Southern Wells Community Schools

Responsible Use Policy

Introduction

Southern Wells recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st-century technology and communication skills.

To that end, we provide access to technologies for student and staff use.

This Responsible Use Policy outlines the guidelines and behaviors that users are expected to follow when using school technologies or when using personally-owned devices on the school campus.

- The Southern Wells network is intended for educational purposes.
- All activity over the network or using district technologies may be monitored and retained.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources can result in disciplinary action.
- Southern Wells makes a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.
- Users of the district network or other technologies are expected to alert IT staff immediately of any concerns for safety or security.

Technologies Covered

Southern Wells may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more.

As new technologies emerge, Southern Wells will attempt to provide access to them. The policies outlined in this document are intended to cover *all* available technologies, not just those specifically listed.

Usage Policies

All technologies provided by the district are intended for education purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Web Access

Southern Wells provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow district protocol to alert an IT staff member or submit the site for review.

Email

Southern Wells provides users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.

If users are provided with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the district policy or the teacher.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Social/Web 2.0 / Collaborative Content

Recognizing the benefits collaboration brings to education, Southern Wells may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.

Mobile Devices Policy

Southern Wells will provide K-1st grade users iPads and 2nd-12th grade users Chromebooks to promote learning inside and outside of the classroom. Users should abide by the same responsible use policies when using school devices off the school network as on the school network. These mobile devices are property of Southern Wells Community Schools and loaned to the students for educational purposes for the academic year.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to IT staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse. Users are responsible for all repair and replacement charges caused intentionally through lack of reasonable care or precaution including lost devices. Users may not opt to keep damaged devices.

Users should bring the mobile device completely charged to school each day.

Users are responsible for backing up personal data. Never consider any document safe when only stored on one device. Students can back up files using school provided Google Drive account. All files stored in Google Drive will be synced across devices. If mobile device crashes or needs restored, the local student data will be lost on the device.

Use of school-issued mobile devices off the school network may be monitored.

Chromebook and iPad Repair/Replacement Fees

	iPads	Chromebooks
Total Replacement	$299	$229
Screen	TBD	$60
Keyboard/Touchpad/Home Button	TBD	$30
Charger	$25	$25
Case	$33	$33
Other Damage Fees may Apply		

Retuning Mobile Device

At the end of the academic year, users will turn in their iPad and Chromebook, charger, and case. Failure to turn in the mobile device will result in the user being charged the full replacement fee of the device and case.

Users who transfer out or withdraw from Southern Wells must turn in the mobile device, charger and case on the last day of attendance. Failure to turn in mobile device will result in charges for the full replacement fee of the device and case. Unpaid fine and fees of students may result in filing of criminal charges or small claims action.

Personally-Owned Devices Policy

Because of security concerns, when personally-owned mobile devices are used on campus, they should not be used over the school network without express permission from IT staff. In some cases, a separate network may be provided for personally-owned devices.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.

If you believe a computer or mobile device you are using might be infected with a virus, please alert IT. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Downloads

Users should not download or attempt to download or run .exe programs over the school network or onto school resources without express permission from IT staff.

You may be able to download other file types, such as images of videos. For the security of our network, download such files only from reputable sites, and only for education purposes.

Netiquette

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.

Users should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.

Users should also remember not to post anything online that they wouldn’t want parents, teachers, or future colleges or employers to see. Once something is online, it’s out there—and can sometimes be shared and spread in ways you never intended.

Plagiarism

Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they didn’t create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission. Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Users should never agree to meet someone they meet online in real life without parental permission.

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

Examples of Responsible Use

I will:

- ✓ Use school technologies for school-related activities.
- ✓ Bring my device fully charged for the day
- ✓ Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- ✓ Treat school resources carefully, and alert staff if there is any problem with their operation.
- ✓ Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- ✓ Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, and posts) online.
- ✓ Use school technologies at appropriate times, in approved places, for educational pursuits.
- ✓ Cite sources when using online sites and resources for research.
- ✓ Recognize that use of school technologies is a privilege and treat it as such.
- ✓ Be cautious to protect the safety of myself and others.
- ✓ Help to protect the security of school resources.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Examples of irresponsible Use

I will **not**:

- ✓ Use school technologies in a way that could be personally or physically harmful.
- ✓ Attempt to find inappropriate images or content.
- ✓ Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- ✓ Try to find ways to circumvent the school's safety measures and filtering tools.
- ✓ Use school technologies to send spam or chain mail.
- ✓ Vandalizing, damaging, or disabling the property of another individual or oganization
- ✓ Plagiarize content I find online.
- ✓ Post personally-identifying information, about myself or others.
- ✓ Agree to meet someone I meet online in real life.
- ✓ Use language online that would be unacceptable in the classroom.
- ✓ Use school technologies for illegal activities or to pursue information on such activities.
- ✓ Attempt to hack or access sites, servers, or content that isn't intended for my use.
- ✓ Alter devices hardware or software.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Limitation of Liability

Southern Wells will not be responsible for damage or harm to persons, files, data, or hardware.

While Southern Wells employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

Southern Wells will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Violations of this Responsible Use Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges
- Notification to parents
- Detention or suspension from school and school-related activities
- Legal action and/or prosecution

Southern Wells Community Schools
Responsible Use Policy Signature Form:

By signing the below, the student and their parent/guardian agree to follow and accept:

- Responsible Use Policy
- That SWCS owns the Chromebook, software and issued peripherals
- If the student ceases to be enrolled in SWCS, the student/parents will return the Chromebook in good working order or pay the full $229.00 replacement cost of the computer. In addition, the student must also return the Chromebook charger and case. If the Chromebook charger or case is not returned, the student/parent must pay $25.00 for the Chromebook charger and $33.00 for the case.
- In no event shall SWCS be held liable to any claim of damage, negligence, or breach of duty.

Student Acknowledgement:

I understand and will abide by the Responsible Use Policy. I further understand that any violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and disciplinary or legal action may be taken.

Print Student Name:	Date:	Grade:
Student Signature:		

Parent/Guardian Acknowledgement:

As the parent or guardian of this student, I have received a copy of the Responsible Use Policy, and I discussed this with my child. I understand that access is designed for educational purposes. Southern Wells Community Schools has taken precautions to discourage access to controversial material; however, I recognize that it is impossible for Southern Wells Community Schools to restrict access to all controversial materials. Hence, I will not hold the school corporation responsible for materials accessed on the network. Further, I understand and accept responsibility for supervision of the user when he/she is not in the school setting. I hereby give permission for the user noted above to be issued an “Internet Authorization Form”.

Print Guardian Name:	Date:
Parent/Guardian Signature:	

Your Network/Google Apps for Education password: A secure password is essential in a digital world. The password is a minimum of 8 letters, numbers and/or symbols. You may use upper and/or lower case letters. Circle all upper case letters so I can enter them correctly.

________________________________ Please check one _____ **New password**

Printed Password _____ **Same as last year**

You must print your password, even if it is the same as last year.