

COLOGNE ACADEMY
MANUAL OF SCHOOL POLICIES APPROVED BY THE BOARD

524 INTERNET ACCEPTABLE USE AND SAFETY POLICY

I. PURPOSE

The purpose of this policy is to set forth policies and guidelines for the use of district and personal technology resources, access to the school district computer system and acceptable and safe use of digital resources, including electronic communications.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding user access to the school district technology resources, including electronic communications, the school district considers its own stated educational mission, goals, and objectives. Access to the school district technology resources enables users to explore countless resources which expand students' worldview while interacting with people locally and globally. The school district expects that employees will blend thoughtful use of the school district technology resources throughout the curriculum and will provide guidance and instruction to students in their use. The school district will educate students on the responsible and ethical use of technology, encompassing respectful online behavior, digital literacy, and awareness of cybersecurity and online safety.

III. LIMITED EDUCATIONAL PURPOSE

The school district is providing students with access to the school district digital resources which includes, but is not limited to desktops, laptops, tablets, district maintained servers, networks, and Internet access. The purpose of the system is more specific than providing students with general access to the Internet. The school district system has a limited educational purpose, which includes use of the system for classroom activities, educational research, and professional or career development activities. Users are expected to use technology resources and Internet access through the district system to further educational and personal goals consistent with the mission of the school district, strategic plan and school policies. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network.

IV. USE OF DIGITAL RESOURCES IS A PRIVILEGE

The use of the school district digital resources and use of the Internet is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the school district system, digital resources, or the Internet may result in one or more of the following consequences: suspension or cancellation of use or access privileges; payments for damages and repairs; discipline under other appropriate school district policies, including suspension, expulsion, exclusion, or termination of employment; or civil or criminal liability under other applicable laws.

V. PERSONAL TECHNOLOGY

Personal technology may be connected to the District's network or systems if it complies with district standards and is compatible with the district systems. Personal technology attached or connected to the district network are subject to the same policies and procedures established for the use of district owned equipment. The use of personal technology must adhere to the district Acceptable Use Policy (AUP).

District technicians will not service, repair, or maintain any personal technology. District will not be held liable for personal content housed on the device. Any software residing on personal technology must not interfere with the normal operation of district owned resources. District is not responsible for any physical damage, loss, or theft of the device. Internet usage or texting charges are the responsibility of the student.

VI. ACCEPTABLE USE GUIDELINES

A. Users must respect and protect the privacy of others by:

1. Using only assigned accounts.
2. Only accessing passwords, data, or networks to which they are authorized.
3. Refraining from distributing private information about others or themselves.

B. Users must respect and protect the integrity, availability, and security of all electronic resources by:

1. Observing all district Internet filters and posted network security practices.
2. Reporting security risks or violations to a teacher or network administrator.
3. Not destroying or damaging data, networks, or other resources that do not belong to them, without clear permission of the owner.
4. Notifying a staff member or administrator of computer or network malfunctions through the creation of a service request.

- C. Users must respect and protect the intellectual property of others by:
1. Following copyright laws (not making illegal copies of music, games, or movies).
 2. Citing sources when using others' work (not plagiarizing).

- D. Users must respect and practice the principles of community by:
1. Communicating only in ways that are kind and respectful.
 2. Reporting threatening or discomforting materials to a teacher or administrator.
 3. Not intentionally accessing, transmitting, copying, or creating material that violates the school's code of conduct (such as messages/content that are pornographic, threatening, rude, discriminatory, or meant to harass).
 4. Not intentionally accessing, sharing, copying, or creating material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).
 5. Not using the resources to further other acts that are criminal or violate the school's code of conduct.
 6. Avoiding spam, chain letters, or other mass unsolicited mailings.
 7. Refraining from buying, selling, advertising, or otherwise conducting business, unless approved as a school project.
 8. Not using any personal or school district device, such as a tablet, smartphone, computer, camera, or other electronic device, to take or electronically capture during school hours or at a school sponsored event an image (including a picture, video, or audio recording) of another student(s) or school employee(s) and then, at any time, post, share, or distribute an image of another student(s) or school employee(s) if the posting, sharing, or distributing of that image results in disruption of school operations, could be reasonably anticipated to disrupt school operations, or violates the data privacy rights of others.
 9. Not using any personal or school district device, such as a tablet, smartphone, computer, camera, or other electronic device, to take or electronically capture images of instructional materials, including, but not limited to, tests, worksheets, etc. without explicit consent from the teacher.

- E. Users may, if in accord with the policy above:
1. Design and post web pages and other material from school resources.
 2. Communicate electronically via tools such as email, chat, text, or videoconferencing (students require a teacher's permission).
 3. Install or download software, if also in conformity with laws and licenses (students must be under the supervision of a teacher).
 4. Use the resources for any educational purpose.

F. Consequences for Violation

Violations of these rules may result in disciplinary action, including the loss of a user's privileges to use the school's digital resources. Further

discipline may be imposed in accordance with the Board's Code of Conduct up to and including suspension or expulsion depending on the degree and severity of the violation.

G. Supervision and Monitoring

- B. The use of District owned information technology resources is not private. School and network administrators and their authorized employees monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement. The district reserves the right to determine which uses constitute acceptable use and to limit access to such uses. The district also reserves the right to limit the time of access and use.

VII. FILTER

- A. With respect to any of its computers with Internet access, the school district will monitor the online activities of both minors and adults and employ technology protection measures during any use of such computers by minors and adults. 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 serious literary, artistic, political, or scientific value as to minors.
- C. Software filtering technology shall be narrowly tailored and shall not discriminate based on viewpoint.
- D. An administrator, supervisor, or other person authorized by the Superintendent may disable the technology protection measure, during use

by an adult, to enable access for bona fide research or other lawful purposes.

- E. The school district will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

VIII. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of the District technology resources and use of the Internet shall be consistent with school district policies, student handbook and the mission of the school district.

IX. LIMITED EXPECTATION OF PRIVACY

- A. Users should have no expectation of privacy when using district equipment and networks.
- B. By authorizing use of the school district system, the school district does not relinquish control over materials on the system or contained in files on the system. Users should expect that all communications transmitted or received on the district system are PUBLIC INFORMATION and can be given to law enforcement agencies WITHOUT the user's prior consent.
- C. Routine maintenance and monitoring of the school district system may lead to a discovery that a user has violated this policy, another school district policy, or the law.
- D. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy.
- E. Families have the right at any time to investigate or review the contents of their student's files and email files. Families have the right to request the termination of their student's individual account at any time.
- F. The school district will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school district policies conducted through the school district system.

X. INTERNET USE AGREEMENT

- A. The proper use of the Internet, and the educational value to be gained from proper Internet use, is the joint responsibility of students, families and employees of the school district.

- B. This policy requires the permission of and supervision by the school's designated professional staff before a student may use a school account or resource to access the Internet.
- C. The Internet Use Agreement form for students must be read and signed by the user, family, and the supervising teacher. The form must then be filed at the school office. As supervising teacher's change, the agreement signed by the new teacher shall be attached to the original agreement.

XI. LIMITATION ON SCHOOL LIABILITY

Use of the school district system is at the user's own risk. The system is provided on an "as is, as available" basis. The school district will not be responsible for any damage users may suffer, including, but not limited to, loss, damage or unavailability of data stored on school district storage media, hard drives or servers, or for delays or changes in or interruptions of service or misdeliveries or non-deliveries of information or materials, regardless of the cause. The school district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system. The school district will not be responsible for financial obligations arising through unauthorized use of the school district system or the Internet.

XII. USER NOTIFICATION

- A. All users shall be notified of the school district's policies related to Internet use.
- B. This notification shall include the following:
 - 1. Notification that Internet use is subject to compliance with school district policies.
 - 2. Disclaimers limiting the school district's liability relative to:
 - a. Information stored on school district media devices, services, or servers.
 - b. Information retrieved through school district computers, networks, or online resources.
 - c. Personal property used to access school district computers, networks, or online resources.
 - d. Unauthorized financial obligations resulting from use of school district resources/accounts to access the Internet

3. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.
4. Notification that, even though the school district may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.
5. 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 and/or the student's family.
6. 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 Pupil Records.
7. Notification that, should the user violate the school district's acceptable use policy, the user's access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action may be taken.
8. Notification that all provisions of the acceptable use policy are subordinate to local, state, and federal laws.

XIII. FAMILY ' RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE

- A. Outside of school, families bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies, and other possibly offensive media. Families are responsible for monitoring their student's use of the school district system and of the Internet if the student is accessing the school district system from home or a remote location.
- B. Notification of this policy and the requirements herein will be provided to families and students as part of the annual district handbook.
- C. Families are herein notified that their students will be using school district resources/accounts to access the Internet.
- D. Limited alternatives to internet access may be available. Families requesting alternate access should contact your student's principal.

XIV. NOTIFICATION REGARDING TECHNOLOGY PROVIDERS

- A. "Technology provider" means a person who:
1. contracts with the school district, as part of a one-to-one program or otherwise, to provide a school-issued device for student use; and
 2. creates, receives, or maintains educational data pursuant or incidental to a contract with the school district.
- B. "Family" includes a natural parent, a guardian, or an individual acting as a parent or guardian in the absence of a parent or a guardian.
- C. Within 30 days of the start of each school year, the school district must give families and students direct and timely notice, by United States mail, e-mail, or other direct form of communication, of any curriculum, testing, or assessment technology provider contract affecting a student's educational data. The notice must:
1. identify each curriculum, testing, or assessment technology provider with access to educational data;
 2. identify the educational data affected by the curriculum, testing, or assessment technology provider contract; and
 3. include information about the contract inspection and provide contact information for a school department to which families or students may direct questions or concerns regarding any program or activity that allows a curriculum, testing, or assessment technology provider to access a student's educational data.
- D. The school district must provide families and students an opportunity to inspect a complete copy of any contract with a technology provider.
- E. A contract between a technology provider and the school district must include requirements to ensure appropriate security safeguards for educational data. The contract must require that:
- the technology provider's employees or contractors have access to educational data only if authorized; and
 - the technology provider's employees or contractors may be authorized to access educational data only if access is necessary to fulfill the official duties of the employee or contractor.
- F. All educational data created, received, maintained, or disseminated by a technology provider pursuant or incidental to a contract with a public educational agency or institution are not the technology provider's property.

XV. LIMIT ON SCREEN TIME FOR CHILDREN IN PRESCHOOL AND KINDERGARTEN

A. The school district administration may develop appropriate user notification forms, guidelines and procedures necessary to implement this policy for submission to the School Board for approval. Upon approval by the School Board, such guidelines, forms and procedures shall be an addendum to this policy.

B. The administration shall revise the user notifications, including student and family notifications, if necessary, to reflect the adoption of these guidelines and procedures.

C. The school district Internet policies and procedures are available for review by all family, staff and members of the community.

D. Because of the rapid changes in the development of technology, the School Board shall conduct an annual review of this policy.