

Southside School District Acceptable Use of Technology and Internet Safety Policy 2012 - 2015

The Southside School District is responsible for securing its network and computer systems against unauthorized access and/or abuse, while making the technology available for authorized users. This responsibility includes informing users of expected standards of conduct and the punitive measures for not adhering to this policy.

The Technology Committee of Southside School has developed the following policy for the student body and faculty/staff covering the use of a computer and/or computer network. Any person using a computer and/or computer network is covered by this policy while on the school campus or when accessing the school's system from a computer outside the physical boundaries of the school.

All users of computer/computer networks (including the Internet) at Southside School will receive the following policy and complete the attached application and contract agreement before being granted access to the system. No student will be granted Internet access until a computer-use agreement is signed by both the student and parent or legal guardian (if the student is under the age of eighteen).

Southside School District endeavors to protect the safety and security of students when navigating the Internet. Southside School District continuously works to educate all students about appropriate online behavior, including but not limited to contact with individuals on social networking websites and cyber bullying awareness and response.

Educational Purposes

1. This network has been established for educational and administrative purposes only. Southside School District uses a state provided Internet filtering system which filters each computer on campus from access to materials harmful to minors.
2. Use of the computer is a privilege, not a right, and misuse of the computer or computer network will result in temporary/permanent revocation of this privilege.
3. All computers are in teacher-supervised areas, including classrooms, media centers and computer labs. The computers/network will be used for the pursuit of intellectual activities, to seek educational resources, access libraries and communicate through e-mail. The school's network shall be used only for approved education purposes. An adult will be in the room at all times when students are using computer equipment. The adult will monitor student

computer use and will take appropriate action if misuse is detected. District personnel will also monitor all non-student computer activity.

4. It is the user's responsibility not to initiate access to inappropriate material on the Internet. Network administrators reserve the right to regulate access to Internet materials.

Internet/Network Access

1. All Southside School students will have access to the network and Internet resources through their classroom, media center and/or school computer lab.
2. Students bringing personal computers, e-readers, tablets, or other wireless devices must access the filtered school network. No external storage devices including USB or flash drives may access the school network. No student may bring any CD, DVD or USB drive from home for personal use. Prior permission must be obtained for school use.

Personal Safety

1. Students will protect their personal safety while using the Internet.
2. Students will not post personal contact information about themselves or other people. Personal contact information includes your name, school address, work address, home address, social security number, telephone number, credit card numbers, etc.
3. Students may not visit social networking sites, unless authorized by the instructor for a class activity directly supervised by a staff member. Further, the posting of any private or confidential school district material on such websites is strictly prohibited.
4. Students should promptly disclose to a teacher or other adult any message received that is inappropriate or threatening.

Unacceptable Uses of Network

1. The computer shall not be used to harm people in any manner. The approved School Board Policy on bullying, electronic bullying, and harassment will be followed. Southside School District educates minors about appropriate online behavior, including interacting with other individuals on social networking websites, in chat rooms, cyberbullying awareness and response.
2. All computers and computer work shall be free from interference by others.
3. Computers/computer networks shall not be abused or harmed in any way.
4. The technology shall not be used in any immoral or unethical manner.
5. The school network may not be used for commercial purposes. You may not offer, provide or purchase products or services through this network.
6. Users of the network will not engage in any illegal act, such as arranging for a drug sale, the purchase of alcohol, criminal gang activity, etc.
7. Students will not be allowed to post web pages on the school's network. No commercial links will be placed on the school website
8. Deletion, examination, copying or modification of files and/or data belonging to others is prohibited without their consent.
9. Software may not be copied unless it is legal to do so.

10. Access to programs, computer games, or the Internet without authorization from a teacher is prohibited.
11. Any unauthorized, deliberate action, which damages or disrupts a computer, a network, or related hardware and software, alters the normal performance of said equipment, or causes it to malfunction is a violation of this policy regardless of system location or time duration.
12. Students may not visit nor download materials from any site, which contains offensive or immoral pictures, language, or any other material inappropriate for an educational setting. The school, either by itself or in combination with the provider of Internet access, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors.

Sharing a User ID/password with any other person is prohibited. In the event that a person does share his/her User ID/password with another person, both parties will be disciplined and the owner of the ID/password will be held responsible for the actions of the user. The district follows the State Security Office K-12 Student Password Management Standards. All student passwords must be at least 8 characters in length and contain both alpha and non-alpha characters. Student passwords are changed each semester or as needed.

Security on any computer system is high priority. If a security problem is detected, the system administrator must be notified immediately. Do not attempt to use another individual's account. Attempts to log in to the system as another user will result in cancellation of all computer privileges. Any user identified by the system administrator as a security risk or as having a history of problems with computer/computer systems may be denied use privileges.

Security Systems

The following rules shall apply to the security of the system:

1. Decoding or attempting to decode system or user passwords is prohibited.
2. The copying of systems files is prohibited.
3. The copying of copyrighted materials, such as third party software without the express written permission of the owner or without the proper license, is prohibited.
4. Intentional attempts to "crash", "hack into", or invade or damage network system or programs are prohibited.
5. Attempts to secure a higher level of privilege on network system are prohibited.
6. The willful introduction of computer "viruses" or other disruptive/destructive programs into the Southside networks or external network is prohibited.

Network/Technology activities will not lead to intimidation, embarrassment, or harassment.

1. Forgery (or attempted forgery) of e-mail is prohibited.
2. Attempts to read, delete, copy or modify the e-mail of other users are prohibited.

3. Attempts at sending unsolicited junk mail, “for-profit” messages, or chain letters are prohibited. “Spamming” is prohibited. Spamming is the unsolicited sending of bulk or commercial messages over the Internet.
4. No profane, offensive, abusive or otherwise objectionable language shall be entered in to the computer.
5. Users will not use any method to bypass the school’s selected filtering process.
6. Students may not visit nor download materials from any site, which contains offensive or immoral pictures, language, or any other materials inappropriate for an educational setting. Any type of “chat room” or other form of direct electronic communications (including messengers) is prohibited. Neither shall you access material that advocates illegal acts, violence or discrimination towards other people.

Definition of the penalty for inappropriate computer/network/technology usage:

- A. First Offense – One week suspension from Internet use at school plus any other action as deemed necessary by the school principal. Student will be responsible for all assigned computer work while suspended.
- B. Second Offense – Two weeks suspension from Internet use at school plus any other action as deemed necessary by the school principal. A parent-principal conference will be conducted to emphasize that future offenses will result in suspension for the remainder of the semester. The student will do his/her computer assignments outside of school or he/she will receive no credit.
- C. Third Offense – Suspension for the remainder of the semester from computer use at school, plus any other action as deemed necessary by the school principal. Student will be responsible for all assigned computer work while suspended.
- D. SEVERE CLAUSE: The principal has the discretion to bypass any level of offense and invoke a higher level of penalty.

Network and Internet access is provided as a tool for education, The school district reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the Southside School District and no user shall have any expectation of privacy regarding such materials. Any student or user under the age of 18 agrees to make this policy known to his/her parents and to obtain their written approval in order to use the Southside computers/network. Students and their cosigners shall be liable for any and all cost incurred through the student’s use of the computers or the Internet including penalties for copyright violations.

The school district makes no warranties of any kind, either expressed or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this policy. The school will not be responsible for any claim, losses, damages or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user's use of its computer networks or the Internet under this policy. By signing this policy, users are taking full responsibility for computer use, and the user who is 18 or older or, in the case of a user under 18, the parent(s) or guardian(s) are agreeing to indemnify and hold the school, the school district, the data acquisition site that provides the computer and Internet access opportunity to the school district and of their administrators, teachers, and staff harmless from any and all loss, costs, claims or damages resulting from the user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s) or guardian(s) agree to cooperate with school in the event of the school's initiating an investigation of a user's use of his or her access to its computer network and the Internet, whether that use is on a school computer or on another computer outside the school district's network.

This policy will be periodically reviewed/revised as deemed necessary by the Southside School District Technology Committee.

Acceptable Use of Technology and Internet Safety Policy

STUDENT'S AGREEMENT

Every student, regardless of age, must read and sign below:

User Contract

I have received the Acceptable Use of Technology and Internet Safety Policy of the Southside School District. I wish to be assigned a log in name and a password. These will grant me the privilege of using the computer/network at Southside School. I agree to abide by the rules and regulations of the Southside Acceptable Use of Technology and Internet Safety Policy.

I understand that certified staff or system administrator may periodically monitor activity on my account. I understand that I must follow Southside School District's Acceptable Use of Technology and Internet Safety Policy. I also understand that I am subject to penalties of all state and federal laws governing the use of computers, software, copyrights, etc. Violations may result in loss of computer privileges/access, removal of my account from the computer network, suspensions and/or additional disciplinary actions. Suspensions or actions will not cancel my responsibilities in the computer classes in which I am enrolled. I will be accountable for all assignments.

Student Name (PRINT CLEARLY)

Student signature

Address

Home Phone

Date

For all applicants less than 18 years of age, the signature of a parent/guardian is required

Acceptable Use of Technology and Internet Safety Policy

PARENT/GUARDIAN AGREEMENT

Student's Name _____

As the parent or guardian of the above named student, I have received the Southside Acceptable Use of Technology and Internet Safety Policy and the user contract. I understand that computer usage is designed for educational purposes and that the Southside School District has taken available precautions to eliminate controversial material. However, I also recognize that restricting access to all offensive and controversial materials is impossible for the school district and understand my child's responsibility for abiding by the policy. I will not hold the school or its employees responsible for material found on the network. Further, I accept full responsibility for my child's use of the computer/network at school under this policy. I hereby give my permission to issue an account for my child.

Parent/Guardian (please print): _____

Signature: _____

Daytime Telephone: _____ Evening Telephone: _____

Adopted:

Revised:

Legal References:

Children's Internet Protection Act of 2000 (H.R. 4577, P.L. 106-554)
Communications Act of 1934, as amended (47 U.S.C.254 [h],[l])
Elementary and Secondary Education Act of 1965, as amended (20 U.S.C. 6801 et seq., Part F)

Acceptable Use of Technology and Internet Safety Policy

APPLICATION AND CONTRACT AGREEMENT
INTERNET ACCOUNT/COMPUTER ACCESS

Last Name: _____ First Name: _____

Home Address: _____ Home Phone: _____

I am a (check one): _____ Teacher _____ Paraprofessional
 _____ Media Specialist _____ Support Staff
 _____ Administrator

After receiving the Acceptable Use of Technology and Internet Safety Policy of the Southside School District, please read and fill out the appropriate portions of the following contract. Please return the contract to the Principal's or Superintendent's Office.

User Contract

I have received the Acceptable Use of Technology and Internet Safety Policy of the Southside School District. I understand and agree to abide by the stated terms and conditions set forth in this document. I further understand that violations of the regulations are unethical and may constitute a criminal offense. Should I commit a violation, my access privileges may be revoked, school disciplinary and/or appropriate legal action may be taken.

The district follows the State Security Office K-12 Faculty/Staff Password Management Standards. All staff passwords must be at least 8 characters in length and contain both alpha and non-alpha characters. Passwords for staff are changed every 90 days or as needed. It is extremely important that teachers NEVER share their passwords with students. To protect the security of your own and other's files, please NEVER share your password with anyone and always log out when you leave your computer. Do not allow a student to use the computer with your login name and password.

User Name (please print): _____

User Signature: _____ Date: _____