent the possibility that a student will access material that is inconsistent with the educational mission, goals, and policies of the district. Use of the network is logged and is subject to administrative monitoring/review at any time. The district makes no warranties for the service it is providing. The district is not responsible for any damages a user may suffer including loss of data, nor can it warranty the accuracy or quality of information obtained through the use of the computer/information systems.

#### Acceptable Use

Access will be in support of research or usage consistent with the educational and instructional policies and goals of the district. The access includes, but is not limited to the following:

1. Intellectual activities and research.
2. Seeking or sharing resources.
3. Accessing libraries, university libraries, Library of Congress, etc.
4. Completing research projects assigned by teachers.
5. Appropriate and proper communication with others through the network.
6. Sharing research, projects, and information with others around the world.
7. Collaborative learning with other students, teachers, and districts.
8. Global information news.

9. Public domain and shrewder computer software.
10. Discussion groups.
11. "Fair Use" of any information that is legally found on informational networks. This use is for educational/instructional use ONLY.
12. Only authorized software will be installed on district computers; no person (student or staff) shall install their personal software on district computers.

#### Unacceptable Use

Access will be denied to any individual when district policies are not followed. The denial of access includes, but is not limited to the following:

1. Using or attempting to use another user's account, files, or vandalizing such data.
2. Violation of federal and state laws.
3. Violation of others' rights (use of vulgar, abusive, obscene, threatening, harmful, and/or harassing communication).
4. Accessing sites that are non-instructional.
5. Disruption of normal network use and service.
  - A. Viruses.
  - B. Violation of personal privacy.
  - C. Unauthorized access to protected and private network resources.
  - D. Maliciously accessing, altering, deleting, damaging and/or destroying any computer system, network, program, or data.
6. Forwarding personal communication without the author's prior consent.
7. Stealing data, equipment, or intellectual property.
8. Vandalism
  - A. Attempt to harm or destroy Internet or other networks including the creation of or uploading computer viruses.
  - B. Destruction of equipment through abuse or negligence.
9. Plagiarism.

10. Commercial activities such as solicitation of business.
11. Possessing any data considered a violation of this policy on paper, disk, etc.
12. Copyright violations -- if caught with illegal software, an individual or organization may be criminally prosecuted. **(This violation is punishable up to \$250,000.00 and/or up to 5 years in prison for the first offense, or both. 17 U.S.C., section 2319; 18 U.S.C., section 3571).**

#### Safe Use of the Internet

1. Teaching children safe use of the communicative tools.
  - A. Prior to use of the Internet, students will receive instruction that will explicitly explain safe use of the Internet.
  - B. Prior to use of the Internet, students will return a signed agreement between the school, the student, and parents/guardians, specifying what safe use is and providing parental approval for use of the Internet.
  - C. Students will be instructed to:
    - (1) Never give out identifying information (home address, school name, or telephone number) in a public message such as chat rooms or bulletin boards.
    - (2) Only communicate with someone approved by their parent/guardian(s) or teachers.
    - (3) Think carefully before revealing any personal information such as age, marital status, or financial information.
    - (4) Not post photographs on web sites or newsgroups that are public.
    - (5) Consider using a pseudonym.
    - (6) Never arrange a face-to-face meeting with another computer user without first obtaining a teacher's or parent/guardian(s)' permission.
    - (7) Never respond to messages that are suggestive, obscene, belligerent, threatening, or make you feel uncomfortable.
    - (8) Report any of the above messages to your teacher or administrator.
    - (9) Remember that people on the other end of the line may not be who they seem to be--they could be your worst enemy.
    - (10) Never send a person your picture over the Internet without getting a teacher's or parent/guardian(s)' approval.

2. Monitoring of students to ensure safe practices are followed.
  - A. Students will only access the Internet under direct supervision of a teacher, administrator or supervisor who will monitor the use of electronic mail, chat rooms, and other forms of direct electronic communications.
  - B. Monitoring of students combined with the current use of filtering software is expected to provide a safe environment for educating youth.
  
3. Unauthorized disclosure, use, and dissemination of personal information regarding minors.
  - A. The school will take every precaution to ensure personal information about students is not disclosed or disseminated over the Internet or any other forms of electronic communication.
    - (1) Pictures of students can only be used in digital format with the specific written permission by the parent/guardian(s).
    - (2) Names are not to be used in electronic publications that can be associated with pictures.
  - B. Dissemination of personal information about students will only be done under the specific direction of the Board of Education and will be in compliance with state and federal laws.

### Consequences of Violation

#### 1. Students

Unethical and unacceptable behavior are just cause for taking disciplinary action. Violation of the acceptable use policy will be referred to the administration for a determination of consequences. Consequences of violations include but are not limited to:

- Suspension of computer/information systems access
- Revocation of computer/information systems access
- School suspension
- School expulsion
- Legal action and referral to appropriate local, state, or federal authorities for further disposition.
- A violation of this policy may also constitute a violation of provisions of the Student Disciplinary Policy and separate punishment may be imposed under each section.

## 2. Staff

Unethical and unacceptable behavior are just cause for taking disciplinary action. Consequences of violations include but are not limited to:

- Suspension of computer/information systems access
- Revocation of computer/information systems access
- Legal action and referral to appropriate local, state, or federal authorities for further disposition.
- Costs associated with misuse of equipment

## 3. Suspension During Investigation

Any violation of this policy will be reported to the staff member's direct supervisor, who may take appropriate disciplinary action in accordance with this policy, or who may refer this matter to the superintendent for further consideration.

Evidence of attempted or actual system security integrity or performance related incidents, will be cause for immediate access denial. The purpose of access denial in these cases is to prevent further damage to the system or data while an investigation is conducted. After investigation, the case may be referred to the superintendent of schools for disciplinary action.

## Compatibility, Purchasing, and Maintenance

### General

1. The Hickman Mills C-1 school district is committed to providing affordable technology that will improve instruction, productivity, and enhance communication throughout the district.
2. The following policies are included to ensure that:
  - A. Equipment purchased will be compatible with existing systems.
  - B. The quality of the equipment purchased will meet the needs of the district.
  - C. That adequate efforts will be made to prevent theft or damage to the equipment.
  - D. That adequate and appropriate instruction will be given to those using the equipment.
  - E. That adequate maintenance will be available to ensure that the equipment is in working condition.

## Compatibility with Existing Systems

### Standards of Computer Systems

1. The district has standardized on a platform that will ensure users of the system will be compatible. This platform includes the network software, the workstations attached to the network, and the software used on the workstations.
2. Because of cost issues, board approval will be required if and when systems listed above are to be changed or replaced with other platforms.
3. Technology Department will ensure that timely and appropriate upgrades are implemented as funding for the upgrades is approved.
4. Technology Department will ensure that new equipment/software is compatible with existing systems.
5. Operating systems standards for computer equipment software will be prepared by the Technology Department on a yearly basis. Once the standard has been established, it will be presented to the District Technology Committee for review and recommendations. The standard will then be presented for approval to the Board of Education prior to the vendor selection process (described below).
6. Technology Department will report at the Board's convenience on these standards.

### Quality of Equipment Purchased

1. The Technology Department will ensure that District funds are spent for equipment that is compliant with the District standard and will withstand the rigors of the educational environment.
2. The Technology Department, in conjunction with the Finance Department, will select, through a bid process, a single vendor for computer software and hardware.

3. Vendor selection will be made according to the following:
  - A. The quality of the equipment that will meet the standards and needs of the district as determined by the Technology Department in conjunction with the District Technology Committee and approved by the Board of Education.
  - B. Service in past years.
  - C. Availability of ongoing technical support.
  - D. Recommendations from other districts using their services.
4. Vendor selection will be made during the months of April and May.
5. The service contract for the selected vendor will be from July 1 to June 30.
6. The vendor will need to:
  - A. Guarantee all pricing at or below the bid price for the duration of the 12-month contract.
  - B. Guarantee that price reductions will be passed on to the district.
  - C. Fulfill all orders in a timely manner.
  - D. Provide adequate support.
  - E. Guarantee that replacement parts will be available for a minimum of five years. Exceptions to this must be endorsed by the Technology Department prior to purchase of items affected by the exception and will be done on an item-by-item basis.

#### Processing Orders

1. To ensure compatibility, timely installation, training, and support, all computer systems/software will be processed through the Technology Department.
2. Process:
  - A. Items to be purchased will be submitted to the Technology Department for compatibility approval and to resolve connectivity issues.
  - B. Departments or organizations must submit an authorized account code against which the equipment will be billed.
  - C. Parent organizations or other groups with outside funding are required to be in compliance with district standards and policies before purchasing equipment for the district.
  - D. All equipment purchased for the district must be inventoried by the district before being installed in district buildings.

- E. Maintenance for such equipment will be provided by the Technology Department who will also ensure that said equipment is properly secured and prepared for use.
- F. The Technology Department will process all orders for computer equipment/software purchased with district moneys, or grant moneys available to the district.
- G. The Technology Department will ensure that equipment purchased is properly installed and secured in a timely fashion prior to use by staff or students.
- H. The Technology Department will ensure that legal licenses are maintained on all software used in the district.

#### Maintenance of District-owned Equipment

1. The Technology Department is responsible for maintenance on all district computers/software. They will maintain a list of vendors who can assist in this process when necessary. The Technology Department will determine the most expedient method for repairs.
2. Repair work includes:
  - A. Warranty work done by manufacturer.
  - B. In-house repairs.
  - C. Contracted repairs through independent vendors.
3. The Technology Department will ensure that warranty work is completed by vendor/manufacturer rather than district staff, and that the work be of sufficient quality to ensure the continued use of the equipment.
4. The Technology Department will ensure that repairs are performed expeditiously, and that where possible, backup units and parts are maintained to prevent long delays in use of the equipment while parts are being ordered or reconditioned.
5. The Technology Department will maintain adequate lists to ensure that materials returned to manufacturers or sent to independent contractors are tracked and returned to the district.

6. Funding for repairs.
  - A. The Technology Department will be responsible for payment of all repairs.
  - B. The Technology Department will fund all repairs made for computer equipment at Central Office including equipment used by the Board of Education.
  - C. Funding for all other repairs will come from the department or school to whom the equipment is assigned. These departments/schools will provide an account code to the Technology department with sufficient funding to cover the expense of repairs prior to the repair being made.
  - D. Repairs needed to equipment caused by negligence, misuse, or uses of equipment other than district purposes will be the responsibility of the employee to whom equipment is assigned.
  - E. The Technology Department will complete all repairs, regardless of reason.
7. Expendable items (ribbons, cartridges, paper, forms) are to be ordered by the department/school using the items.
8. Yearly Maintenance
  - A. District-owned computers will be cleaned and checked at least once a year.
    - (1) Maintenance will include:
      - a. Blowing out the computer case.
      - b. Defragmenting the hard drive of computer.
      - c. Cleaning the cases and keyboards.
      - d. Reinstalling software when necessary.
      - e. Checking on the overall performance/serviceability of the equipment.
      - f. Checking printers for wear/replacement.

#### Instruction for Staff/Faculty

1. The Technology Department in conjunction with the departments of secondary and elementary instruction will ensure that adequate instruction is provided teachers and staff who will be assigned to use the computer systems purchased by the district and made available for their use.
2. Staff/faculty will be encouraged to receive training provided at the Baptiste Computer Training Lab.
3. Instructors hired to train staff/faculty will be compensated per district policy.

4. Staff/faculty will either be provided with release time or hourly compensation according to district policies for in-district training.
5. The Technology Department will maintain a help desk to assist users with various software and hardware issues.