SUBJECT: OPERATION OF MOTOR-DRIVEN VEHICLES ON DISTRICT PROPERTY

The use of motor-driven vehicles, including cars, snowmobiles, mini-bikes, motorcycles, all-terrain vehicles (ATVs), electric scooters (e-scooters), bicycles with an electric assist (e-bikes), and other like vehicles, is prohibited on any school grounds or areas except for authorized school functions or purposes. A school function means a school-sponsored or school-authorized extracurricular event or activity regardless of where the event or activity takes place, including any event or activity that may take place in another state.

All student vehicles must be registered with the high school principal and parked in authorized areas only.

Education Law Section 2801(1)
Vehicle and Traffic Law Section 1670

Adoption Date: 6/13/22
Revised:

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, or licensed 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, email, or other personal account-based platforms.

j) 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.

(Continued)

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

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: 6/13/22
Revised Date:

SUBJECT: STUDENT DIRECTORY INFORMATION

The District will publish an annual public notice informing parents, persons in parental relation, or eligible students (i.e., a student 18 years of age or older or who is attending an institution of post-secondary education) of (1) the District's definition of directory information; (2) the parent's, person in parental relation's, or eligible student's right to opt-out of, in writing, the release of student directory information; and (3) the time period in which to do so.

Directory information is information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Following this public notice and a reasonable period to opt-out, the District may release this information to an outside group without individual consent.

The Family Educational Rights and Privacy Act defines student directory information as any of the items as indicated in the following list. The District defines student directory information to include only the items of information checked below:

X___ Student's name
_____ Address
_____ Telephone listing
_____ Date of birth
_____ Place of birth**
X___ Major field of study
X___ Grade level
X___ Participation in officially recognized activities and sports
_____ Weight and height (for members of athletic teams)
_____ Dates of attendance
X___ Honors, degrees, and awards received
_____ Email address
X___ Photograph
X___ Name of educational institution previously attended
_____ Student ID number, user ID, or other unique personal identifier used to communicate in electronic systems but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a PIN, password, or other factor known or possessed only by the authorized user.
_____ Student ID number or other unique personal identifier that is displayed on a student ID badge, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a PIN, password, or other factor known or possessed only by the authorized user.

** June 2025 New York State Education Department document "Questions and Answers Regarding Directory Information" notes that releasing student place of birth may be considered harmful and an invasion of privacy under current standards, and that educational agencies should not deem place of birth to be directory information.

(Continued)

SUBJECT: STUDENT DIRECTORY INFORMATION (Cont'd.)

Parents, persons in parental relation, and eligible students may not, by opting out of disclosure of directory information, prevent a school from requiring a student to wear or present a student identification card or a badge that displays information that may be directory information. A student's social security number, in whole or part, will not be designated as directory information.

20 USC Section 1232g
34 CFR Part 99

NOTE: Refer also to Policies #7240 -- Student Records: Access and Challenge
#7242 -- Military Recruiters and Institutions of Higher Education

Adoption Date: 6/13/22
Revised:

SUBJECT: ACCEPTABLE USE POLICY (STUDENT)

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, or licensed 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.

Overview

Prior to accessing district digital information systems all students 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.

Students are provided with access to the District's digital information systems for the purpose of completing instructional assignments under the guidance of a teacher. Student use of the systems must comply with the standards in district policy, the District Code of Conduct, and/or other similar documents. Failure to comply may result in disciplinary action.

(Continued)

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

Except for any privilege or confidentiality recognized by law, students 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 students. 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 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 student use of district digital information systems 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 student uses of the District's digital information systems include, but are not limited to:

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

b) Using digital information systems to support learning;

c) Maintaining respectful conduct in their online communications and behavior;

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.

In addition, students will ensure that their usage of the district digital information systems is aligned with the competencies of good digital citizenship. Students should be:

a) Informed: evaluate the accuracy, perspective, and validity of digital media;

b) Inclusive: open to hearing and recognizing multiple viewpoints and engaging others online with respect and empathy;

c) Balanced: participate in a healthy variety of online activities and prioritize their time between virtual and physical activities;

(Continued)

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

d) Engaged: use technology and digital channels to solve problems and be a force for good in their community; and

e) Alert: aware of their digital actions and know how to be safe online.

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.

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

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, or for-profit business activities;

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, email, or other personal account-based platforms.

(Continued)

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

j) Individual accountability is required when accessing all district digital information systems. Student 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 student users must treat their credentials as confidential information which must not be disclosed or shared. All student 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 #7316 -- Use of Internet-Enabled Devices During the School Day
#8271 -- Internet Safety/Internet Content Filtering
District Code of Conduct

Adoption Date: 6/13/22
Revised Date: