FIVE STAR INTERLOCAL COOPERATIVE BOARD OF DIRECTORS POLICY	*Section VIII - Technology* Adopted: March 7, 2012 Revised: November 6, 2013

INTERNET AND TECHNOLOGY SAFETY PURSUANT TO THE CHILDREN'S INTERNET PROTECTION ACT

It is the policy of FSILC to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic or digital communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 U.S.C. §254(h)].

Definition

Key terms as defined in the Children's Internet Protection Act:

Access to Inappropriate Material - To the extent practical, technology protection measures (or "Internet Filters") shall be used to block or filter Internet (or other forms of electronic or digital communications) access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

Any individual who uses FSILC resources to access the Internet or engage in any electronic or digital communication is required to participate in FSILC's education efforts (undertaken pursuant to the Children's Internet Protection Act) and comply with FSILC's acceptable use policy.

Supervision and Monitoring

All employees are responsible for supervising and monitoring student use of the Internet in accordance with FSILC's technology policies and the Children's Internet Protection Act. The IT director shall establish and implement procedures regarding technology protection measures. No individual will be permitted to use FSILC's technology resources in a manner inconsistent with FSILC's policies.

Personal Safety

Employees and students shall not use FSILC's technology resources in any manner that jeopardizes personal safety. Students and employees must follow FSILC technology policies, including the acceptable use policy which details FSILC's safe use standards.

FIVE STAR INTERLOCAL COOPERATIVE BOARD OF DIRECTORS POLICY	*Section VIII - Technology* Adopted: March 7, 2012 Revised: February 6, 2013 Revised: November 6, 2013

ACCEPTABLE USE OF INTERNET AND ELECTRONIC AND DIGITAL COMMUNICATIONS DEVICES

The forms of electronic and digital communications change rapidly. This policy addresses common existing forms of electronic and digital communication (email, texting, blogging, tweeting, posting, etc.) but is intended to cover any new form of electronic or digital communication which utilizes a computer, phone or other digital or electronic device.

As a part of the resources available to employees, FSILC provides Internet access at its administrative offices. FSILC intends for this resource to be used for educational purposes and not to be used for conduct which is harmful. This policy outlines FSILC's expectations regarding Internet access. The ability to access the Internet while on FSILC property is a privilege and not a right. Access cannot be granted until an individual has completed an "Internet Access Agreement" and access may be revoked at any time.

Any individual using FSILC resources to engage in electronic or digital communications has no expectation of privacy. Further, employees must be cognizant of the fact that electronic or digital communications which occur on private equipment are often permanently available and may be available to FSILC administrators.

Employees are expected to use good judgment in all their electronic or digital communications - whether such activities occur on or off campus or whether the activity uses personal or FSILC technology. Any electronic or digital communication which can be considered inappropriate, harassing, intimidating, threatening or bullying to a FSILC, or school employee or student - regardless of whether the activity uses FSILC equipment or occurs during school/work hours - is strictly forbidden. Employees face the possibility of penalties, including termination, for failing to abide by FSILC policies when accessing and using electronic or digital communications.

The Internet provides users the ability to quickly access information on any topic - even topics which are considered harmful to minors. FSILC has attempted to filter this access in order to protect individuals from harmful content. In the event inappropriate material is inadvertently accessed, a report should be made to the supervisor. No individual is permitted to circumvent FSILC's privacy settings by accessing blocked content through alternate methods. In the event an employee needs access to blocked content, he/she should make arrangements through the director.

Although FSILC has taken appropriate steps to block offensive material, users may unwittingly encounter offensive material. All users of FSILC's electronic resources are required to exercise personal responsibility for the material they access, send or display, and must not engage in electronic conduct which is prohibited by law or policy. No

individual is permitted to access, view or distribute materials which are inappropriate or create a hostile environment.

Internet Access - Terms and Conditions.

Employees agree to access material in furtherance of educational goals, including research and professional development. Employees are also permitted to judiciously use FSILC's electronic resources for limited personal use, provided that the use is of no cost to FSILC, does not preempt business activity, impede productivity, or otherwise interfere with work responsibilities. Electronic or digital communications made using FSILC owned equipment must be professional in nature and cannot be used for the exercise of the employee's free speech rights.

Any electronic or digital communication in which the employee can be identified as an employee of FSILC – regardless of whether the communication is made with FSILC owned equipment or during work hours - must be a professional communication. Accordingly, if the individual is identifiable as a FSILC employee, electronic or digital communications must not contain sexual, harassing, discriminatory or immoral content. Further, the communication cannot promote the use of tobacco, drugs, alcohol or be otherwise inconsistent with FSILC's objectives.

Employees are required to maintain appropriate electronic boundaries with students. Such boundaries require that employees refrain from engaging in electronic or digital communications which show an undue interest in select student(s), are of a personal nature, model inappropriate conduct, or are otherwise inconsistent with FSILC's mission and goals. In order to maintain appropriate boundaries, FSILC encourages employees to:

- Send group texts or emails
- Use separate personal and school electronic accounts
- Obtain written parental permission prior to posting pictures of minors
- Respect individual privacy, including privacy rights granted by FERPA

Employees are expressly forbidden from using electronic or digital communication in a manner inconsistent with their position as a role model for students. Any employee who engages in inappropriate electronic or digital communication with students is acting outside the scope of his/her employment with FSILC.

Prohibited Use. Users specifically agree that they will not use the Internet to access material which is: threatening, indecent, lewd, obscene, or protected by trade secret. Users further agree that they will not use FSILC's electronic resources for commercial activity, charitable endeavors (without prior administrative approval), product advertisement or political lobbying.

Privilege of Use. FSILC's electronic resources, including Internet access, is a privilege which can be revoked at any time for misuse. Prior to receiving Internet access, all users will be required to successfully complete an Internet training program administered by FSILC.

Internet Etiquette. All users are required to comply with generally accepted standards for electronic or digital communications, including:

a. Appropriate Language. Users must refrain from the use of abusive, discriminatory, vulgar, lewd or profane language in their electronic or digital communications.

b. Content. Users must refrain from the use of hostile, threatening, discriminatory, intimidating, or bullying content in their electronic or digital communications.

c. Privacy. Users understand that FSILC has access to and can read all electronic or digital communications created and received with FSILC resources. Users agree that they will not use FSILC resources to create or receive any electronic or digital communications which they want to be private.

d. System Resources. Users agree to use FSILC's electronic resources carefully so as not to damage them or impede others' use of FSILC's resources. Users will not:

- install any hardware, software, program or app without approval from the director
- download large files during peak use hours
- disable security features
- create or run a program known or intended to be malicious
- stream music or video for personal entertainment

e. Intellectual Property and Copyrights. Users will respect others' works by giving proper credit and not plagiarizing, even if using websites designed for educational and classroom purposes (*See* www.copyright.gov/fls/fl102.html) Users agree to ask the director for assistance in citing sources as needed.

Limitation of Liability. FSILC makes no warranties of any kind, whether express or implied, for the services provided and is not responsible for any damages arising from use of FSILC's technology resources. FSILC is not responsible for the information obtained from the use of its electronic resources and is not responsible for any charges a user may incur while using its electronic resources.

Security. If a user notices a potential security problem, he/she should notify the director immediately but should not demonstrate the problem to others or attempt to identify potential security problems. Users are responsible for their individual account and should not allow others to use their account. Users should not share their access code or password with others. If a user believes his/her account has been compromised, he/she must notify the director immediately. Any attempt to log on to FSILC's electronic resources as another user or administrator, or to access restricted material, may result in the loss of access for the remainder of the school year or other disciplinary measures.

Vandalism. No user may harm or attempt to harm any of FSILC's electronic resources. This includes, but is not limited to, uploading or creating a virus or taking any action to disrupt, crash, disable, damage, or destroy any part of FSILC's electronic resources. Further, no user may use FSILC's electronic resources to hack vandalize another computer or system.

Inappropriate Material. Access to information shall not be restricted or denied solely because of the political, religious or philosophical content of the material. Access will be denied for material which is:

a. Obscene to minors, meaning (i) material which, taken as a whole, lacks serious literary, artistic, political or scientific value for minors and, (ii) when an average person, applying contemporary community standards, would find that the written material, taken as a whole, appeals to an obsessive interest in sex by minors.

b. Libelous, meaning a false and unprivileged statement about a specific individual which tends to harm the individual's reputation.

c. Vulgar, lewd or indecent, meaning material which, taken as a whole, an average person would deem improper for access by or distribution to minors because of sexual connotations or profane language.

d. Display or promotion of unlawful products or services, meaning material which advertises or advocates the use of products or services prohibited by law from being sold or provided to minors.

e. Group defamation or hate literature, meaning material which disparages a group or a member of a group on the basis of race, color, sex, national origin, religion, disability, veteran status, sexual orientation, age, or genetic information or advocates illegal conduct or violence or discrimination toward any particular group of people. This includes racial and religious epithets, "slurs", insults and abuse.

f. Disruptive of FSILC operations, meaning material which, on the basis of past experience or based upon specific instances of actual or threatened disruptions relating to the information or material in question, is likely to cause a material and substantial disruption of the proper and orderly operation of FSILC activities or business.

Application and Enforceability. The terms and conditions set forth in this policy shall be deemed to be incorporated in their entirety in the Internet Access Agreement executed by each user. By executing the Internet Access Agreement, the user agrees to abide by the terms and conditions contained in this policy. The user acknowledges that any violation of this policy may result in access privileges being revoked and disciplinary action being taken, including termination of employment.

INTERNET ACCESS AGREEMENT

Employee Name: _____

Position: _____

School or Site: _____

Home Address: _____

Home Phone No.: _____

I have received a copy of the policy titled *Acceptable Use of Internet and Electronic and Digital Communications Devices*. I have read and agree to abide by its provisions. I understand that any violation of the use provisions may result in disciplinary action including suspension and/or revocation of network privileges as well as any discipline allowed by law including termination of employment.

_____ _____

Employee Signature Date

FIVE STAR INTERLOCAL COOPERATIVE BOARD OF DIRECTORS POLICY	*Section VIII - Technology* Adopted: March 7, 2012 Revised: November 6, 2013

PERSONAL WIRELESS DEVICES

FSILC requires that all individuals devote their full attention to education while at school or during work activities. Accordingly, FSILC expects employees to limit their use of personal wireless devices at work. Wireless devices include, but are not limited to, cell phones, laptops, recorders, etc.

Personal wireless devices shall be turned off and out-of-sight in locations such as restrooms, locker rooms, changing rooms, etc. ("private areas"). The use of any audio/visual recording and camera features are strictly prohibited in private areas. Employees who observe a violation of this provision shall immediately report this conduct to the director.

Personal wireless devices may only be used during work time if the use of the device furthers the employee's performance of his/her professional responsibilities. No employee may use work time to engage in any personal electronic or digital communication, Internet activity, gaming, etc. Employees will make reasonable efforts to use FSILC or assigned school site resources rather than personal wireless devices for electronic or digital communications with other employees, parents, and students.

No individual may use any personal wireless device while operating a FSILC vehicle or while conducting FSILC business in a personal vehicle.

Personal wireless devices may not be used to photograph or record conversations or events outside private areas without first obtaining consent to record from all parties. In the case of students, permission from the building principal of the assigned site must be obtained. Administrative approval for recordings of students will take into consideration whether prior approval has been granted from parents/guardians and whether the recording would identify a specific category of students such as special education students.

Personal wireless devices may only be shared with students for emergency use.

No employee may use a personal wireless device to engage in conduct which is illegal or which could be construed as inappropriate conduct with a student or students. In the event an employee receives an inappropriate electronic or digital communication from a student or parent, the communication must be promptly reported to the director.

FSILC fully acknowledges that personal wireless communications devices are the personal property of the employee. Unless the director has reasonable suspicion that an employee's personal equipment contains prohibited content, the director may not inspect an employee's personal equipment without the employee's express consent.

Warning: Possessing, taking, disseminating, transferring, or sharing obscene, pornographic, lewd, or otherwise illegal images, photographs, or communications, whether by electronic data transfer or otherwise (commonly called texting, sexting, emailing, and other modes of electronic or digital communication) may constitute a CRIME under state and/or federal law. Any person possessing, taking, disseminating, transferring, or sharing obscene, pornographic, lewd or otherwise illegal images, photographs, or communications will be reported to law enforcement and/or other appropriate state or federal agencies, which may result in arrest, criminal prosecution, and inclusion on sexual offender registries.