SHERIDAN COMMUNITY SCHOOLS
STUDENT COMPUTING AND INTERNET USE AGREEMENT

Please review this form and the attached Sheridan Community Schools (SCS) Student Computing Policy with your child. Both student and parent signatures are required. A signed form is required at each building level (once at Elementary, once at Middle School and once at High School) or if a student leaves SCS and returns at a later time. Please also remember to check the appropriate box below indicating whether or not you give Internet access permission. Please feel free to direct any questions to the SCS District Technology Director, Lea Jessup at (317) 758-4431.

STUDENT COMPUTING AND INTERNET USE AGREEMENT

I have read and agree to abide by the Student Technology Acceptable Use and Safety Policy and Guidelines. I understand that any violation of the terms and conditions set forth in the Policy and Guideline is inappropriate and may constitute a criminal offense. As a user of the Corporation's Technology Resources, I agree to communicate over the Internet and the Technology Resources in an appropriate manner, honoring all relevant laws, restrictions and guidelines.

Student User Name (please print)_____

Student User Signature_____

Student Grade:_____   Date_____

PARENT OR GUARDIAN INTERNET PERMISSION AGREEMENT

As the parent/guardian of this student, I have read the Student Technology Acceptable Use and safety policy and guidelines, and have discussed them with my child. I understand that student access to the Internet is designed for educational purposed and that the Corporation has taken available precautions to restrict and/or control student access to material on the Internet that is obscene, objectionable, inappropriate and /or harmful to minors. However, I recognize that it is impossible for the Corporation to restrict access to all objectionable and/or controversial materials that may be found on the Internet. I will not hold the Corporation (or any of its employees, administrators, or officers) responsible for materials my child may acquire or come in contact with while on the Internet. Additionally, I accept responsibility for communicating to my child guidance concerning his/her acceptable use of the Internet, i.e. setting and conveying standards for my child to follow when selecting, sharing and exploring information and resources on the Internet. I further understand that individuals and families may be liable for violations. I give permission for my child to use and access the Internet at school and for the Corporation to issue an e-mail account to my child.

Parent/Guardian Signature_____Date_____

POLICY

Sheridan Community Schools
STUDENT - COMPUTING POLICY

I.   **PURPOSE**

       A.   Computing Facilities/Equipment at Sheridan Community Schools (SCS) are provided for instructional and administrative use to help the district more effectively fulfill its educational mission. The following policies are provided in order to assure that the district's significant investment in computing is used in accordance with this purpose.

II.   **AUTHORIZED USERS**

       A.   District computers, whether single systems, networks, or lab systems, are provided for the use of SCS students, faculty, staff, and administrators.

III.   **COMPUTER ACCOUNTS**

       A.   Computer accounts and the files on them are the exclusive property of the district and not the user's private property. Accounts are assigned for school-related work. If there is reasonable suspicion of illegal or unethical activities, the district reserves the right to inspect its property. It is important to remember that the computer is not a secure environment for private material.

       B.   SCS Technology staff will provide accounts and activate them for authorized users based on input from school offices.

       C.   Users should keep their passwords confidential. Giving your password to another student is in direct violation of acceptable use, and disciplinary action will be taken. Users may change their passwords frequently and should avoid using their names, friends' names, or a password that could easily be guessed.

       D.   All student computer usage is to be supervised by a SCS staff member. No students should access a computer in an unsupervised classroom or instructional area.

       E.   Use of a SCS computing account by anyone other than the owner to whom the account has been assigned is prohibited.

       F.   In addition to other sanctions, access to a computer account may be revoked for a violation of security provisions, unlawful activity, or violation of SCS Board policy. Violators are subject to applicable disciplinary procedures.

IV.   UNAUTHORIZED USES

A.   General Policies

1.   Use of a computer in violation of SCS Board policy is prohibited.

2.   No person shall knowingly gain access to, or attempt to gain access to, any computer, computer system, computer network, information storage media, or peripheral equipment for which they have no legitimate need, without the consent of a SCS teacher or technology staff member.

3.   Use of a computer account or computer to access resources and facilities is limited to bona fide instructional purposes. Using a computer account for non-educational computerized entertainment, games and multi-user chat, message boards or email facilities is not allowed.

4.   No person shall knowingly alter, delete, or destroy data, information, or programmatic instructions contained on or in a computer, computer system, computer network, information storage media, or peripheral equipment, without permission from authorized personnel from the SCS Technology department. This does not apply to personally generated files and documents that can be deleted by the user who created them.

5.   No person shall knowingly introduce a set of instructions, programmatic or otherwise, into a computer, computer system, computer network, information storage media, or peripheral equipment, without permission from authorized personnel from the SCS Technology department.

(Examples of 4 and 5 include, but are not limited to, batch files, computer "viruses," "Trojan horses," "time bombs," "logic bombs," and "worms.")

6.   No person shall add, delete, or modify the default setup on school computers or files on the file server without permission from authorized personnel from the SCS Technology department. This includes changing screen savers, enabling file sharing capabilities, or installing personal software on hard drives or network drives. Computers will be periodically checked, and anything not authorized will be deleted.

7.   Attempting to circumvent SCS computer security systems, or using SCS computer systems or computer networks in attempting to circumvent security systems elsewhere is prohibited.

8.   No person shall use a computer to eavesdrop on another user or to collect passwords or other authentication information.

9. No person shall use a computer anonymously or use pseudonyms to attempt to escape from prosecution of laws or regulations, or otherwise to escape responsibility for their actions.

10. Wasteful or extravagant use of SCS computer resources is prohibited. Such wasteful or extravagant use can be illustrated by, but is not limited to, any printing of posters and banners for personal parties and events, printing multiple copies of documents, and making multiple copies of handouts and papers.

11. It is inappropriate to use SCS computer resources for financial gain.

B. Software Issues

1. Sheridan Community Schools respects the intellectual property rights of others. When the district enters into software license agreements, it is the district policy that we will comply with their terms and conditions, including restrictions on copying and use. Copyright laws must be respected at SCS. Failure to comply with a software license agreement can result in our losing the use of the software and legal action.

   a) Computer software or data may not be copied or used in violation of the software manufacturer's license agreement or copyright provisions.

   b) Unless specifically allowed by its owner and copyright, proprietary software must not be placed into public locations. Such locations include, but are not limited to, file servers, non-private computer files or folders, and computer bulletin boards.

2. No unauthorized person shall provide computer software or data containing passwords to another person.

3. SCS Technology Department staff or their designated agents are the only individuals authorized to load software on district owned computer equipment.

V. **PHYSICAL PROPERTY ISSUES**

A. SCS computing equipment may not be moved by a student to another office, lab, or elsewhere on or off campus without the authorization of the building technology coordinator.

B. No student or unauthorized person shall knowingly connect, disconnect, tamper with, or make changes to any physical components of SCS computing equipment. This includes removing keyboards, peripherals, cords, or any physical part of a computer.

VI.   DATA FILE STORAGE

   A.   Students are allocated personal storage of school-related documents on a cloud storage drive (Google Drive).

   B.   Access to other network drives other than a user's personal folder is strictly prohibited, whether viewable or accessible.

   C.   Files stored on individual workstation hard drives are not secure. Anyone who turns on a workstation can access files stored on local hard drives. Because of this, storing files on local hard drives is discouraged. Files stored in the user's folder on the fileserver are secure because a user ID and password are required to access the folder. Saving all files to the fileserver is the most secure method of data storage.

   D.   In the event of a workstation failure due to a hardware malfunction or software corruption, it may be necessary to re-configure the workstation. Re-configuring the workstation returns the workstation to its original state. This means that any documents or files on the computer's hard drive are lost. This is the most efficient method to correct major computer problems; however, it does result in the loss of all stored documents. This is another reason to store all documents and data in the user folder on the fileserver.

VII.   E-MAIL USAGE

   A.   SCS issues each student an educational e-mail account which is subject to review and restrictions as deemed appropriate by SCS administration and Technology staff. This e-mail account is for the sole use of the student's educational purposes. Students should keep their account credentials secured and not share that information with others.

VIII.   INTERNET ACCEPTABLE USE

   A. Sheridan Community Schools is pleased to offer its faculty, staff, and students access to the Internet. The Internet is an electronic highway connecting hundreds of thousands of computers and millions of individual users all over the world. This computer technology will help propel our schools through the communication age by allowing students and staff to access and use resources from distant computers, communicate and collaborate with other individuals and groups around the world, and significantly expand their available information base.

   a. While the district's intent is to make Internet access available in order to further educational goals and objectives, it is possible to access other materials as well. All users should be aware that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate, or potentially offensive to some people. SCS institutes technical methods or systems to regulate Internet access,

however, those methods can not guarantee compliance with the district's acceptable use policy. That notwithstanding, the district believes that the benefits to users exceed any disadvantages.

b. The primary purpose of district-provided Internet access is to facilitate communications in support of research and education. To remain eligible as users, use must be in support of and consistent with the educational objectives of Sheridan Community Schools. Access is a privilege, not a right. Access entails responsibility.

c. Users should not expect that files stored on school-based computers will always be private. SCS reserves the right to monitor and audit all internal and external usage. Administrators may spot-check files and network traffic to maintain the performance/reliability of the network and insure that users are acting responsibly. Students are responsible for good behavior on-line just as they are in a classroom or other area of school.

d. The following uses of school-provided Internet access are not permitted:

i. to access, upload, download, or distribute illegal, vulgar, abusive, pornographic, obscene, or sexually explicit material,

ii. to transmit vulgar, obscene, abusive, or sexually explicit language,

iii. to violate any local, state, or federal statute,

iv. to vandalize, damage, or disable the property of another individual or organization,

v. to access another individual's materials, information, or files without permission,

vi. to download software without the permission of building technology staff (this includes screen savers, shareware, and any other programmatic data file),

vii. to violate copyright, plagiarize or otherwise use the intellectual property of another individual or organization without permission,

viii. to reveal information about yourself, such as your personal address, phone number, or those of others,

ix. to purchase or sell goods and services.

e. The following uses of school-provided Internet access are permitted:

i. using the Internet in support of education or school appropriate research.

f. Any violation of district policy and rules may result in loss of district-provided access to its computer services. When and where applicable, law enforcement agencies may be involved.

g. Sheridan Community Schools makes no warranties of any kind, neither expressed nor implied, for the Internet access it is providing. The district will not be responsible for any damages users suffer, including, but not limited to, loss of data resulting from delays or interruptions in service. The district will not be responsible for the accuracy, nature, or quality of information stored on district diskettes, hard drives, or servers; nor for the accuracy, nature, or quality of information gathered through district-provided Internet access. The district will not be responsible for personal property used to access district computers or networks or for district-provided Internet access. The district will not be responsible for unauthorized financial obligations resulting from district-provided access to the Internet.

Care of Equipment – The student will exercise all due and reasonable care in handling the use of the device and associated peripherals and agrees to return the equipment in good condition at the end of each school year. SCS accepts and acknowledges reasonable and normal wear and tear of the device over the course of its useful life.

Terms of Use of Equipment – Your right to possession and use of the property terminates no later than the last day of the school year unless terminated by the District or upon withdrawal from the District.

Assistance with Equipment Issues – If you are experiencing problems with your device, technicians will be on staff to assist you. Please report a problem with your device to: SES-your teacher; SMS-Media Center; SHS-Media Center.

I understand that if the device and/or charger are lost or stolen, I will be responsible for reimbursing the school corporation as outlined below:

Lost\Stolen\Damaged Device:
Student is responsible for the replacement cost of the device and bag to be determined at the time of incident.

Parts Replacement\Repair:

Broken Screen	Mother Board	Keyboard	Power Adapter	Misc. Parts
$50	**$150**	**$25**	**$35**	**Repair cost of particular part**

Carrying Case Replacement - $30.00
Total Chromebook Replacement - $300

* School administrators are responsible for determining if the damage is accidental or intentional. * Repair costs are subject to change

Any violation of District policy and rules may result in loss of school-provided device and/or access to the Internet. Additional disciplinary action may be determined at the building level in keeping with existing procedures and practices regarding inappropriate language or behavior. When and where applicable, law enforcement agencies may be involved.

SCS makes no warranties of any kind; either expressed or implied for the Internet access provided. SCS will not be responsible for accuracy, nature, or quality of information gathered through school-provided access to the Internet.