School District of Springfield Township	No 815 SECTION: Administrative, Professional and Support Employees TITLE: Acceptable Use of Computers, Etc. By Employees ADOPTED: May 16, 2005 REVISED: May 16, 2011

1. Purpose	**No. 815. Acceptable Use of the Computers, Network, Internet, Electronic Communications and Information Systems By Employees** The School District of Springfield Township ("School District") provides employees with access to the School District's electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means. Employees must read, understand and comply with this policy, which governs network and Internet usage, electronic communications, telecommunications, copyright and information security measures. The School District provides technology resources with a firm belief that the educational advantages outweigh the potential for misuse. In return, the School District expects students and employees to exercise appropriate personal responsibility in their use of these resources. Our goals are to provide access to educational tools, resources, and communication to encourage innovation and collaboration. Our policies are intended to promote the most effective, safe, productive, and instructionally sound uses of these tools. The School District encourages staff to hone their digital presence. Staff must model appropriate and creative digital citizenship as they navigate ever-changing digital landscapes. Experimentation, evaluation, and synthesis in these environments are expected. For employees, the School District's ICTsystems must be used primarily for education-related purposes and performance of School District job duties. Incidental personal use of school computers is permitted for employees so long as such use does not interfere with the employee's job duties and performance, with system operations, or with other system users. Personal use must comply with this policy and all other applicable School District policies, procedures and rules contained in this policy, as well as the Internet service provider ("ISP"), local, state and federal laws and must not damage the School District's ICT systems.

	The School District intends to strictly protect its ICT systems against numerous outside and internal risks and vulnerabilities. Employees are important and critical contributors in protecting these School District assets and in lessening the risks that can destroy these important and critical assets. Consequently, employees are required to fully comply with this policy, and to immediately report any violations or suspicious activities to building principal, Director of Technology, and Network Manager. Conduct otherwise will result in actions further described in this and in other relevant School District policies.
2. Definitions	ICT- Computers, network, Internet, electronic communications and information systems (collectively "Information and Communication Technology or ICT systems") provide access to vast, diverse and unique resources. Use of any technological resource accessed through our ICT is subject to the parameters of this definition and policy. The Board will provide access to the School District's ICT systems to facilitate learning and teaching to foster the educational purpose and mission of the School District. 1. Access to the Internet – A device will be considered to have access to the Internet if it is connected to a School District network. 2. Device – A device is defined as any electronic equipment capable of storing, receiving, and transmitting data or information. It includes but is not limited to any personal hardware such as a computer, phone, software, or other technology used on School District premises or at School District events. It includes items connected to the School District Internet. Devices may also contain School District programs or School District or student data (including images, files, and other information). 3. Electronic Communications Systems – This is any messaging, collaboration, publishing, broadcast, or distribution system that depends on resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across network systems between or among individuals or groups. 4. Educational Purpose- This includes the use of the ICT systems for teaching, learning, and school affiliated activities. 5. Harmful to Minors- This includes any picture, image, graphic

	image file or other visual depictions that: a. taken as a whole, with respect to minors, appeals to the prurient interest in nudity, sex, or excretion; b. depicts, describes, or represents in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual content, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals, and c. taken as a whole lacks serious literary, artistic, political, or scientific value with regard to minors. 6. Inappropriate Material- This includes any material (visual, graphic, text, and any other form) that is profane, obscene (pornography or child pornography), sexually explicit, threatening, terroristic, harassing or otherwise unlawful, advocates illegal acts, violence or discrimination (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability) towards people or property. 7. Minor- For purposes of compliance with the Children's Internet Protection Act ("CIPA"), an individual who has not yet attained the age of seventeen is a minor. For other purposes, minor will mean the age of minority as defined in the relevant law. 8. Network- This is a system that links two or more electronic devices, including all components necessary to effect the operation. 9. Obscene- The material meets the following elements upon analysis: a. Whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest; b. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state of federal law to be obscene; and c. Whether the work taken as a whole lacks serious literary, artistic, political, or scientific value. 10. Technology Protection Measure(s)- This is a specific technology that blocks or filters Internet access.
3. Authority	In conjunction with the ever increasing role technology plays in learning, the School District provides access to the ICT systems. These systems as well as user accounts and information, are the property of the School District. The School District reserves the right to deny access to prevent

unauthorized, inappropriate, or illegal activity. The School District may also revoke access and/or administer appropriate disciplinary action including termination.

1. The School District will cooperate fully with ISP, local, state and federal officials in any investigation concerning or related to the misuse of the ICT systems.

2. It is often necessary to access user accounts in order to perform routine maintenance and security tasks. System administrators have the right to access the stored, transmitted or received communications or information of user accounts for any reason in order to uphold this policy and to maintain the system.

3. Users have no privacy expectation in the contents of their personal files or any of their use of the School District's ICTsystems.

4. The School District reserves the right to monitor, track, log and access ICT systems use and to monitor and allocate fileserver space.

5. The School District reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through software blocking or general policy. Measures designed to restrict adults' and minors' access to material harmful to minors may be disabled to enable an adult to access bona fide research or for another lawful purpose.

6. The School District has the right, but not the duty, to monitor, track, log, access and report all aspects of its computer information technology and related systems of all users to protect the School District's resources and to ensure compliance with this policy, other School District policies and the law.

7. The School District has the right to intercept communications for maintenance and security purposes and, if doing so, determines that this policy has been violated by the School District, may take disciplinary action.

8. The School District reserves the right to restrict or limit usage of lower priority ICT systems and computer uses when network and computing requirements exceed available capacity according to the following priorities; determined on a case by case basis:
    a. Highest – uses that directly support the education of the students.

	b. Medium – uses that indirectly benefit the education of the students. c. Lowest – uses that include reasonable and limited educationally-related interpersonal communications and incidental personnel communications. 9. The School District additionally reserves the right to: a. Determine which ICT systems will be provided through School District resources. b. View and monitor network traffic, file server space, processor, and system utilization, and all applications provided through the network and communications systems, including e-mail, whether the work taken as a whole lacks serious literary, artistic, political, or scientific value. c. Remove personal or expired e-mails or files taking up excessive server disk space as determined by the Director of Technology. A warning will be given prior to removing email or files, unless the files present an imminent threat to the ICT. d. Revoke user privileges, remove user accounts, or refer to legal authorities when violation of this and/or any other applicable School District policies occur or state or federal law is violated.
4. Responsibility	In compliance with the Children's Internet Protection Act ("CIPA"), the School District actively filters Internet content. The dynamic and interactive nature of the Internet makes it impossible to filter and block all inappropriate content. Intentionally accessing or using inappropriate content may result in disciplinary action explained further in this and other relevant policies. 1. Employees must become proficient in the use of the School District's ICT systems, devices and software relevant to the employee's responsibilities. Employees must also sign a User Agreement and agree to the requirements of this policy in order to be permitted to use the School District's ICT systems. 2. School District Limitation of Liability The School District makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the School District's ICT systems will be error-free or without defect. The School District does not warrant the effectiveness of Internet filtering. The electronic information available to users does not imply endorsement of the content by

	the School District, nor is the School District responsible for the accuracy or quality of the information obtained through or stored on the ICT systems. The School District will not be responsible for any damage users may suffer, including but not limited to, information that may be lost, damaged, delayed, misdelivered, or unavailable when using the computers, network and electronic communications systems. The School District will not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The School District will not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the School District's ICT systems. In no event will the School District be liable to the user for any damages whether direct, indirect, special or consequential, arising out the use of the ICT systems. The School District will not be held liable for any damage that may occur as a result of connecting to the District Network or any electrical power source. The School District will not be held responsible for any physical damage, loss or theft of the personally-owned device, and reserves the right to inspect, at any time, any personally-owned network capable device whether or not it is connected to the District Network. Student and employee use of personally-owned devices in the classroom setting may be permitted based on the instructional value of its use. Persons connecting devices to the School District of Springfield Township Network agree to maintain current anti-virus software enabled on their devices and to provide applicable addresses in order to provide updates and information.
5. Delegation of Responsibility	1. The Director of Technology and/or designee will serve as the coordinator to oversee the School District's ICT systems approve activities, provide leadership in proper training for all users in the use of ICT systems and the requirements of this policy, establish a system to insure adequate supervision of the ICT systems, maintain executed user agreements, and interpret and enforce this policy. 2. The Director of Technology and/or designee will establish a process for setting-up individual and class accounts, set quotas for disk usage on the system, establish a retention schedule, and establish the School District virus protection process.
6. Guidelines	1. Access to the ICT Systems a. ICT system user accounts will be used only by authorized owners of the accounts for authorized purposes. b. An account will be made available according to a procedure developed by appropriate School District

authorities. The procedures will require that all users review this policy and sign a User Agreement prior to the issuance of an account.

c. Guests may receive an individual account with the approval of the Director of Technology and/or designee if there is a specific, School District-related purpose requiring such access. Use of the ICT systems by a guest must be specifically limited to the School District-related purpose. Guest passwords will be changed at least weekly and provided to individuals as needed.
d. This and other School District policies, as well as applicable laws and regulations govern employee use of the School District's ICT systems.
e. School District employees and students will have access to the Internet through the School District's ICT systems as needed.
f. Remove personal or expired e-mail or files taking up excessive server disk space as determined by the Director of Technology. A warning will be given prior to removing email or files, unless the files present an imminent threat to the ICT.

2. Acceptable Behaviors
Employees, as consumers and creator of content on the District ICT, must:
   a. Use the District computer system in a manner consistent with District policies and the educational mission.
   b. Use the system for only educationally related initiatives and activities or incidental personal use.
   c. Promptly disclose any message that is harassing or inappropriate to a member of the school staff.
   d. Remain responsible for their individual use, including taking reasonable precautions to prevent others from using their accounts and keeping their passwords private.
   e. Promptly notify the Director of Technology of any possible security problems.
   f. Promptly disclose any inadvertent access to unacceptable materials or information or any unacceptable Internet information to the Director of Technology.

3. Prohibitions
The use of the School District's ICT systems for illegal, inappropriate, unacceptable, or unethical purposes by users is prohibited. Such activities engaged in by users are strictly prohibited and illustrated below. These prohibitions are in effect any time School District resources are accessed whether on School

	District property or remotely, directly or indirectly from another ISP whether using district equipment or personal equipment. Employees as consumers and creators of content of the District ICT, will not: a. Access, review, upload, download, store, print, post, or distribute pornographic, obscene, sexually explicit, or other materials harmful to minors. b. Transmit or receive inappropriate materials as defined in this policy. c. Access, review, upload, download, store, print, post, or distribute materials that use language or images that are inappropriate in the educational setting or disruptive to the educational process or post information or materials that could cause damage or danger of disruption. d. Knowingly or recklessly post false or defamatory information about a person or organization, harass another person, or engage in personal attacks, including libelous or slanderous attacks. e. Engage in any illegal act or violate any local, state, or federal statute or law. f. Vandalize, damage, or disable the property of another person or organization, including the School District, or attempt to degrade or disrupt equipment, software, or system performance by spreading computer viruses or by any other means tamper with, modify, or change the District computer system software, hardware, or wiring, or take any action to violate the system security or use the system in such a way as to disrupt its use by other users. g. Hack or otherwise gain unauthorized access to resources or access another person's materials, information, or files without the direct permission of that person or to provide access to unauthorized users. h. Hack or otherwise gain unauthorized access to the District computer system or any other system through the District computer system; attempt to log in through another person's account; use computer accounts, access codes, or network identification other than those assigned to the user; or distribute passwords to others. i. Violate copyright laws or usage licensing agreements or otherwise use another person's property without the person's prior approval or proper citation, including downloading or exchanging pirated software or copying software to or from any school computer or plagiarizing works they find on the Internet. j. Use ICT to conduct a business, further unauthorized commercial purposes, attain financial gain unrelated to the

mission of the District, offer or provide goods or services, or make product advertisement or purchase goods or services for personal use without authorization of the appropriate school official.

k. Support any political or lobbying activity.

l. Post chain letters or engage in "spamming," i.e. the sending of annoying or unnecessary messages to a large number of people.

4. Content Guidelines

Information electronically published on the School District's ICT systems will be subject to the following guidelines:

a. Published documents, audio, video, or conference presentations may include a child's likeness or name unless a parent or guardian submits a completed Opt-Out Form. The Director of Technology will maintain parental Opt Out Forms.

b. Published documents, audio, video, or conference presentations may include a staff member's likeness or name unless a staff member submits a completed Opt-Out Form. The Director of Technology will maintain staff Opt Out Forms.

c. Documents, web pages, electronic communications, or video conferences may not contain inappropriate material as defined by this policy or point directly to inappropriate materials.

d. Documents, web pages, and electronic communications must conform to all School District policies and guidelines, as well as applicable laws and regulations, including but not limited to, restrictions on use and publication of copyrighted material.

5. Due Process

a. The School District will cooperate with the School District's ISP, local, state, and federal officials to the extent legally required in investigations concerning or relating to any illegal activities conducted through the School District's ICT systems.

b. If employees possess due process rights for discipline resulting from the violation of this policy, they will be provided such rights.

c. The School District may terminate the account privileges by providing notice to the user.

6. Search and Seizure
    a. The School District has the right to monitor, track, log, and access any electronic communications, including but not limited to, Internet access and e-mails at any time for any reason.
    b. Users have no legitimate expectation of privacy in their use of the School District's ICT systems, and other School District technology, even when used for personal reasons.
    c. The School District reserves the right, but not the obligation, to access any personal technology device brought onto the School District's premises or at School District events that has been connected or is believed to have been connected to the School District network to determine whether the device contains School District programs or School District or student data (including images, files, and other information) to protect the School District's resources, and to ensure compliance with this policy, other School District policies, and applicable law.

7. Copyright and Fair Use
   Federal law pertaining to copyrights governs the use of material accessed through the School District resources. Users must comply with Policy 814 regarding the use of copyrighted materials and media guidelines with educational fair use. Consequences for inappropriate, unauthorized, and illegal use include:
    a. Use of ICT demands personal responsibility and an understanding of acceptable uses of the Internet.
    b. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the District computer system may result in consequences including: warnings, usage restrictions, loss of privileges, oral or written reprimands, suspensions, termination, and legal proceedings on a case-by-case basis.
        i. This policy incorporates all other relevant School District Policies such as, but not limited to, copyright policy, property policy, curriculum policies, terroristic threat policy, and harassment policies.
        ii. The user will be responsible for damages to the network, equipment, electronic communications systems, and software resulting from deliberate and willful acts. The user will also be financially responsible for incidental or unintended damage resulting from willful or deliberate violations of this policy.
        iii. Vandalism may result in cancellation of access to

	the School District's ICT systems and resources and is subject to discipline and/or legal action. iv. Violations as described in this policy may be reported to the School District, appropriate legal authorities, whether the ISP, local, state, or federal law enforcement. The School District will cooperate to the extent legally required with authorities in all such investigations.

School District of Springfield Township

Staff Digital Expectations

The school district provides technology resources with a firm belief that the educational advantages outweigh the potential for misuse. In return, the school district expects students and employees to exercise appropriate personal responsibility in their use of these resources. Teachers must create an online presence using social media that showcases teaching craft. Professionals' images on social media can affect their careers whether it is used for personal or professional reasons.

Students need modeling to learn appropriate ways to navigate online resources and information. Teachers must model appropriate and creative digital citizenship as they navigate ever-changing digital landscapes. The school district's goals are to provide access to educational tools, resources, and communication, and to encourage innovation and collaboration. The school district's policies are intended to promote the most effective, safe, productive, and instructionally sound uses of these tools. Experimentation, evaluation, and synthesis in these environments are expected.

1. When you are online, you are a public figure. Be aware that information about you that is publicly posted online can be considered by the district.
2. Help the district be fiscally responsible. Use district server space only to save school-related resources.
3. We are a thoughtful, diverse community. Board policy prohibits the use of email to sell goods/services or to express political/religious views.
4. We pride ourselves on effective communication. Email should be brief. Anything requiring extensive explanation should occur via phone. Use the rule—"If it requires more than 2 emails to clarify, make a phone call."
5. The district maintains extensive records as required by law. All email is archived and can be recalled under subpoena. You only need to save sensitive email exchanges with parents or other stakeholders for one academic year.
6. Stay current. Please clean out your files regularly to ensure that you are not saving outdated instructional materials. Other documents (memos, files, budgets, etc.) should be retained for 5 years.

EMPLOYEE USER AGREEMENT

I acknowledge that I have received the School District of Springfield Township Acceptable Use of Technology Policy for Staff, recognize its importance, and understand this policy governs my use of the District networks and Internet. I have been instructed to read and adhere to the provisions of this policy. Additionally, I understand that if I violate the policy, I am subject to School District discipline and could be subject to ISP, as well as local, state and federal legal recourse. I agree to comply with the School District of Springfield Township Acceptable Use of Technology Policy for Employees.

Printed Name_____

Signature _____ Date: _____