SUBJECT: ACCEPTABLE USE POLICY (PERSONNEL)

The District provides access to digital information systems through the District's computer network. This policy establishes acceptable use expectations, safeguards district information resources, and assists in compliance with applicable laws, regulations, and district procedures.

Definitions

For the purposes of this policy, the following definitions apply:

a) "Digital information systems" means:

1. All computer hardware, devices, and systems owned or leased by the District, including but not limited to:

   (a) Computers of any size and form factor, including smartphones, tablets, and interactive whiteboards;

   (b) Networks;

   (c) Internet access;

   (d) Network servers;

   (e) Routers, cables, and switches;

   (f) Video conferencing equipment; and

   (g) Internet of things devices (devices that collect and share data, such as security systems or wearable devices); and

2. Software that is owned, leased, licensed, and/or used (including free) by the District, or that the District has the use of through a cooperative services agreement (CoSer), and that is used to create, modify, store, or transmit information in a digitized form.

b) "Personnel" means all district employees, substitutes, contractors, consultants, student teachers, volunteers, and any other individuals granted access to district digital information systems.

Overview

Prior to accessing these digital information systems, all personnel must read, sign, and return the applicable acceptable use form(s). The District will provide reasonable oversight for their digital information systems, however, responsibility for their use ultimately lies with the individual user.

(Continued)

SUBJECT: ACCEPTABLE USE POLICY (PERSONNEL) (Cont'd.)

Except for any privilege or confidentiality recognized by law, district personnel have no legitimate expectation of privacy during any use of the District's digital information systems or in any data on those systems. Any use may be monitored, recorded, or accessed in any manner by authorized personnel without additional prior notice to personnel. Periodic monitoring may be conducted of digital information systems used, including, but not limited to, all computer files and all forms of electronic communication.

The District reserves the right to impose restrictions on the use of particular digital resources. For example, the District may block access to websites, services, or applications not serving legitimate business or educational purposes or may restrict users' ability to attach personal devices to the District's digital information systems or devices.

Acceptable Use

All uses of district digital information systems by district personnel must comply with district policies, standards, procedures, and regulations, as well as any applicable federal and state laws and regulations, including but not limited to copyright laws and licensing agreements.

Acceptable uses of the district digital information systems include, but are not limited to, the following:

a) Protecting confidential information and student data from unauthorized use or disclosure;

b) Using digital information systems to support student learning and district business operations;

c) Maintaining professional conduct in online communications and behavior as in all other aspects of work;

d) Reporting suspected cybersecurity incidents to appropriate district information technology personnel immediately; and

e) Observing authorized levels of access and utilizing only approved digital information system devices and services.

Unacceptable Use

The following list is not intended to be exhaustive, but provides a framework for determining activities that constitute unacceptable use of district digital information systems.

(Continued)

SUBJECT: ACCEPTABLE USE POLICY (PERSONNEL) (Cont'd.)

Unacceptable uses of the district digital information systems include, but are not limited to, the following:

a) Distributing, transmitting, posting, or storing any electronic communications, materials, or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;

b) Engaging in unauthorized use or disclosure of personal, private, sensitive, and/or confidential information, including entering this information into generative artificial intelligence (AI) or other AI systems;

c) Connecting unapproved devices to the district digital information systems;

d) Installing, downloading, or running software that has not been approved in accordance with district policies;

e) Using district digital information systems for commercial or personal purposes, including solicitation or advertisement, in support of religious, political, not-for-profit organizations, for-profit business activities, or in support of other outside employment or business activity;

f) Providing unauthorized third parties access to the district digital information systems;

g) Tampering with, disengaging, or otherwise circumventing district-implemented IT security;

h) Plagiarizing or engaging in copyright infringement; and

i) Using district digital information systems to access personal social media platforms, or other personal account-based platforms.

Occasional and Incidental Personal Use

The District permits occasional and incidental personal use of its digital information systems, provided the use is consistent with this policy, is limited in amount and duration, does not conflict with the user's ability to perform their duties, and does not impede the ability of other users to utilize the system for legitimate work purposes, including but not limited to, extensive bandwidth, resource, or storage utilization. The District may revoke or limit this permission at any time.

(Continued)

SUBJECT: ACCEPTABLE USE POLICY (PERSONNEL) (Cont'd.)

Individual Accountability

Individual accountability is required when accessing all district digital information systems. Users must comply with district procedures and any other applicable district documents for data networks and security access which may include password protocols, use of multi-factor authentication, and other security measures as defined by the District. All users must treat their credentials as confidential information which must not be disclosed or shared. All users are responsible for protecting against unauthorized activities performed under their user ID, devices, or any other district system.

Compliance

Any violation of this policy may subject the user to disciplinary action, civil penalties, and/or criminal prosecution. The District will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

NOTE: Refer also to Policies #5672 -- Information Security Breach and Notification
#5676 -- Privacy and Security for Student Data and Teacher and Principal Data
#5850 -- Data Networks and Security Access
#5851 -- Cybersecurity Incident Response
#6411 -- Use of Email in the District
#6412 -- Social Media Use
#8271 -- Internet Safety/Internet Content Filtering

Adoption Date