



WiredTrust's "Socially Safe" and "Socially Safe Kids" Best Practices Seal Programs

The Socially Safe Seal and Socially Safe Kids Seal are offered by WiredTrust and cover cybersafety and best practices for Web 2.0 sites, interactive digital technologies, tools and features and their related services, games, products and networks (any of the foregoing, a "Community Technology"). The Socially Safe Seal is for all general audience, teen (that are not primarily directed at tweens or preteens) Community Technologies and those that only permit users who are thirteen years of age or older. The Socially Safe Kids Seal is for Community Technologies directed primarily at tweens and preteens. Both seals now also cover marketing companies involved in marketing and promotions to tweens and teens.

In order to qualify for the Socially Safe Seal and/or the Socially Safe Kids Seal, an applicant must demonstrate that they already meet, or must adopt and adhere to, best practices for their market segment. This includes adopting and articulating internal operation policies and creating external guides for key stakeholder groups, as specified, for its Community Technologies. It also includes vetting internal staff and outside providers to make sure that risk managers and customer service personnel are selected, trained, supervised and managed in the right way. In addition, they must provide certain information to WiredTrust and updates of that information throughout the term of the Seal.

The Socially Safe best practices guidelines require that the site, network or provider know its users and customers and how their Community Technologies are used. They must understand the stakeholders impacted by their site, network, product or service and identify and address their privacy, safety and communication needs. Socially Safe seal holders must create an internal operation that ensures consistency in customer service and communications. (Too often the safety and security of users depends on which moderator or customer service representative addresses their problem or questions, rather than being a system-wide consistent response.) High risk issues should be handled by risk management personnel trained to address them in the appropriate manner, and escalation policies must be adopted to make sure that reports and problems identified by the network are steered to the right high risk escalation team members. Triaging of reports and identified risks must be built into their moderation and abuse report systems. And data must be maintained for a minimum time to permit responses to be audited and legal access to data for investigations.

Each Socially Safe Seal holder must have a process in place for law enforcement investigations and inquiries and written guide explaining that process place. They must have addressed the issues of illegal activities and content and created a special communication process for confirmed members of law enforcement who are investigating active cases or who need information regarding the Seal holder's practices, technologies and data retention for official inquiries. The more interactive a Community Technology is, or the more UGC the Community Technology permits to be shared at the site, the more stringent the standards to address the increased risks.

While the priority is always safety, WiredTrust is practical too. It takes into consideration the size and duration of operation of the Community Technology, as well as its projected risks. (Experts at WiredTrust have been advising the industry, government, law enforcement and the public in these matters since 1995 and can usually forecast risks, as well as identify solutions.)

Start-ups, especially when their user-base is low, have a lower “Threat Profile” by the nature of their size and reduced start-up activity. Once their user-base increases, their obligations to adopt more stringent policies and procedures does as well. Established Community Technologies with smaller adoption rates and those that do not permit UGC or collect location or offline contact information from their users have fewer obligations than their larger counterparts. The Community Technology track record is reviewed as well. Have they been the subject of government regulatory action? Has a COPPA seal program notified them of COPPA violations? Have they had adverse media or attacks from non-profits or user groups? Each of these is evaluated for the purposes of setting the right level of risk-management and best practices standards for each applicant.

Community Technologies directed at children and preteens must be the safest of all, with those directed at teens a close second. Vulnerable demographic groups (such as sexual abuse survivors, cancer patients and special needs groups) and sensitive themes (such as racial or religious topics, abortion and birth control and political debates) are more often targeted online and Community Technologies used by or directed to them must have higher risk management solutions as well. Reports of high-risk activities, such as suicide threats, cutting and self-mutilation, eating disorders and bomb threats, must be handled with the assistance of subject matter experts and specially-trained high-risk moderation staff.

WiredTrust will review the business models, operations, compliance and risks management history and audience of the Seal applicant to help determine the right standards for that Community Technology provider and which levels should apply. Risks are balanced for each applicant in making that determination. Where and how are they operating? How large is their staff? What is the nature of their Community Technology? What is their target demographic? What data do they collect, how and how long is it stored? Is the Community Technology provider an entity with a proven risk management track record, or new to the industry? All of these are reviewed and evaluated and used to help identify the right set of best practice standards that apply to the Community Technology.

The Seal Application Process:

When an applicant seeks a Socially Safe or Socially Safe Kids Seal for its Community Technologies, it will contract with WiredTrust to complete an audit of its current status and to help bring it into compliance with best practices during a defined Qualification Period. The audit will require applicant to complete several detailed questionnaires. These are used to compile a disclosure report which must be certified by an officer of the applicant to its accuracy.

WiredTrust Team Members will review the disclosures looking for, among other things, risks, practices and policies (internal and external), methods of operation and consistency. WiredTrust may also, in its discretion, conduct independent tests and probes of the Community Technologies. Once the audit is complete, WiredTrust will advise the applicant of the outcome of the audit, including all changes, additions or deletions that must be implemented in order to bring the Community Technology into compliance with the WiredTrust Socially Safe Standards. Upon confirmation that all necessary requirements have been met, the applicant will be issued the appropriate Seal for a one-year term, subject to the WiredTrust Seal Participation Agreement terms and conditions.

In most cases the same requirements will apply to Community Technologies that fall into a category and size. In special situations, WiredTrust may grant an exemption temporarily or for the Seal period based upon its review of the risks, circumstances and the reasonability of the exemption request.

Once awarded, the Seals may be displayed on packaging and products (and in certain approved situations, in marketing and promotions) that comply with the Socially Safe Seal requirements, under the conditions set forth in the Seal Program. The Socially Safe Seals can apply to digital games, gaming networks and virtual worlds, social networks, mobile technologies, parental control technologies, communication tools and features, applications and devices, as well as any technological feature, product or service that permits interactive communications, user-generated content, networking and engagement.

Community Technology Categories:

Applicants will be categorized according to the Community Technologies' audience type, size and any other relevant or unique features. All applicants' Community Technologies will be required to meet the applicable Seal Requirements for that category and their size. Smaller sites and start-ups are given exemptions from certain requirements, such as having to engage special risk managers. And sites that do not collect contact information or IP information from their users may be able to avoid having a 24/7 law enforcement response and liaison. If a Community Technology provider believes that certain requirements are onerous or should not apply to them, given their operations or audience, WiredTrust will review their request for exemptions or customized solutions. These will be granted only in WiredTrust's sole and absolute discretion and must always address the goal of safety, security and responsible use. Some may only be granted temporarily.

Many of the Socially Safe Seal applicants are innovators in technology and may not fit precisely into a pre-existing category. Those Community Technologies that involve unique goods, services, business models, applications, etc. may be required to meet certain additional or customized Seal Requirements warranted by their categorization and/or the nature of their Community Technologies.

Audience Demographic Categories:

- GA "General Audience" sites do not specifically target children or teens. They do not ask the age of their users. Examples include CNN, Yahoo, MSNBC and ESPN. Their content is not specifically designed to attract minors as a group. A General Audience site will have to abide by general best practices, but will not have to address specifically issues unique to teens, children or high risk users unless special circumstances exist.

- GA13+ "General Audience" sites have a significant and known percentage of teen users. They ask for users' age and require them to represent that they are at least 13 to join or to access certain site features. If they don't ask for age, they may have a special section of the site or network directed at minors. While they may market to teens or have a teen section they have a broad user-base of adults (which may include a broad user-base of college students or young adults) as well. Examples of GA13+ sites include Facebook, MyYearbook and MTV. A General Audience 13+ site will have to abide by general best practices and address additional issues particular to the teen/minors age group, including school and parental policies and guides. They must also employ customer service or moderation personnel trained in high risk teen issues. Privacy settings must include a "do not disturb" setting, allowing the teens (or all users) to block all friend requests.

- TA "Teen Audience" sites target a predominantly teen audience of between 13 and 16 years of age. Examples of TA sites include Seventeen Magazine, eSpin and BeingGirl. Teen Audience sites will

have to abide by general best practices and address additional issues particular to this age group, including school and parental policies and guides, and teen safety tutorials. They must also employ customer service or moderation personnel trained in high risk teen issues. Privacy settings must include a “do not disturb” setting, allowing the teens (or all users) to block all friend requests.

PA “Preteen Audience” sites target a predominantly preteen audience of children under age 13. Examples include Webkinz, Club Penguin and Nickelodeon. Preteen Audience sites will have to abide by general best practices and be compliant with COPPA (assuming COPPA applies to their operations), as well as with additional best practices requirements for younger audiences. They will also have to provide school and parent policies and preteen safety tutorials, as well as a preteen Code of Conduct. They must also employ customer service or moderation personnel trained in communicating with preteens and with high risk preteen issues. Privacy settings must include a “do not disturb” setting, allowing the preteens to block all friend requests.

These Community Technologies must qualify for the Socially Safe Kids Seal, and are not eligible for the Socially Safe Seal unless they also have a substantial GA, GA13 or TA audience.

HR “High Risk” Sites that target a high-risk demographic (for example, battered women, cancer survivors, etc.), are related to a heavily-regulated industry (gambling or healthcare providers) or focus on a high-risk topic (for example, health issues, financial issues, suicide, addiction, etc.) will be categorized as high risk because of the increased likelihood of harassment and possible victimization and vulnerability of their users. The High Risk category also includes technologies and sites designed to provide a platform for potentially abusive conduct (for example, “Honesty Box” or the former JuicyCampus.com site.) High Risk sites and technologies will have to abide by general best practices as well as additional requirements based upon best practices tailored to the particulars of their high-risk classification.

Size and Status Categories:

- Start-up (within one year of launch and up to 800,000 unique users)
- Start-up (within one year of launch and 800,000 and more unique users)
- Start-up (within one year of launch and 1,500,000 unique users)
- Existing under 800,000 unique users (more than one year since initial launch)
- Existing 800,000 to 2,000,000 unique users (more than one year since initial launch)
- Existing 2,000,000 to 6,000,000 unique users (more than one year since initial launch)
- Existing 6,000,000 to 15,000,000 unique users (more than one year since initial launch)
- Existing 15,000,000 to 35,000,000
- Existing 35,000,000 and more unique users (more than one year since initial launch)

Note that WiredTrust may modify some of these requirements to adapt to the unique business model of the seal applicant or the special risks or risk management solutions in use by that applicant. These requirements can be changed at any time and from time to time, on 30 days’ written notice to any Seal Participant.

Last updated: October 1, 2009