South Spencer County School Corporation

Student Technology Acceptable Use Policy

Introduction

South Spencer offers students access to electronic information, Internet and email. With access to the Internet and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. SS has taken reasonable precautions to restrict access to inappropriate materials, which do not serve a legitimate educational purpose. However, on a global network it is impossible to control all materials and an industrious user may discover controversial information. The Board 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 this technology

Students are responsible for appropriate behavior when using the Internet, just as they are in classrooms and hallways. Therefore, general school rules and the guidelines for behavior set forth in the student handbook apply. The acceptable use guidelines for the Internet are set forth below. Noncompliance with these guidelines or the use of the Internet to violate any school rules or rules set forth in the student handbook shall result in disciplinary action, up to and including, suspension and expulsion.

No Privacy Guarantee

School district personnel have the right to access information stored in any user directory, on the current user screen, or in electronic mail. They may review files and communications to maintain system integrity and ensure that individuals are using the system in accordance with District policies and guidelines. Students should not expect files stored on District servers or through District provided or sponsored technology services to be private. By accepting these terms and conditions, students waive any right to privacy or confidentiality to material that was created, sent, accessed, or stored using a District computer or a District-provided network account.

Student Responsibilities for Internet/Network Use

1. Students will have access to the resources of the Internet/Network provided they comply with the rules and restrictions established by this policy and any policy, procedure, regulation, or other rule established by the District.

2. Each student and student's parent or guardian must annually sign the student handbook and/or the Student Technology Acceptable Use Policy acknowledging receipt and acceptance of the terms of this policy.

3. Students are responsible for their own behavior when using the Internet, consistent with the educational purpose outlined in this policy.

4. Students, parents/guardians, and employees of the District are jointly responsible for ensuring the educational value of the information and resources which are accessed, stored, and published.

<u>As a condition of my right to use the Internet/Network, I understand and agree to the following:</u>

1. I will use computing resources lawfully and respectfully.

- I will not use the Internet to create, distribute, access, or obtain information that:
  - Is harmful or prejudicial to others; for example, materials which are defamatory or libelous (knowingly writing something that is untrue about another person which causes that person harm),
  - Is pornographic, obscene, or sexually explicit;
  - Constitutes bullying (including cyberbullying) or harassment or otherwise fosters disruptiveness among the students so as to interfere with the learning environment of the school district;
  - Threatens immediate harm to the welfare of the school community or to any individual;
  - Discriminates against any segment of the student body or interferes with another's individual rights;
  - Encourages or abets unlawful activity.
- I will not use the Internet for illegal activity, including the violation of copyright laws.
- I will not use the Internet to intentionally cause damage to hardware, software, or data.
- I will not use the Internet to create or share computer viruses.
- I will not use the Internet to gain or attempt to gain access to restricted material or systems.
- I will not use the Internet for gambling.
- I will not use the Internet for commercial activities, product promotion, or political lobbying.
- I will not bypass the District's security controls or web filter.
- I will not use the Internet to maliciously attempt to harm or destroy the data of another user.
- I will not use the Internet to disrupt the efficient operation and/or educational programs of SS.
- I will not use the Internet to otherwise violate school rules, the student handbook, or District policies.

2. **I will use computing resources safely and responsibly.**
    - I will not share access to my login account or use another person's account.
    - I will not share my password.
    - I will not give out my name, picture, address, email, or any personally identifying information online.
    - I will not clear my web-browser history because I understand that school employees will view the Internet history to ensure that I am not violating this user agreement or any other District or school rule by my use of the computer.
    - While at school:
        - I will use the Internet and other computer resources for academic activities only; unless otherwise instructed by school personnel.
        - I will only play educational games authorized by school personnel;
        - I will not download games, applications, software, or music unless instructed by my teacher.
        - I will follow the guidelines for printing set by my school.
        - I will only access chat rooms, bulletin boards, blogs, or post to an Internet site when given permission by school personnel.
        - I will not use multi-user games unless instructed by my teacher.

3. **I will use computing resources in a manner that respects the intellectual property of others.**
    - I will not install, store, or distribute unauthorized copyrighted software or materials.
    - I will submit work that I have created myself or that I have created as part of a group project. If I borrow or copy materials from other sources, I will properly cite those resources.

<u>Disclaimers on the Use of the Internet</u>:

1. Neither the District nor its employees are responsible for any damages incurred as the result of the use of the Internet, including but not limited to the loss of data stored on the Internet/Network, or the loss of personal property used to access the Internet.

2. The District is not responsible for unauthorized financial obligations incurred through the use of the Internet.
3. The Internet security is designed to allow access to selected areas by designated users only; however, the Internet administrators may review files and communications to maintain system integrity and ensure that students are using the system responsibly. Students and other users should not expect that files or other information stored using school devices or accounts will be private.

4. The District is not responsible for the accuracy, nature, or quality of information gathered through Internet access.

5. District employees may utilize social networking sites for instructional, administrative, or other work-related communication purposes if they obtain permission for such a site from the Superintendent/designee; develop the site in accordance with any guidelines developed by the Superintendent/designee (including granting access to the site to school/District technology staff); monitor and manage the site to promote safe and acceptable use; and observe confidentiality restrictions concerning the release of student information under state and federal law. By signing this form, parents are giving permission for their child to become "friends" with such District-approved social networking sites.

Hardware Use

1. Students who attend South Spencer may be issued an electronic device at the beginning of each school year.

2. The Principal shall provide notification to parents/guardians whose child is eligible to be issued an electronic device before the beginning of the school year containing information relating to that program/device.

3. Each student and student's parent or guardian must annually sign the student handbook and/or Student Technology Acceptable Use form acknowledging receipt of this policy.

4. **The restrictions set forth above for the Internet apply in their entirety to District-issued devices, even when the devices are used outside the district network.**

5. To protect students and to meet the Children's Internet Protection Act (CIPA) requirements, access to the Internet is filtered through a commercial filtering system.

6. The rental cost of the device is approved by the board annually and is charged as a textbook fee. In the event the device is accidentally damaged, parents/guardians will be responsible for repair costs up to $100 for the first instance and the entire amount for all other damages after that first instance. An insurance option will be made available but it is not mandatory. If damage is intentional or the student shows negligence, parents/guardians will be responsible to the school for the entire cost of the device. Further disciplinary action may be taken by the school. In the event the device is damaged, the device must be returned to the District so that the District can

make any necessary repairs. If the device is lost, this event should be immediately reported to the District. If the device is stolen, this event should be immediately reported to the District and a police report should be immediately filed. A copy of this police report should be submitted to the District. Parents/guardians and student are responsible to the District for the total replacement cost of the device which is lost or stolen, while the device is in the possession, custody, or control of the student.

7. Students and parents/guardians may not attempt any repairs/services on the device and damaged hardware must be returned to the District for repair/service.

8. Remote software or configuration changes that are necessary for maintenance, security and to ensure that only authorized software is installed on the devices may be sent out. Such software maintenance may involve the correction of an altered code or programming and, in some cases, may remove files if the files are deemed to be a threat to the operation or security of the network or are stored in unauthorized software. No notification will precede this type of remote access. However, if it becomes necessary for a school technology official to remotely access the device, the official will attempt to notify the student prior to remotely accessing his/her device.

9. The device has a limited amount of storage for apps and files. Student owned materials will be removed if storage space becomes an issue.

10. Students may not permit individuals other than school personnel to use or access the device.

11. Students may not share their District-issued power cords.

12. The device is at all times the property of the District and the student has no right to disable or modify any hardware or installed software. Apps may be installed by the student as long as the app meets an educational need.

13. Students shall not remove District labels or tags from the device nor shall they add stickers, labels, or other markings to the device or case.

14. If the device comes with a protective case, the device must remain in the protective case at all times. Only South Spencer staff should remove the case if there is a problem. Do not purchase a different case. Lost cases and/or charging cables will be replaced at the student's expense.

15. The school owned device is deemed to be in the custody of the student from the time the student receives the device until it is returned to the designated school representative. If the device is lost or stolen, parent/guardian and student shall immediately advise the Principal/designee of the incident and provide all relevant

information**. When a device is reported lost or stolen, the District may utilize Internet Protocol tracking if available.**

16. The device must be returned at the end of the school year, on the date of withdrawal from a SS school, or upon request by a school administrator. The student must return the device to the District in the same condition that it was originally provided to the student, ordinary wear and tear excepted. Failure to return the student-issued device in accordance with these stated conditions may result in disciplinary action and/or prosecution for all applicable crimes to include, but not be limited to, grand larceny.

17. The device may be reimaged/erased during the summer. All information/apps stored on the device will be wiped clean for the new school year.

18. The District retains the right to review any material sent, mailed, or accessed through a District-owned device or District-provided network account. School district personnel have the right to inspect all material stored on a District-owned device. Students have no right to privacy or confidentiality in material that was created, sent, accessed, or stored using a District-owned device or a District-provided network account.

19. If the school determines that the student failed to adequately care for the District's device or violates District rules or policies, the District shall impose appropriate consequences. If the District determines that the student acted with intent to damage the District's property, then, in addition to any other available remedies, the District may refer the matter for appropriate civil, criminal, and/or juvenile proceedings.

20. Students will use the district owned device and will not be allowed to connect their own device to the network unless permitted by school administrators. If a student is permitted to connect a personal device to the SS network, all rights to privacy on this device are waived when the device is on school property and the device may be managed and controlled by a school owned software management solution.

Consequences for Violations of the Student Technology Acceptable Use Policy

Students are responsible for following the guidelines and rules set forth in the Student Technology Acceptable Use Policy.

Violations of these policies may result in one of the following disciplinary actions:

- Restitution (money paid in compensation for theft, loss, or damage)
- Student/Parent Conference
- Removal of Unauthorized Files and Folders
- Restriction of The Internet Privileges*
- Restriction of District-Issued device Use Privileges**
- Short Term Suspension
- Intermediate Suspension
- Court Referral/Criminal Charges
- Alternative School Placement
- Expulsion

If a violation of the Student Technology Acceptable Use violates other rules of the student handbook, consequences appropriate for violations of those rules may also be imposed.

*If a student's Internet privileges are restricted, this means that for the period of the restriction, the student may only access Internet while at school, and/or under teacher supervision and/or access to certain Internet categories.
**If a student's District-Issued device privileges are restricted, this means that for the period of the restriction, the student may only use his/her device while at school and under teacher supervision.

The following rubric is not meant to be all-encompassing but to serve as a guideline for determining appropriate disciplinary action when a violation of a technology rule occurs.

LEVEL I OFFENSES	LEVEL II OFFENSES
Level I offenses are less serious and begin with a student and/or parent conference. However, depending on the frequency, a Level I violation may merit a more severe disciplinary action such as the ones set forth above.	Level II offenses are more serious and begin with a required conference, the restriction of the Internet and/or District-owned device privileges, and an in-school alternative placement. However, depending on the seriousness and frequency of the violation, a Level II offense may merit a more serious disciplinary action such as the ones set forth above.
Examples of Level I Offenses: • Sharing passwords • Plagiarism • Bypassing District security controls • Defacing computers (e.g., stickers, marker) • Removing District labels or tags • Repeated failure to charge battery • Clearing web browser history • Creating, accessing, downloading, or distributing non-educational materials (e.g., games, music) • Commercial or Political Use • Accessing chat rooms, bulletin boards, or blogs without teacher permission • Posting information online without teacher permission • Failure to Follow Teacher Directives • Failure to Be Polite and Courteous	Examples of Level II Offenses • Downloading, posting, or distributing materials that : □ Are harmful or prejudicial to others (ex. defamatory or libelous) □ Are pornographic, obscene, or sexually explicit, or profane (e.g. music) □ Are Illegal (e.g. copyrighted materials) □ Reference weapons, alcohol, guns, drugs, or gangs □ Constitute gambling □ Are restricted • Engaging in online activity that threatens, intimidates, bullies, harasses, discriminates, or defames • Intentionally destroying hardware or software • Engaging in theft • Engaging in any illegal activity • Harming or destroying another user's data • Creating or sharing a computer virus • Disrupting the network or the educational process

Best Practice Guidelines for Use of the Internet and Electronic Device

- Do not attempt to gain access to the internal electronics or repair the device. If your device fails to work or is damaged, report the problem to the office as soon as possible. You may be issued a temporary unit or other materials until your device is working properly or replaced.
- Always keep track of your device and take reasonable precautions to keep it safe. Never leave unattended unless it is secured in a locked location.
- Never remove the device from the District provided case.
- Do not place the power cord or adapter against the screen in your backpack. This will cause the screen to break.
- Plug the charging cable in the correct port. Make sure the right side is up when connecting the charging cable.
- Do not use the device on your lap with the charging cable connected. You may damage the charging port.
- Never place any items on the device.
- Do Not apply liquids to the device screen. The screen can be cleaned with a soft, lint-free cloth. Avoid getting moisture in the openings. Do not use window cleaners, household cleaners, aerosol sprays, solvents, alcohol, ammonia, or abrasives to clean the screen. Use of unapproved cleaners may remove the protective film covering the face of the screen.
- Never throw a book bag that contains the device. Never place a device in a book bag that contains food, liquids, heavy, or sharp objects.
- Never expose the device to long term extremes in temperature or direct sun light.
- If you notice that your device is working slowly or functioning in a strange or abnormal way, report it to the Technology Center in your building.
- Remember to charge your device each night.
- Do not leave the device in a vehicle.
- Do not eat or drink while using the device or have food or drinks in close proximity.
- Do not allow pets near your device.
- Do not stack objects on your device.
- Do not check the device as luggage at the airport.
- Do not share your device with others.
- Keep your device out of reach of babies and young children.
- Use email safely.
- Do not open, forward, or reply to suspicious emails. If you have a question about whether or not to open an email, check with the Technology Center in your building.
- Do not open email attachments from someone you don't know – it may be a virus or a malicious program.

- Never respond to emails that ask you for personal information, your user name, or your password.
- Think before you write and send an e-mail. Be polite and courteous at all times.
- Do not pass on chain letters. They often contain links to viruses or are scams themselves.
- Use the Internet safely.
- Do not go to inappropriate/questionable websites or click on links that you do not recognize because this may trigger spam or a computer virus attack.
- Be polite and courteous on the Internet. Do not use offensive language such as curse words or insults.
- Remember that once any text or photo is placed online, it is completely out of your control, even if you limit access to your page. Anything posted online is available to the world.
- You should not post information, photos, or other items online that could embarrass you or others.
- Do not post personal information, such as your address, phone number, date of birth, class schedule, your whereabouts, or your daily activities. You could be providing this information to online predators.
- Remember many potential employers and colleges and universities now search the Internet to screen applicants.
- Saving information.
- It is recommended that you save/backup any important files. Your student folder will be maintained for the entire school year. At the end of the school year, all student folders will be erased.

ACKNOWLEDGEMENT OF RECEIPT OF THE

Student Technology Acceptable Use Policy

Student's Name:_____

Student's School:_____

As the parent/guardian of _____, I have read and understand the terms of the Student Technology Acceptable Use Policy.

Parent/Guardian (please print):_____

Parent/Guardian Signature:_____ Date:_____

As the student, my signature indicates that I have read or had explained to me and understand the terms of the Student Technology Acceptable Use Policy and I accept responsibility for abiding by the terms and conditions outlined and for using these resources for educational purposes.

Student (please print):_____

Student Signature:_____ Date:_____