

ACCEPTABLE USE REGULATIONS FOR STAFF

A. BACKGROUND

The network is provided for staff and students to tap educational resources, conduct research and communicate with others. Communications over the network are often public in nature therefore general rules and standards for professional behavior and communications will apply.

Staff will employ electronic mail on a regular basis at work as a tool for communications. The District may rely upon this medium to communicate information, and all staff will be responsible for checking and reading messages regularly.

B. INFORMATION TECHNOLOGY RULES

Electronic mail and telecommunications are not to be utilized by employees to share confidential information about students or other employees because messages are not entirely secure.

Network administrators may review files and communications to maintain system integrity and to ensure that staff members are using the system responsibly. Users should not expect that files stored on District servers are private.

The Network Engineer will report inappropriate behaviors to the employee's supervisor or administrator. Violations may result in disciplinary action and/or a loss of access. When applicable, law enforcement agencies may be involved.

Each employee will be given a copy of the Information Technology policy, regulations and exhibits on an annual basis in their school handbook.

1. Personal Safety

- a. Users will not post personal contact information about themselves or other people. Personal contact information includes name, address, telephone numbers, home address, etc.

FOR STAFF

- b. Users will promptly disclose to their building principal or supervisor any message they receive that is inappropriate or makes them feel uncomfortable.

2. Illegal Activities

- a. Users will not attempt to gain unauthorized access to the District network. This includes attempting to log in through another person's account or access another person's files.
- b. Users will not make deliberate attempts to disrupt the network performance or destroy data by spreading computer viruses or by any other means.
- c. Users will not use the District system to engage in any illegal act.

3. System Security

- a. Users are responsible for the use of their individual account. They should take reasonable precautions to prevent others from access.
- b. Users will immediately notify the Network Engineer if they have identified a possible security problem.

4. Inappropriate Language

- a. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
- b. Restrictions against inappropriate language apply to public messages, private messages, and material posted on web pages.

5. Unacceptable Activities

Users are not permitted to:

- a. Send or display offensive messages or pictures;
- b. Harass, insult or attack others;
- c. Intentionally waste limited resources;
- d. Download songs, games and other non-curriculum information;
- e. Use a password other than their own; and/or
- f. Utilize the network for banking, political lobbying, commercial ventures, union activities, gambling or personal purchases.

DATE: June 23, 1999