Code No. 603.10

SOUTH HAMILTON COMMUNITY SCHOOL DISTRICT
TECHNOLOGY ACCEPTABLE USE POLICY

I. Introduction

Technology is a vital part of modern education and is widely used in curriculum at the South Hamilton Community District. Internet access is provided to employees and students for this reason. Appropriate and equitable use is provided for computers, computer network systems, and Internet access.

Students and staff will be assigned access to computers, computer network systems, and Internet access. This access will include email accounts, licensed software, file storage, electronic subscription services, and other electronic access as deemed necessary for job functions and student activities. All accounts, usernames, passwords, and data generated by or on computers, computer network systems, and Internet access owned by the South Hamilton Community School District are covered under the rules and regulations of this policy.

All accounts, usernames, passwords, and data generated by or on computers, computer network systems, and internet access are subject to retention, review, override, supervision, and are the property of South Hamilton Community School District. Emails that end in the District's purchased and governed domain name are electronic documents owned and governed by the District as such. All network access be it Wi-Fi or wired, guest or otherwise noted is still owned and operated by the District and this policy will govern said use equally for all staff and students.

Electronic communications on personal cell phone devices not owned by the District are private according to the FCC and are not blocked by the District when used between the cell phone service provider and the private subscriber only. If a private cell phone device joins the company email, company Wi-Fi, or accesses systems regulated by the District's systems or internet access, that cell phone is no longer private and is subject to laws and regulations as well as this policy of Acceptable Use, data retention, review, and supervision.

The District reserves the right to limit access or use of personal cell phones during scheduled times of operation for staff and students alike. The District can request the removal of personal cell phones from classrooms, locker rooms, or other areas where they are considered a disruption to education, privacy violation, or discipline issue. If you bring a personal cell phone to this environment as a staff member or student you agree to these terms and conditions. If you do not agree to these terms and conditions the District recognizes your cell phone is not a tool for your job or your learning and is not needed at these facilities.

The District recognizes any communication between employees of the District and students protected by the District via text, email, or other forms of electronic communication are subject for review and discipline as per the protection of children and staff in our care and is governed by the Policy of Acceptable Use.

Continue-

II. What is Acceptable Use

1. Use of District equipment for education content as assigned by district staff.
   a. The content, delivery, and supervision of electronic education must adhere to Federal, State, & Local laws as well as District Policy.
   b. The content must be age appropriate, related to a field of study, refrain from illegal or illicit activities, be in no violation of copyright laws or end user agreements of services, and all content falls under review of the District's Administrative Team at all times.
   c. Content at no time can be used to discriminate against students or staff for any reason, be used to harass or coerce staff or students.
   d. Content at no time can be used to slander, defame, or bully students or staff.
   e. Student devices are not issued for entertainment or recreational use, they are issued for schoolwork as assigned by the district. They are not to be used for social networks, music, movies, or games.
2. Use of District equipment for job performance.
   a. The content, delivery, and supervision of electronic education must adhere to Federal, State, & Local laws as well as District Policy.
   b. The content must be professional in nature, related to an area of business duties, and appropriate for a professional environment.
   c. Content at no time can be used to discriminate against students or staff for any reason, be used to harass or coerce staff or students.
   d. Content at no time can be used to slander, defame, or bully students or staff.
   e. Staff devices may be used to access personal email, social networks, professional and nonprofessional peer groups; however all data created and accessed by company issued staff equipment and electronic accounts are still governed by and reviewed by District Administration. Non company use of company equipment can be evaluative as it relates to job performance, professionalism, and laws that govern data.

III. Monitoring

1. Monitoring by government agencies outside of our district.
   a. The District receives services & funding from other government agencies and they can and do monitor data on electronic communications.
   b. The State Department of Education can access student records, grades, testing results, and demographic information.
   c. The State Communications and Information Technology team can and does monitor the Iowa Communications Network known as the ICN. Our District does receive internet access from this network and is monitored and governed as such.
   d. The Area Education Agencies known as the AEA provide electronic subscription services, and as such can monitor and control access to shared systems and subscription services.
2. Monitoring by internal IT staff and Administrative Team.
   a. Servers, Firewalls, Wi-Fi Access Points, and other District owned equipment have the ability to monitor, retain, and review all electronic data and communications. Some communications initiate flagged events and require Administrative review. Examples may include but are not limited to; Suicide, Profanity, Pornography, Harassment, Violence, and Fraud.

Continue-

3. Monitoring by cloud based or Internet services.
   a. Much of our District's data is generated and housed on Internet or cloud based servers as owned or rented by the District. The district subscribes to cloud based monitoring systems that can monitor district equipment and accounts at all times regardless of location, time of day, or time of year. District owned equipment and accounts generating district owned and controlled data is monitored by cloud services. Some communications initiate flagged events and require Administrative review. Examples may include but are not limited to; Suicide, Profanity, Pornography, Harassment, Violence, and Fraud.

IV. Response

The District's Administrative Team will have discipline responses per building in the district. The Elementary, Middle School, and High School may have different policies and procedures on discipline due to the different natures in ages, ability to take or not take equipment home, and content appropriateness.

Each Building's Student Hand Book will outline AUP Violation severity levels and consequences.

The District's Administrative Team will handle staff violations. The District's Administration Team will use laws, regulations, and District Policies to determine what constitutes inappropriate use, and their decision is final when signed by the Superintendent of Schools.

V. Warning

The Internet is an ever evolving and expanding electronic landscape. Data is created at a pace that is impossible to filter with 100% accuracy and assurance. Filter services do not discover some harmful elements of the Internet, and content management systems until complaints or data verification has deemed them harmful. Staff and students may find information on the internet that is not factual or has no basis in reality, may be illegal or illicit in nature, may contain unauthorized copies of copyrighted materials, may be controversial in nature and views/opinions posted may be offensive, and more. It is the intention of the District's Board of Directors, Administrative Team, and Staff to create and maintain a safe learning environment in the classroom as well as online. As part of this agreement, staff and students are instructed to exit sites that are offensive, illegal, or have material unsuitable for an education environment and minors.

Approved: 9/16/96	Reviewed: 12/97	Revised:	6/13/05
	Reviewed: 2/10	Revised:	6/07
	Reviewed: 5/14	Revised:	6/16

Legal References: Children's Internet Protection Act, 47 U.S.C. 254(h)
Iowa Code 279.8(1999)

SOUTH HAMILTON COMMUNITY SCHOOL DISTRICT
RECOGNITION OF THE CHILDREN'S INTERNET PROTECTION ACT

The Board of Directors of the South Hamilton Community School District is committed to making available to students and staff members access to a wide range of electronic learning facilities, equipment, and software, including computers, computer network systems, and the internet.

The goal in providing this technology and access is to support the educational objectives and mission of the South Hamilton Community School District and to promote resource sharing, innovation, problem solving, and communication.

The District's computers, computer network and/or Internet connection is not a public access service or a public forum. The District has a right to place restrictions on the material accessed and/or posted through the use of its computers, computer network, and/or Internet connection.

Access to District technology resources is a privilege, not a guaranteed or protected right. Each student and staff member must have signed an acceptable use agreement, binding them to the terms and conditions of use, prior to any access to the District's computers, computer network, and Internet connection. The amount of time and type of access provided to the District's students and staff may be monitored and restricted by the District's technology settings.

All computers, computer network systems, and Internet connections provided to students and staff will be subject to the Children's Internet Protection Act known as CIPA. The following segment is from the Federal Communications Commission (FCC) providing details of CIPA that apply to the District's computers, computer network, and Internet access.

What CJPA requires

Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors), before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.

Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors; and
2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response.

Continue-

Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing:

A. Access by minors to inappropriate matter on the Internet
B. The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications
C. Unauthorized access, including so-called "hacking" and other unlawful activities by minors online
D. Unauthorized disclosure, use, and dissemination of personal information regarding minors
E. Measures restricting minors' access to materials harmful to them

Schools and libraries must certify they are in compliance with CIPA before they can receive E-rate funding.

In adherence with these federal rules and regulations:

Students and staff members shall only engage in appropriate, ethical, and legal utilization of the District's computers, computer network systems, and Internet access. Inappropriate use and/or access will result in the restriction and/or termination of this privilege and may result in further discipline for the staff members and students. Students may be suspended, expelled, and/or face legal action depending on the severity of the offense as determined by the Administrative Team at South Hamilton Community School District. Staff may warned verbally, warned in writing, suspended with pay, suspended without pay, terminated from employment, and/or face legal action depending on the severity of the offense as determined by the Administrative Team at South Hamilton Community School District.

The District's Administration Team will use laws, regulations, and District Policies to determine what constitutes inappropriate use, and their decision is final when signed by the Superintendent of Schools.

The District's Director of Technology may close or suspend a user account of any student at any time as required to meet the requests of the District's Administrators, Faculty, and Parents as it relates to computer, computer network systems, and internet access. The District's Director of Technology may close or suspend a user account of any staff member at the request of any member of the District's Administrative Team. Students and staff members will be instructed and trained annually on this policy.

Approved: 9/16/96	Reviewed: 12/97	Revised: 6/13/05
	Reviewed: 2/10	Revised: 6/07
	Reviewed: 5/14	Revised: 6/16