Employee Use of Technology

User Obligations and Responsibilities

Employees are authorized to use the District's on-line and network services in accordance with the user obligations and responsibilities specified below.

1. Employees shall use the system only for purposes related to their employment in conducting the District's business. Commercial, political and/or personal use of the system is strictly prohibited. The District reserves the right to monitor any on-line communications for improper use.

2. Users shall not read other users' mail or files. They shall not attempt to interfere with others users' ability to send or receive electronic mail, nor shall they attempt to read, delete, copy, modify or forge others users' mail.

3. If passwords are used, passwords must be known to the Superintendent or designee so that he/she may have system access when the employee is absent. Employees may not use private passwords that prohibit District access to information for which the District has responsibility for or ownership thereof. The District has a need for and maintains access to all information on the District's network.

4. Users shall not use the system to promote unethical practices or any activity prohibited by law or District policy.

5. Users shall not transmit material that is threatening, obscene, disruptive or sexually explicit, or that could be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age disability, religion or political beliefs.

6. Copyrighted material may not be placed on the system without the author's permission. Users may download copyrighted material for instructional use only and only in accordance with copyright laws.

7. The employee in whose name an on-line services account is issued is responsible for its proper use at all times. Users shall keep personal account numbers, home addresses and telephone numbers private. They shall use the system only under their own account number.

Employee Use of Technology (continued)

8. Vandalism will result in the cancellation of user privileges. Vandalism includes uploading, downloading or creating computer viruses and/or any malicious attempt to harm or destroy District equipment or materials or the data of any other user.

9. Employees understand that electronic messages may be archived and available to the Superintendent or designee on an as-needed basis to monitor system usage.

10. Users shall report any security problem or misuse of the District's network to the Superintendent or designee.