

## TECHNOLOGY CONDUCT - EMPLOYEES

Technology offers opportunities for educators to enhance and expand their learning, as well as that of the students served in the Mason City Community School District. There are important responsibilities as well. The school district provides access, training and support to the extent possible so that all employees have the opportunity to benefit professionally and personally. District employees are expected to exhibit the same high level of ethical and business standards when using technology as they do with more traditional workplace communication resources. The many technologies provided by the district are intended for educationally-related use. It is the responsibility of employees to see that technology is used in an efficient, ethical and lawful manner.

### Employee Responsibility:

All employees are responsible for safeguarding information and the physical assets that store this information. Employees are responsible for using computing resources in an effective and lawful manner, consistent with the provisions of this policy.

All employees understand that there is no right to privacy associated with the Mason City Community School District equipment, the Internet, electronic mail, or any other communications devices. Mason City Community School District has the responsibility and the right to monitor all communications, retain records of all communications, and use all communications as permitted by law.

### Compliance:

Employees will comply with all sections of this policy. Violations of this policy may result in disciplinary action, which may include denial of system access, termination and/or criminal prosecution as deemed appropriate by the school district. It is not possible to list all behaviors that are prohibited or considered unacceptable. This list is representative of the types of activities which may result in disciplinary action and is not intended to be all-inclusive.

1. Unauthorized copying or installation of any software (including operating systems, programs, applications, databases, or code), which is licensed or protected by copyright.
2. "Computer hacking" (i.e. unwanted or unsolicited entry into a computer system)
3. Knowingly introducing a virus to a computer or network.
4. Unauthorized access, intentional damage, or misuse of systems, applications, databases, code, or data. (examples, but not limited to these)
  - a. Attempting to gain another user's password or log on as another user
  - b. Permitting use of an assigned account by another person
5. Inappropriate, unauthorized or unlawful use of any form of media or technology, system, or network owned or leased by the school district. (examples, but not limited to these)
  - a. Transfer or use of copyrighted materials through the school's computer resources, without explicit consent of the owner
  - b. Taking or altering another's work without permission
  - c. Knowingly allow non-school personnel access to or use of MCCSD equipment
6. Use of the district's technology for personal financial gain.
7. Fraudulent, harassing, threatening, discriminatory, sexually explicit or obscene messages and/or materials that are transmitted, printed, requested or stored. "Chain letters," solicitations and other forms of mass mailings are not permitted.
8. Use of district technology for political activity, lobbying, or any other use which would be in conflict with ethical standards of public employees.
9. Using technology resources excessively or in such a manner that primary educational responsibilities of the staff member are not fulfilled.

Regulation 404.1R1 contains E-mail regulations, 404.1R2 contains Internet regulations, and 404.1R3 contains general regulations.

Legal Reference: Iowa Code § 279.8 (2003).

Approved 03-18-96 Reviewed 1998, 2001, 2004, 2009 Revised 03-16-98, 01-15-01, 03-15-04