INVER GROVE HEIGHTS SCHOOLS ISD 199

STUDENT ELECTRONIC TECHNOLOGIES ACCEPTABLE USE

POLICY:	524
ADOPTED:	04/27/20
REVISED:	05/16/22

I. Purpose

The purpose of this policy is to set forth policy and guidelines for student access to the school district electronic technologies, use of personal electronic devices within the district, electronic communications, use of the district's network, Internet, and social networking tools.

II. General Statement of Policy

District 199 considers its own stated educational mission, goals, and objectives when making decisions regarding student access to School District technology. Access to the district's network and Internet enables students to explore libraries, databases, web pages, other online resources, and connect with people around the world.

District electronic technologies are used for educational purposes. Use of the district's electronic technologies is a privilege, not a right. The district's network, an educational technology, is a limited forum; the district may restrict speech for educational reasons.

All ISD 199 students are issued a district technology device to be used for educational purposes. Students are expected to use their district issued devices for educational purposes while in school. Non-school issued devices shall not be permitted to connect to the school district network during the school day. ISD 199 is not responsible for any non-school issued devices on school property.

III. Guidelines in Use of Electronic Technologies

Electronic technologies are assets of the school district and are protected from unauthorized access, modification, destruction or disclosure. Use of personal devices, while on district property, is subject to all policies and guidelines, as applicable, plus any state and federal laws related to Internet use, including copyright laws.

A. The district reserves the right to monitor, read or copy any item on or using the district's electronic technologies, including its network.

B. By authorizing use of the district system, the district does not relinquish control over materials on the system or contained in files on the system. Users should not expect privacy in the contents of personal files on the district system.

C. Students will not vandalize, damage or disable any electronic technology or system used by the district.

D. Routine maintenance and monitoring of electronic technologies, including the

district network, may lead to a discovery that a user has violated this policy, another school district policy or the law.

IV. User Notification

Users will be notified of school district policies relating to Internet use. This notification must include the following:

A. Notification that Internet use is subject to compliance with district policies.

B. Disclaimers limiting the district's liability relative to:

1. Information stored on district media, drives or servers.

2. Information retrieved through district computers, networks or online resources.

3. Personal property used to access district computers, networks or online resources.

4. Unauthorized financial obligations resulting from use of district resources or accounts to access the Internet.

C. A description of the privacy rights and limitations of district sponsored or managed Internet accounts.

D. Notification that the collection, creation, reception, maintenance and dissemination of data via the Internet, including electronic communications, is governed by Policy 406, Public and Private Personnel Data, and Policy 515, Protection and Privacy of Student Records.

E. Notification that should the user violate the district's acceptable use policy, the user's access privileges may be revoked, academic sanctions may result, school disciplinary action may be taken, and/or appropriate legal action may be taken.

F. Notification that all provisions of the acceptable use policy are subordinate to local, state and federal laws.

G. Family Notification

1. Notification that the district uses technical means to limit student Internet access however, the limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.

2. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student or the student's parents and/or guardians.

V. Unacceptable Uses of Electronic Technologies and District Network

Misuse of the district's electronic technologies may lead to discipline of the offending student. The following uses of school district electronic technologies while either on/off district property and/or personal electronic technologies while on district property and district network ("electronic technologies") are considered unacceptable:

A. Users will not use electronic technologies to create, access, review, upload, download, complete, store, print, post, receive, link, transmit or distribute:

1. Pornographic, obscene or sexually explicit material or other visual depictions;

2. Obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful or sexually explicit language;

3. Materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;

4. Materials that use language or images that advocate violence or discrimination toward other people or that may constitute harassment, discrimination or threatens the safety of others;

5. Storage of personal photos, videos, music or files on district servers or cloud services. The district does not take responsibility for personal files stored on district technologies.

B. Users will not use electronic technologies to knowingly or recklessly post, transmit or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

C. Users will not use electronic technologies to engage in any illegal act or violate any local, state or federal laws.

D. Users will not use electronic technologies for political campaigning.

E. Users will not use electronic technologies to vandalize, damage or disable the property of another person or organization. Users will not make deliberate attempts to degrade or disrupt equipment, software or system performance. Users will not tamper with, modify or change the district system software, hardware or wiring or take any action to violate the district's security system. Users will not use the district's electronic technologies in such a way as to disrupt the use of the system by other users.

F. Users will not use electronic technologies to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct permission of that person.

G. Users must not deliberately or knowingly delete other users files or data.

H. Users will not use electronic technologies to post information in public access areas regarding private or confidential information about another person. Private or confidential information is defined by board policy, state law, and federal law.

1. Refer to Policy 515 (Protection and Privacy of Student Records) for directions on directory information for students and how this can be used.

2. This paragraph does not prohibit communications between employees, parents/guardians or other staff members related to students.

3. This paragraph specifically prohibits the use of electronic technologies to post private or confidential information about another individual, employee or student, on social networks, including but not limited to social networks such as “Facebook,” “Twitter,” “Instagram,” Snapchat,” and “Reddit,” and similar websites or applications.

I. Users will not repost or resend a message that was sent to the user privately without the permission of the person who sent the message.

J. Users will not attempt to gain unauthorized access to the district’s electronic technologies or any other system through electronic technologies.

K. Users will not attempt to log in through another person’s account, or use computer accounts, access codes or network credentials other than those assigned to the user.

L. Users must keep all account information and passwords private.

M. Messages and records on the district’s electronic technologies may not be encrypted without the permission of the Director of Instructional Technology.

N. Users will not use electronic technologies to violate copyright laws or usage licensing agreements:

1. Users will not use another person’s property without the person’s prior approval or proper citation;

2. Users will not download, copy or exchange pirated software including freeware and shareware; and

3. Users will not plagiarize works found on the Internet or other information resources.

O. Users will not use electronic technologies for unauthorized commercial

purposes or financial gain unrelated to the district's mission. Users will not use electronic technologies to offer or provide goods or services or for product placement.

P. Use of Unmanned Airborne Vehicles (UAV's) or drones is prohibited on school property without prior approval of the Director of Instructional Technology or building principal.

VI. Student Electronic Technologies Use

All student electronic device users will follow the school district's guidelines for electronic devices. **All required student digital learning device agreements must be signed by the student and/or parent or guardian before a device will be assigned**. Due to the rapid evolution of educational technologies these agreements will be reviewed on an as-needed basis.

A. Students using educational technologies for social networking are limited to educational purposes and must follow the student digital learning device agreements and Policy 514, Bullying Prohibition.

B. The proper use of the Internet and educational technologies and the educational value to be gained from proper usage is the joint responsibility of students, parents/guardians and employees of the school district.

C. The school district provides access to electronic mail for district communication between district employees and students, families, and the community. Students in grades K-8 will only be allowed to send emails within the isd199.org domain.

1. The email system will not be used for outside business ventures or other activities that conflict with board policy.

2. All emails received by, sent through, or generated by electronic technologies using the district network are subject to review by the district.

3. Appropriate language must be used when communicating using the district email system or network.

4. All emails are assumed to be documents that can be disclosed to the public unless the content of the email is protected as private or confidential information under data privacy laws. All information contained in an email must be treated in accordance with Policy 406, Public and Private Personnel Data, and Policy 515, Protection and Privacy of Student Records regarding student and employee data privacy.

5. Students will not provide access to their email accounts.

6. Students will report inappropriate emails to the school administration.

VII. Student Inappropriate Internet Use

Electronic technologies are provided primarily for school-related, educational purposes.

A. Inappropriate use of electronic technologies includes, but is not limited to:

1. Posting, viewing, downloading or otherwise receiving or transmitting offensive, defamatory, pornographic or sexually explicit materials;

2. Posting, viewing, downloading or otherwise receiving or transmitting materials that use language or images that advocate violence or discrimination toward other persons;

3. Posting, viewing, downloading or otherwise receiving or transmitting material that may constitute harassment or discrimination contrary to district policy and state and federal law;

4. Engaging in computer hacking or other related activities;

5. Attempting to, actually disabling or compromising the security of information contained on the district network or any computer;

6. Using encrypted technologies, such as but not limited to VPN, to circumvent the district web filtering system.

7. Engaging in any illegal act in violation of any local, state or federal laws.

B. Students may participate in public Internet discussion groups using the electronic technologies, but only to the extent that the participation:

1. Is school-related and is permitted by district staff;

2. Does not reflect adversely on the district;

3. Is consistent with district policy; and

4. Does not express any position that is, or may be interpreted as, inconsistent with the district's mission, goal or strategic plan.

C. Students may not use the district network or electronic technologies to post unauthorized or inappropriate personal information about another individual on social networks, including but not limited to social networks such as "Facebook," "Twitter," "Instagram," Snapchat," and "Reddit," and similar websites or applications.

D. Students will observe all copyright laws. Information posted, viewed or downloaded from the Internet may be protected by copyright. Students may reproduce copyrighted materials only in accordance with Policy 622,

Copyright Policy.

VIII. Student Responsibilities

A. Individual passwords for electronic devices are confidential and must not be shared.

1. If a student's password is compromised or learned by another person, the Department of Instructional Technology must be notified.

2. A student is responsible for all activities performed using the student's password.

3. No student should attempt to gain access to another student's documents without prior express authorization.

4. Any device with access to private data must not be left unattended and must be protected by password protected screen savers.

B. Students will care for all district issued technologies as outlined in student digital learning device agreements.

C. Students who fail to adhere to district policy are subject to disciplinary action. Disciplinary action may include suspension or withdrawal of Internet or email access, payment for damages or repair, termination and/or referral to civil or criminal authorities for prosecution.

IX. Records Management and Archiving

All technological data is data under the Minnesota Government Data Practices Act, the Family Educational Rights and Privacy Act, Records Retention Schedule, and school board policy.

X. Filter

A. With respect to any of its electronic technologies with Internet access, the district will follow the guidelines provided by the Children's Internet Protection Act, and will monitor the online activities of users and employ technology protection measures during any use of such computers by users. The technology protection measures utilized will block or filter Internet access to any visual depictions that are:

1. Obscene;

2. Child pornography; or

3. Harmful to minors.

B. The term “harmful to minors” means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion; or

2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts or a lewd exhibition of the genitals; and

3. Taken as a whole, lacks value to minors.

C. Disclaimer limiting the district’s liability

The district uses technical means to filter Internet access however, this does not provide foolproof means for enforcing the provisions of this acceptable use policy.

XI. Liability

Use of the school district’s electronic technologies is at the user’s own risk. The system is provided on an “as is, as available” basis. The district will not be responsible for any damage users may suffer. The district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system, nor is it responsible for damages or injuries from improper communications or damage to property used to access school computers and online resources. The district will not be responsible for financial obligations arising through unauthorized use of the district’s educational technologies or the Internet.

XII. Implementation and Policy Review

A. The school district administration may develop appropriate user notification forms, guidelines and procedures necessary to implement this policy. These guidelines, forms and procedures will be an addendum to this policy.

B. The administration will revise the user notifications, including student and parent/guardian notifications, if necessary, to reflect the adoption of these guidelines and procedures.

C. The district educational technologies policy is available for review by parents/guardians, employees and members of the community.

D. This policy will be reviewed annually.

Legal References:
15 U.S.C. § 6501 et seq. – Children's Online Privacy Protection Act
17 U.S.C. § 101 et. seq. – Copyrights
20 U.S.C. § 6751 et seq. – Enhancing Education through Technology Act of 2001
47 U.S.C. § 254 - Children's Internet Protection Act of 2000 (CIPA)
47 C.F.R. § 54.520 - FCC rules implementing CIPA
Minn. Stat. § 121A.031 – School Student Bullying Policy
Minn. Stat. § 125B.15 – Internet Access for Students
Minn. Stat. § 125B.26 – Telecommunications/Internet Access Equity Act
Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503 (1969)
United States v. American Library Association, 539 U.S. 194 (2003)
Doninger v. Niehoff, 527 F.3d 41 (2nd Cir. 2008)
R.S. v. Minnewaska Area Sch. Dist. No. 2149, No. 12-588, 2012 WL 3870868 (D. Minn. 2012)
Tatro v. Univ. of Minnesota, 800 N.W.2d 811 (Minn. App. 2011), aff'd on other grounds 816 N.W.2d 509 (Minn. 2012)
S.J.W. v. Lee's Summit R-7 Sch. Dist., 696 F.3d 771 (8th Cir. 2012)
Kowalski v. Berkeley County Sch., 652 F.3d 565 (4th Cir. 2011)
Layshock v. Hermitage Sch. Dist., 650 F.3d 205 (3rd Cir. 2011)
Parents, Families and Friends of Lesbians and Gays, Inc. v. Camdenton R-III Sch. Dist., 853 F.Supp.2d 888 (W.D. Mo. 2012)
M.T. v. Cent. York Sch. Dist., 937 A.2d 538 (Pa. Commw. Ct. 2007)

Cross References:
Policy 403 - Discipline, Suspension, and Dismissal of School District Employees
Policy 406 - Public and Private Personnel Data
Policy 424 - Employee Electronic Technologies Acceptable Use
Policy 505 - Distribution of Non-school Sponsored Materials on School Premises by Students and Employees
Policy 506 - Student Discipline
Policy 514 - Bullying Prohibition Policy
Policy 515 - Protection and Privacy of Student Records
Policy 519 - Interviews of Students by Outside Agencies
Policy 521 - Student Disability Nondiscrimination
Policy 522 - Student Sex Nondiscrimination
Policy 603 - Curriculum Development
Policy 604 - Instructional Curriculum
Policy 606 - Textbooks and Instructional Materials
Policy 806 - Crisis Management Policy
Policy 904 - Distribution of Materials on School District Property by Nonschool Persons
Elementary and Secondary Student Expectations Handbooks