

# **Swartz Creek Community Schools Acceptable Use Procedures (AUP)**

**Swartz Creek Community Schools provides a wide range of computer and technological resources to its students and staff for the purpose of advancing the educational mission of the District. These resources are provided and maintained at the District's expense and therefore, the public's expense and are to be used by members of the school community with *respect* for the public trust through which they have been provided. The District Internet access is filtered by the GEN Net content filtering system. This filter meets all the standards of the Children's Internet Protection Act.**

**The Acceptable Use Procedures that follow provides details regarding the appropriate and inappropriate use of the District's technology. The procedures do not attempt to articulate all required or proscribed behavior by users. Successful operation of the District's technology network requires that all users conduct themselves in a responsible manner while using the District's computers and other technology. All users are expected to review the guidelines and procedures in this document.**

## TECHNOLOGY ACCESS AND ACCEPTABLE USE PROCEDURES SUMMARY

This is a *procedures summary*. Students and staff should read and will be accountable for following the entire posted program.

1. Technology covered by this procedure includes the use of District software, audio and video media, computers and hardware peripherals, networks, internet, telecommunications, video and audio equipment.
2. The use of District technology is a privilege, which can be revoked at any time by the District.
3. Each individual user is responsible for the reasonable care of technology, including hardware and software while in their possession or while they are using it.
4. Users of District technology will be responsible for its use and misuse. Appropriate use of District technology is defined as use in furtherance of the instructional goals and mission of the District. Users should consider any use, which does not fall under this definition of appropriate use as being potential misuse for which a loss of technology use and disciplinary consequences may occur.
5. Staff and students acknowledge that software, audio and video media are protected by a variety of licensing agreements and copyright laws. Any misuse of technology may subject the user, as well as the District, to a variety of legal liabilities. Staff and students need the written permission of the Network Administrator to install software or media.
6. Users are responsible for the security of the technology, including the ability to use that technology to access confidential information, while such technology is in their possession or under their control. Staff and students are not to either use or disclose confidential information per FERPA.
7. Passwords are the property of the user and are not to be used by anyone else.
8. Swartz Creek Community Schools does not guarantee that Internet and/or e-mail filtering and other precautions we have taken to block potentially objectionable content will control user access to such materials.
9. E-mail is not considered private communication. It may be re-posted. It may be accessed by others and is subject to subpoena. School officials reserve the right to monitor any or all activity on the district's computer system and to inspect any user's e-mail files. Users should not expect that their communications on the system are private. Confidential information should not be transmitted via e-mail.

## Internet and Network Access

Access to the public Internet is a powerful and effective educational tool. It also poses serious potential security risks to Swartz Creek Community Schools computing and communications resources. The security risks generally result from the possibility of inappropriate use of the Internet. To minimize these risks, Swartz Creek Community School District has established standards, procedures and technical controls governing the use of the Internet and the (SCCS) network.

All SCCS network system “users” must adhere to this Acceptable Use Procedures (AUP) when using the network/Internet. For purposes of this AUP, “users” are defined as employees and students of SCCS and other individuals authorized to use the SCCS computing and communications networks. Users are expected to act responsibly and in SCCS’s best interests whenever they use SCCS’s computing resources and communications networks, including but not limited to:

- Accessing only those SCCS computing and communication resources for which they are authorized;
- Using only those SCCS computing and communication resources needed to perform job-related functions;
- Maintaining professionalism, personal responsibility, and a standard of “good taste” in all communications (e.g. among peers and in public forums); and
- Protecting SCCS’s resources, reputation, public trust and public image.

### Network Etiquette

Members are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to:

1. Do not reveal the personally identifiable information of students or colleagues. Personal information includes but is not limited to home address, phone number, school email address, and is protected by the Family Educational Rights and Privacy Act (“FERPA”).
2. Do not assume that only you can read your email; others may be able to read or access your mail. Do not send or keep anything that you would be uncomfortable seeing in the daily newspaper.
3. Be polite. Do not get abusive in your messages to others. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Illegal activities are strictly forbidden.
4. Do not use the network in a way that would disrupt other users on the network. Disruptive network conduct includes but is not limited to: excessive bandwidth use, damaging programs and/or files, establishing illegal services, modifying operating systems, changing background images on the desktop, establishing a link to another computer in the network without permission, etc.
5. Do not use someone else’s network account or password.
6. Do not use someone else’s workstation without their prior knowledge and consent.
7. Do not use your network account for non-school/non-work related activities.
8. All Internet use of any type must be school or work-related.
9. Do not use unauthorized copies of commercial software or download software from the Internet without permission from the Technology Office.
10. K-12 students must not access controversial information without the permission of their parent/guardian, and/or educational sponsor. (This includes ftp, telnet, or other Internet programs that can transmit images, words or data.) Controversial is defined as inappropriate for the culture of the organization. **K-12 student users must be strictly monitored by a trained adult user and must have a signed student AUP on file.**
11. K-12 organizations creating web pages must comply with appropriate legal restrictions on information that relates to students under the age of 18 years. This means that personal identifying information about

students, including full names, or individual pictures with full names, may not be published. Web pages must comply with the written mission of Swartz Creek Community Schools.

12. All information (excluding email) accessible via the network/Internet should be assumed to be private property unless otherwise stipulated

### **SCCS Management Responsibilities**

SCCS management is responsible for determining who can access the Internet/network based on business need, and for providing general supervision of authorized users who are granted network/Internet access. This includes requiring that users understand and accept their individual obligations as set forth in this AUP. Access to the computer/network/Internet will require an electronic signing of the AUP agreement daily. This serves as a daily reminder of the expectations of the district and a daily acknowledgement of the user's responsibilities.

### **User Responsibilities and Provisions of Usage**

The following usage provisions have been established to protect the SCCS computing resources and communications networks. Their purpose is to assure that users are responsible and productive in their use of the network/Internet, including, without limitation, complying with all applicable laws, regulations and other legal requirements, and the SCCS guidelines for employee conduct.

In exchange for the privilege of using/accessing the SCCS computing resources and communications networks, all SCCS users understand and agree to the following:

1. Network resources are intended for the exclusive use of its registered/authorized users. Users are responsible for account passwords and privileges. Any problems that arise from the use of a staff member's account are the responsibility of the account holder. Use of an account by someone other than the registered account holder is forbidden.
2. Users will maintain a professional demeanor in all Internet/network communications/access. Participation in any communications or other activities that may constitute harassment, political activity, personal profit or gain, or possible illegal activity is forbidden.
3. The district reserves the right to remove and/or monitor any material stored in files and will remove any material the district, at its sole discretion, believes may be unlawful, offensive or disrespectful of others. User accounts/access will not be used to access, view, download, or otherwise gain access to such materials.
4. Network users will abide by all applicable laws and regulations, including laws and regulations pertaining to copyrights, trademarks, patents, data, and software protection. Installation of or copying of illegally licensed software via the SCCS network or on SCCS networked work stations is prohibited.
5. Authorized email accounts will be cleaned regularly by the account holder to avoid excessive use of the electronic mail disk space.
6. The district reserves the right to log network use and to monitor fileserver space utilization by users.
7. The sharing of personal information (e.g. name, address, email address, phone, etc) about any authorized SCCS user without the permission of the user is forbidden.
8. The district does not guarantee the functions of the system will meet any specific requirement the user may have, or that it will be error free or uninterrupted, nor shall it be liable for any direct or indirect, incidental or consequential damages (including lost data, information, or time) sustained or incurred in connection with the use, operation, or inability to use the system.
9. Authorized users are expected to not engage in any activities that could disrupt or compromise the integrity or security, or otherwise result in the misuse of SCCS computing resources and communications networks. Report all security breaches to SCCS management.
10. Use the Internet/network and the communications resources in a manner that minimizes cost to SCCS while maximizing value and productivity for SCCS business purposes.

11. No non-district owned computers or peripherals are to be connected to the network. Foreign equipment may be confiscated.
12. Users are expected to report abuse or misuse of the network/Internet system to their supervisor or the network administrator.

### **Access to Potentially Objectionable Content**

Users are advised that some systems may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material. Users, Swartz Creek Community Schools and system administrators do not condone the use of such materials. Users and parents of students accessing the system should be aware of the existence of such materials and are responsible for monitoring usage of the system.

Despite the precautions that Swartz Creek Community Schools may take to prevent access to potentially objectionable content, Swartz Creek Community Schools does not guarantee that it will control user access to such materials, or that users will not have access to such materials while using Swartz Creek Community Schools' technological resources. The school district will make every effort to prevent such access or exposure through the use of filtering software.

### **Warranties Not Provided**

Swartz Creek Community Schools will not be responsible for any damages suffered by the user. Use of any information obtained via the Internet/network is at the user's own risk. Swartz Creek Community Schools specifically denies any responsibility for the accuracy or quality of information obtained through the network/Internet.

Swartz Creek Community Schools is not liable for any information or data that may be lost, damaged, or unavailable due to technical or other difficulties, delays, non-deliveries, or service interruptions caused by its own negligence, subcontractors or the user's errors or omissions.

Swartz Creek Community Schools is not responsible for any damages to a user's own hardware or software caused by downloading computer viruses or other contaminants.

Members using district technology will be responsible for its use and misuse. Appropriate use of district technology is defined as a use to further the instructional goals and mission of the district. Members should consider any use outside these instructional goals and mission constitutes potential misuse, which could result in loss of technology privileges and/or in disciplinary consequences. Any questions should be referred to the District Technology Director or Assistant Superintendent for Personnel.

### **Technical Controls**

Access to the network/Internet may be made only via SCCS approved technology equipment. SCCS approved firewalls are designed, operated, monitored, and regularly tested to support the following key technical security controls:

- Allow only authorized users to access the network/Internet
- Prevent any unauthorized user/system from compromising SCCS systems or data;
- Provide audit trails of user/system activity
- Access to content on the Internet is protected by a content filter designed, monitored, and regularly tested to prevent access to inappropriate material.

### **Monitoring and Disciplinary Action**

Users who are granted access to the Internet expressly consent to having their access monitored and recorded in accordance with applicable laws. Such monitoring and recording will be used to verify compliance with this AUP. All messages created, sent or received over the network/Internet are the property of SCCS and should be considered as public information and not private.

SCCS management, in its sole discretion, will determine what constitutes acceptable use of its communication networks and network connections, and reserves the right to block, alter priority, or terminate access to any service or activity. Accordingly, SCCS management, in its sole discretion, may temporarily or permanently disconnect any user at any time. Users are advised that if possible illegal activity is detected, all communications, including text and image, and system records, may be provided to appropriate law enforcement officials or third parties without prior consent of, or notice to, the sender or receiver.

Additionally, failure to comply with this AUP may result in disciplinary action up to and including dismissal.

### **Prohibited Uses of Network**

- *Commercial Use* - Use of District Computers for personal or private gain, personal business or commercial advantage is prohibited.
- *Political Use* - Use of the District Computers for political purposes in violation of federal, state, or local laws is prohibited. This prohibition includes using District computers to assist or to advocate directly for or against a ballot proposition and/or the election of any person to any office.
- *Illegal or Indecent Use* – Using District computers for illegal, harassing, vandalizing, inappropriate, or indecent purposes (including accessing, storing, or viewing pornographic, indecent, or otherwise inappropriate material), or in support of such activities is prohibited. Illegal activities are any violations of federal, state, or local laws (for example, copyright infringement, publishing defamatory information or committing fraud). Harassment includes slurs, comments, jokes, innuendoes, unwelcome compliments, cartoons, pranks, or verbal conduct relating to an individual that (1) have the purpose or effect of creating and intimidating, a hostile or offense environment; (2) have the purpose or effect of unreasonably interfering with an individual's work or school performance, or (3) interfere with school operations. Vandalism is any attempt to harm or destroy the operating system, application software or data. Inappropriate use includes any violation of the purpose and goal of the network.

### **Web Pages and Blogs**

Any web pages that may be constructed by students or staff of Swartz Creek Community Schools that are published through or accessed from a server belonging to the District must meet the following guidelines: A web page cannot contain:

- Abusive, obscene, or inappropriate language, messages or pictures;
- Personal information about students including full name, address, e-mail address, phone number, pictures in which individuals are clearly identified – (unless permission is obtained from the parent/guardian in writing);
- Material that is in violation of copyright laws; and
- Links to sites that are social (for example, chat rooms), controversial, or inappropriate for schools.

A web page must serve an educational purpose; for example an instructional resource or community communications vehicle. Each web page must meet high standards of clarity, grammar, spelling, and punctuation. All information included must be completely accurate and up-to-date. Each web page must

be approved by the building administrator and the Network Administrator prior to placement on the server. Each web page must be maintained on a regular basis to be sure that information is current and all links are functional. This is the responsibility of the author(s) or the web class. If it is not done, the page will be removed from the server. Students may not publish personal web pages on the District servers and a web page may not be used for commercial purposes. Blogs linked from the district website must be a result of a classroom activity or assignment and do not represent the opinions or views of SCCS.

## User Signature Page

I have read the Technology Acceptable Use Procedures for Swartz Creek Community Schools and understand its contents. My signature below designates that I agree to and will follow the guidelines and prohibitions as stated in the document. I am aware that Swartz Creek Community Schools reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the Swartz Creek Community Schools' network and email system at any time, with or without notice, and that such access may occur during or after the regular school/work day.

I further understand that although Swartz Creek Community Schools prohibits abuse of technology, it is impossible to restrict all access to inappropriate materials which may be on the Internet or through electronic communications. Accordingly, I will not hold Swartz Creek Community Schools, its employees, or agents responsible for materials which may be acquired through Swartz Creek Community Schools' network.

I understand that access to available technology is a privilege and a condition of employment at Swartz Creek Community Schools requiring adherence to this agreement.

After I receive my account, I will be given a username and starting password. I understand that I will be required to change my password frequently for security purposes.

Passwords **MUST** be kept confidential. Should I lose my password or be unable to log into my account, I will need to call the Technology Office to reinstate my account.

This agreement will provide services during my tenure with the district. The Acceptable Use Procedures is posted on the District's website for review at any time. Daily access to my account will require a daily electronic signing of this agreement each time I log-in to the network. I further understand that any questions or concerns regarding the AUP should be directed to the Network Administrator.

***Signature acknowledges user has read and understands the terms and conditions of access and agrees to comply with the conditions as stated.***

User Name (Printed) \_\_\_\_\_ User Name (Signature) \_\_\_\_\_

Date: \_\_\_\_\_

Name of School/Building: \_\_\_\_\_

Supervisor's Signature: \_\_\_\_\_

Date: \_\_\_\_\_

## Student/Parent (Guardian) Signature Page

I have read the Technology Acceptable Use Procedures for Swartz Creek Community Schools and understand its contents. My signature below designates that I agree to and will follow the guidelines and prohibitions as stated in the document. I am aware that Swartz Creek Community Schools reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the Swartz Creek Community Schools' network and email system at any time, with or without notice, and that such access may occur during or after the regular school/work day.

I further understand that although Swartz Creek Community Schools prohibits abuse of technology, it is impossible to restrict all access to inappropriate materials which may be on the Internet/network or through electronic communications. Accordingly, I will not hold Swartz Creek Community Schools, its employees, or agents responsible for materials which may be acquired through Swartz Creek Community Schools' network.

I understand that access to available technology is a privilege.

We have read the Technology Acceptable Use Procedures for Swartz Creek Community Schools and understand its content.

Our signatures below designate that we agree to follow the guidelines and prohibitions as stated.

**Please complete and return this page:**

Student's Name (Printed) \_\_\_\_\_ Student's Signature \_\_\_\_\_

Date: \_\_\_\_\_

Sponsoring Educator: \_\_\_\_\_

Date: \_\_\_\_\_

Parent/Guardian's Name (Printed): \_\_\_\_\_

Parent/Guardian's Name (Signature): \_\_\_\_\_

Date: \_\_\_\_\_