



## Anderson School District 3

### **Policy IJNDB Use of Technology Resources in Instruction**

Issued 1/15

Purpose: To establish the board's vision and the basic structure for the use of technology resources in instruction.

The Internet can provide a vast collection of educational resources for students and employees. It is a global network that makes it impossible to control all available information. Because information appears, disappears and changes constantly, it is not possible to predict or control what students may locate. The school district makes no guarantees as to the accuracy of information received on the Internet. Although students will be under teacher supervision while on the network, it is not possible to constantly monitor individual students and what they are accessing on the network. Some students might encounter information that is not of educational value.

Inappropriate use of the district network, Internet or other technological service by any student will not be tolerated, and violations of these guidelines could subject the user to appropriate disciplinary actions including, but not limited to, denial of further access to the technologies, suspension from school and/or expulsion.

#### **Accessing inappropriate sites**

Student Internet activities will be monitored by the district to ensure students are not accessing inappropriate sites that have visual depictions that include obscenity, child pornography or are harmful to minors. In compliance with the Children's Internet Protection Act (CIPA), the school district will use technology protection measures to protect students from inappropriate access.

The district will provide reasonable notice to address and communicate its Internet safety measures.

#### **Reporting**

District and school computer technicians who are working with a computer and come across sexually explicit images of children must report this to local law enforcement. The report must include the name and address of the owner or person in possession of the computer.

The report should also be sent to the superintendent as soon as possible.

#### **Online behavior**

The district will educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. The superintendent or his/her designee will develop a program to educate students on these issues.

#### **Off-campus conduct**

Students, parents/legal guardians, teachers and staff members should be aware that the district may take disciplinary actions for conduct initiated and/or created off-campus involving the inappropriate use of the Internet or web-based resources if such conduct poses a threat or substantially interferes with or disrupts the work and discipline of the schools, including discipline for student harassment and bullying.

## **AR IJNDB-R Use of Technology Resources in Instruction**

Issued 8/18

Purpose: To establish the board's vision and governing rules for the use of technology in Anderson School District 3.

### **Internet Access**

Because technology is a vital part of the educational process and the curriculum of the district, students and staff will be provided access to the Internet. By providing this access, the district intends to promote educational excellence in schools by facilitating resource sharing, innovation, communication, and learning, by allowing access to resources unavailable through traditional means. Through the Internet, students and staff will have access to the following:

- locally networked reference and research sources
- global information and news
- discussion groups on a vast range of topics
- local, regional, public, state and national library catalogs; and world wide web

Additionally, staff will have full access to digital communication services to include electronic mail services. Students will have access to digital communication services to include electronic mail services within the district domain.

The availability of Internet access provides a unique educational opportunity for students and staff to contribute to the district's presence on the World Wide Web. This medium of communication provides an opportunity to share accurate information with the community, the state, and the world about the district's curriculum and instruction, school-authorized activities, and other related information. The district provides this instructional resource as an educational tool for staff and students and its use will be governed by the Responsible Use policy. The failure to follow these policies or responsibilities may result in the loss of privileges or other disciplinary measures.

With access to computers and people all over the world also comes the availability of material that may not be of educational value in the context of the school setting. The district has taken precautions to restrict access to controversial or inappropriate materials; however, on a global network it is impossible to control access to all materials and an industrious user may discover controversial information. The district firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of the district. The district will take measures to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

The smooth operation of the Internet network relies on the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided so that students and staff are aware of their responsibilities when using the Internet. Any violations of these guidelines will subject the user to appropriate disciplinary action and possible denial of access to the Internet. In general, this requires efficient, ethical, and legal utilization of the network resources.

Because access to the network provides connections to other computer systems located all over the world, users (and parents/legal guardians of students who are users) must understand that neither the district nor any district employee controls the content of the information available on the systems. Every effort will be made by the district to monitor and restrict ready access to known objectionable sites. However, the district does not condone the use of controversial or offensive materials and cannot be held responsible for such use.

### **Use of Personal Devices**

The district believes technology is a powerful tool to enhance learning for all students. As we work to prepare students for the 21st century, we must challenge students with increased rigor and personalized academic experiences integrating creativity, communication, collaboration, and critical thinking. Students will be required to use district issued devices when available due to the ability of the district to provide security and support to district owned devices. All students and staff using a personal device must follow all guidelines in this document while on school property, attending any school-sponsored activity, or on any district provided transportation.

Responsibility to keep the device secure rests with the individual owner. Anderson School District Three, its staff or employees, will not be liable for any device stolen, or damages to any device on campus.

- If a device is stolen or damaged, it will be handled through the administrative office similar to other personal items in such situations.
- Each student is responsible for his/her own personal device; set-up, maintenance, charging, and security.
- Personal devices are only to be used for educational purposes at the direction of a classroom teacher.
- Administrators and staff members have the right to prohibit use of devices at certain times or during designated activities that occur during the school day (guest speakers, campus presentations, or other performances).
- An administrator may examine a student's personal device and search its contents, in accordance with disciplinary guidelines.
- Personal devices may only be used on school provided transportation at the discretion of the driver. When using personal devices on school sponsored transportation, students must have only one earbud in ear and have the volume at a level that can only be heard by the user of the device.

### **Technology Protection Measures**

In compliance with the Children's Internet Protection Act ("CIPA"), [Pub. L. No. 106-554](#) & [47 U.S.C. § 254\(h\)](#), the district uses technological devices designed to filter and block the use of any of the district's computers with Internet access to retrieve or transmit any visual depictions that are obscene, child

pornography, or "harmful to minors" as defined in the CIPA. Adult users of a district computer with Internet access may request that the "technology protection measures" be temporarily disabled by the chief building administrator of the building in which the computer is located, for bona fide research purposes or other lawful purposes not otherwise inconsistent with this Acceptable Use Policy.

## **Internet Safety Policy**

For purposes of the Children's Internet Protection Act ("CIPA"), [Pub. L. No. 106-554](#) & [47 U.S.C. § 254\(I\)](#), this administrative rule is the district's "Internet safety policy." This rule includes provisions to address access by minors to inappropriate matter on the Internet and World Wide Web; the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; unauthorized access, including so-called "hacking" and other unlawful activities by minors online; unauthorized disclosure, use, and dissemination of personal identification information regarding minors; measures designed to restrict minors' access to materials harmful to minors, and provide for the education of minors about appropriate online behavior, including interacting with other individuals on social networking sites and chat rooms, and cyber bullying awareness and response.

Students and staff will receive instruction on the appropriate use of the Internet, including interacting with others on social networking sites, in chat rooms, cyber bullying awareness and response, and safety and security of users when using electronic mail and other forms of direct electronic communications. The superintendent or his/her designee will develop a program to educate students on these issues. In addition, internet permission forms are sent home with each student by way of the student packets where students and parents are informed to review policy [IJNDB](#) and administrative rule IJNDB-R which govern the use of technology in our district. This form also gives parents the ability to deny permission for their child to access the internet using district resources should they elect to sign and return the form indicating their decision. Employees are made aware of the need to review this same policy and administrative rule by way of an online safety and compliance system.

## **Terms and Condition of Use**

### **Responsible use**

The purpose of the district's educational network is to provide access to unique educational resources and the opportunity for collaborative work. All use of the Internet and network must be in support of this mission, and consistent with the educational objectives of the district. Use of other networks or computing resources must comply with the rules governing those networks. Transmission of any material in violation of any federal or state laws or regulations is prohibited; this includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secret. Access to computer systems and networks owned or operated by the district impose certain responsibilities and obligations on users and is subject to district policies and local, state, and federal laws.

Acceptable use is always ethical, reflects honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and the individual's rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance.

### **Procedures for use**

Administrators and teachers may access the Internet for educational or work-related purposes at any time, which is not disruptive and does not interfere with the performance of other responsibilities by the employee or other staff members. Occasional employee personal use is permitted.

Students may be allowed to access the Internet and receive digital communication services to include electronic mail services through their school resources and staff. Student use must be supervised at all times by a staff member.

### **Rules governing use**

The use of the Internet is a privilege, not a right, and inappropriate use will result in cancellation of Internet privileges and will be subject to disciplinary consequences described in this policy. All staff and students must abide by the generally accepted rules of network etiquette, including the following:

Vandalism is prohibited and will result in disciplinary and/or legal action. Vandalism includes any malicious attempt to harm or destroy data of another user, Internet, or other networks that are connected to any of the Internet infrastructures. Vandalism also includes, but is not limited to, the uploading or creation of computer viruses, deletion or alteration of other user files or applications, removing protection from restricted areas, or the unauthorized blocking of access to information, applications, or areas of the network.

Never access or attempt to access inappropriate or restricted information, such as pornography or other obscene materials, or other information not directly related to the educational purposes for which access is being provided. Restricted information includes obscene, libelous, indecent, vulgar, profane, or lewd materials, advertisements for products or services not permitted to minors by law, insulting, fighting, and harassing words, and other materials which may cause a substantial disruption of the academic environment. Violations of this policy will result in disciplinary and/or legal action.

- Be polite. Do not be abusive in messages to others. Always use appropriate language.
- Profanity, vulgarities, or other inappropriate language is prohibited. Illegal activities are strictly forbidden.
- Documents, electronic mail, chat room messages, and any other form of direct communications may not include a student's social security number or any other personally identifiable information that may lead to the identity of one's self or others.
- No student pictures (video or still) or audio clips will be published without permission from the student's parent or guardian.
- Documents may include "directory information," including a student's name, address, or telephone number, provided the parent/legal guardian has been informed about the release of "directory information" and has not notified the district in writing that he/she objects to the release of information.
- Electronic mail is not guaranteed to be private. People who operate the system have access to all electronic mail. Messages relating to or in support of illegal or inappropriate activities will be reported to the appropriate authorities.
- Do not disrupt, harass, or annoy other users.
- All communications and information accessible via the network should not be assumed to be private property. Always cite all quotes, references, and sources.

- All subject matter on district web pages will relate to curriculum, instruction, school-authorized activities, or to the district.
- Neither students nor staff may publish personal home pages as part of district web sites, or home pages for other individuals or organizations not directly affiliated with the district.
- All users should use the Internet only for research and academic reasons; non-academic uses are prohibited. Occasional employee personal use is permitted. Users may not use the system for financial or commercial gain unless doing so is in direct relation to educational opportunities or state standards.
- All pages on the district's server(s) are property of the school district.
- Always follow the instructions of the supervising staff members.
- Passwords are not to be used by unauthorized individuals. Individuals given passwords to access the district's systems will assume responsibility for proper use and safe keeping of those passwords. If a staff member feels that there is a security problem on the network, misuse of a district password, or a compromised password the matter should be reported to the building principal or the designated local school technology resource.
- No user of the system may use the system to make an unauthorized disclosure or use of, or otherwise disseminate, personal identification information regarding minors and/or students.

### **Inappropriate uses**

The following list represents some of the inappropriate uses that are not permitted by the district:

- commercial advertising, commercial fundraising, or unethical/illegal solicitation
- accessing a file or web site that contains pornographic or obscene pictures, videos, stories, or other material, making copies of such material, or distributing or exposing others to such material
- using copyrighted material without permission
- Sending messages or materials that are obscene, profane, racist, sexist, inflammatory, threatening, or slanderous toward others
- creating and/or placing a computer virus on the network or any workstation
- sending messages or information misrepresenting the source of information entered or sent
- sending or receiving messages or information that is inconsistent with the school's conduct code or assisting others to violate that code
- requesting or distributing addresses, home phone numbers, or other personal information, which could then be used to make inappropriate calls or contacts
- sending chain letters or engaging in "spamming" (sending an annoying or unnecessary message to large numbers of people)
- using material that is potentially disruptive to the learning environment
- accessing, attempting to access, and/or altering information in restricted areas of any network
- downloading or loading any software or applications without permission from the building network administrator or system administrator
- violating the confidentiality rights of other users on any network
- failing to report abuses or other conditions that may interfere with the appropriate and efficient use of school resources

Users are required to report any violations of this policy to his/her teacher or the building administrator as soon as they are discovered.

### **Penalties for improper use**

An employee who violates the terms of this administrative rule or otherwise misuses the Internet to access inappropriate material will be subject to disciplinary action, up to and including discharge. In addition, the privilege of accessing the Internet will be subject to cancellation. Students who violate the terms of this administrative rule or who otherwise misuse their access to the Internet also will be subject to disciplinary action in accordance with the applicable student related policies. Internet access privileges also may be cancelled. Violations of the laws of the United States or the state of South Carolina also may subject the user to criminal prosecution. If a user incurs unauthorized costs, the user, as well as the user's parents/legal guardian if the user is a student, will be responsible for all such costs.

### **Warranty**

The district makes no warranties of any kind, whether expressed or implied, for the service it is providing. The district will not be responsible for any damages suffered by any user. This includes loss of data resulting from delays, non-deliveries, misdirected deliveries, or service interruptions caused by the system's negligence, user errors, or omissions. Use of any information obtained via the Internet is at the user's own risk. The district specifically denies any responsibility for the accuracy or quality of information obtained through its services.

### **Security**

Security on any computer system is a high priority, especially when the system involves many users. If you feel you have identified a security problem on the network, you must notify the administrator for the school or the district director of technology. Do not demonstrate the problem to other users. Attempts to log on to any network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be subject to severe restriction or cancellation of privileges or other disciplinary and/or legal action.

### **User privacy**

The district reserves the right to examine, restrict, or remove any material that is on or passes through its network, just as it does any other work or material generated or brought to school by staff or students. Access to electronic information related to any student or staff member will be governed by the same policies that would apply to that information if it were not in electronic form.

### **School Board Policies**

All documents on the district's server(s) must conform to school board policies and regulations, as well as established school guidelines. Copies of board policies are available in all school offices and on the district and school websites. Persons developing or maintaining web documents are responsible for complying with these and other policies. Some of the relevant issues and related board policies include the following:

- Electronic transmission of materials is a form of copying. As specified in district policy, no unlawful copies of copyrighted materials may be knowingly produced or transmitted via the district's equipment, including its web server(s).
- Documents created for the web and linked to district web pages will meet the criteria for use as an instructional resource.
- Any links to district web pages that are not specifically curriculum-related will meet the criteria established in the district's Internet related policies. Any other non-curricular materials should be limited to information about other youth activities, agencies, or organizations which are known to be non-sectarian, exclusively devoted to community interests or child welfare, non-profit, and non-discriminatory. Web page links may not include entities whose primary purpose is commercial or political advertising.
- All communications via district web pages will comply with the district Technology Resources policy, Internet Acceptable Use & Safety policy, and the applicable student behavior policies. Offensive behavior that is expressly prohibited by this policy includes religious, racial, and sexual harassment, and/or violence.
- Any student information communicated via District web pages will comply with District policies on Data Privacy and Public Use of School Records.

## **Other**

Material on web pages reflects an individual's thoughts, interests, and activities. Such web pages do not, in any way, represent individual schools or the district, nor are they endorsed or sanctioned by any individual school or the district. Concern about the content of any page(s) created by students or staff should be directed to the building principal of that school.

Given the rapid change in technology, some of the technical standards outlined in this policy may require change throughout the year. Such changes will be made with approval of the superintendent and the school board.

## **Google Consent**

To parents and guardians,

At Anderson School District 3, we use Google Workspace for Education, and we are seeking your permission to provide and manage a Google Workspace for Education account for your child. Google Workspace for Education is a set of education productivity tools from Google including Gmail, Calendar, Docs, Classroom, and more used by tens of millions of students and teachers around the world. At Anderson School District 3, students will use their Google Workspace for Education accounts to complete assignments, communicate with their teachers, sign into their Chromebooks, and learn 21st century digital citizenship skills.

The notice below provides answers to common questions about what Google can and can't do with your child's personal information, including:

What personal information does Google collect?

How does Google use this information?

Will Google disclose my child's personal information?

Does Google use student personal information for users in K-12 schools to target advertising?

Can my child share information with others using the Google Workspace for Education account?

Please read it carefully, let us know of any questions, and then sign below to indicate that you've read the notice and give your consent. If you don't provide your consent, we will not create a Google Workspace for Education account for your child. Not signing will prohibit your student from using a Chromebook or having access to an acsd3.org account, or Google Classroom lessons that their teacher assigns. I give permission for Anderson School District 3 to create/maintain a Google Workspace for Education account for my child and for Google to collect, use, and disclose information about my child only for the purposes described in the notice below.

Thank you,

Aimee Gray, IT Director

### **Google Workspace for Education Notice to Parents and Guardians**

This notice describes the personal information we provide to Google for these accounts and how Google collects, uses, and discloses personal information from students in connection with these accounts.

Using their Google Workspace for Education accounts, students may access and use the following "Core Services" offered by Google (described at [https://workspace.google.com/terms/user\\_features.html](https://workspace.google.com/terms/user_features.html)):

- Gmail
- Currents
- Calendar
- Chrome Sync
- Classroom
- Cloud Search
- Contacts
- Docs, Sheets, Slides, Forms
- Drive
- Groups
- Google Meet
- Jamboard
- Keep
- Sites
- Vault

In addition, we also allow students to access certain other Google services with their Google Workspace for Education accounts. Specifically, your child may have access to the following "Additional Services":

Applied Digital Skills  
Blogger  
Chrome Web Store  
CS First  
Developer Platform  
FeedBurner  
Google Alerts  
Google Bookmarks  
Google Books  
Google Cloud Platform  
Google Cloud Print  
Google Data Studio  
Google Earth  
Google Groups  
Google Maps  
Google My Maps  
Google Photos  
Google Play  
Google Play Console  
Google Public Data  
Google Search Console  
Google Takeout  
Managed Google Play  
Material Gallery  
Scholar Profiles  
Third-Party App Backups  
Tour Creator  
YouTube

Google provides information about the information it collects, as well as how it uses and discloses the information it collects from Google Workspace for Education accounts in its Google Workspace for Education Privacy Notice. You can read that notice online at [https://workspace.google.com/terms/education\\_privacy.html](https://workspace.google.com/terms/education_privacy.html) You should review this information in its entirety.

### **Student/Parent/Legal Guardian Certification Form**

As the parent/legal guardian of this student, I have read and understand the Internet acceptable use policy, administrative rule, and Google Privacy Consent. I understand that this access is designed solely for educational purposes. I further understand that if my child violates these conditions and rules, his/her access privilege may be revoked for up to one year and disciplinary action may be taken.

\_\_\_\_\_ (Date)  
(Parent/Legal guardian)

As the parent/legal guardian of this student, I have read and understand the Internet acceptable use policy, administrative rule, and Google Privacy Consent. I understand and will abide by the conditions and rules set forth therein. I further understand that violations of these conditions and rules are unethical and also may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked for up to one year, disciplinary action may be taken and appropriate legal action also may be instituted.

\_\_\_\_\_ (Date)  
(Student)