

Information Technology Resources Acceptable Use Policy

The District provides information technology resources for use by certified and classified employees and students in connection with its public education missions and programs. For purposes of this Policy, the phrase “information technology resources” means and includes any hardware or software intended for the storage, transmission and use of information as well as the digital content files that may be stored, transmitted, or used with hardware or software. Such definition includes electronic mail, voice systems, local databases, externally accessed databases, CD-ROM, DVD, video, recorded magnetic media, digital video or photographic files, or other digitized information. The phrase also includes any wire, radio, electromagnetic, photo-optical, photo-electronic or other facility used in transmitting electronic information and any computer facilities or related electronic equipment that electronically stores such communications.

Responsibilities of Users

All users of the District’s information technology resources have the following responsibilities:

1. Access to the District’s information technology resources is provided with the expectation that resources will be used in a lawful manner at all times and in compliance with federal and state laws and District policies. Users are responsible for using the District’s information technology resources appropriately to maintain the integrity of the information technology resources and, in appropriate circumstances, the privacy, confidentiality, and security of the electronic information.
2. Individuals may not disclose, give, loan, share, or otherwise permit any other person to use the access privileges granted to them. Access to secured information resources is provided only with proper authorization.
3. Users are responsible for all actions and activities that occur while using District information technology resources assigned or made available to them and shall use such information technology resources only for their intended use.
4. Users may not attempt to circumvent login procedures on any computer system or otherwise attempt to gain unauthorized access. Such actions are a specific violation of this policy and also may be a crime under federal or state law.
5. All users shall use the District’s information technology resources in a manner that does not in any way interfere with, compromise, or impair the performance, functionality, or integrity of the District’s information technology resources and shall comply with all District administrative policies and procedures regarding software installation, upgrades and access to and use of secured data.
6. Users shall not act in any manner that impedes the performance of the District’s information technology resources, may not send “spam”, “chain letters”, internet service attacks or other activities that infringe on the rights of privacy of other users.
7. Users shall respect the rights of copyright owners and, when appropriate, obtain permission from owners before using or copying protected material, including but not limited to, music, movies, software, documents, images, or multimedia objects.

8. Incidental personal use of District information technology resources, including the District's email, is permitted provided that such personal use does not interfere with the District's educational missions and operations, does not violate District policies, does not result in additional costs to the District and does not have a negative impact on the user's academic or job performance, as the case may be.

9. Users may not use information technology resources for commercial purposes, for personal financial gain, or to solicit support for other organizations that are not otherwise authorized to use District facilities or information technology resources.

10. Individuals may use information technology resources to exchange personal ideas and opinions, including those dealing with political issues and such use will be considered incidental personal use. However, the District's information technology resources including email may not be used to support partisan political candidates, political party fund raising or other partisan political activities.

11. Users may not use the District's information technology resources for activities that are illegal, threatening, or deliberately destructive.

District Responsibilities

Because District information technology resources are publicly-owned and maintained, the District has the responsibility to monitor, audit, and assure the proper use of information technology resources. Although the District does not routinely read or monitor individual users' use of the District's information technology resources, it does monitor systems for misuse. Accordingly, users shall not have any expectation of privacy, confidentiality secured access to personal data, email, or other information transmitted or stored on the District's information technology resources.

Reporting Irresponsible Use of Electronic Information Resources

All users have a responsibility to report any discovered unauthorized access attempts or other improper usage of District information technology resources to the District's Director of Technology (telephone 620-615-5640 or email, tsc@usd308.com) who will coordinate the technical and administrative response to any such unauthorized access or use. Reports of all apparent violations of District policies regarding the use of District information technology resources shall be reported and treated in the same manner as is provided for the responding to other violations of District policies and procedures.

Consequences of Violations

Use of the District's information technology resources in violation of this policy or applicable federal or state law is prohibited and may subject the user to disciplinary action including, but not limited to, suspension of the user's access to the electronic information resources. There may be other disciplinary consequences under other District policies and federal or state laws including but not limited to those relating to computer crime and intellectual property rights violations.