



The WiredTrust Socially Safe Seal Program

The Socially Safe Seal covers cybersafety and best practices for participant sites, services, games, products and networks (any of the foregoing, a “Community Technology”). It is not a COPPA seal, such as those offered by ESRB, CARU and Truste.

It is much broader in scope and certifies its holders as among those who know and care enough to do it right, inside out.

In order to qualify for the Socially Safe Seal, the Community Technology must adopt and articulate internal operation policies and create external guides for key stakeholder groups, including law enforcement, general audience users and, if applicable, celebrities and VIPs. If the Community Technologies have users 16 years of age or younger, they must also have parent and school internal policies and external guides.

If they permit users under the age of 13 from the US, they must include cybersafety and privacy information written for the younger user. If COPPA applies to the Technology Community, they must also prove compliance with COPPA (such as holding a COPPA FTC-qualified seal) or retain WiredTrust or other professionals to bring them into compliance. Content filters or other risk management mechanisms to moderate communications must be in place to address cyberbullying, self-harm, sexual exploitation, radicalization threats and inappropriate content or communications.

Moderators and customer service team members must be properly vetted and supervised with background checks, and be trained in handling the kinds of risks encountered with the Community Technologies. Escalation procedures must be in place to enable high-risk reports to be handled by managers trained in those risks. Relationships must exist between the Community Technology and reputable subject matter experts in each of the relevant high-risk areas, either directly or through WiredTrust. Written policies must address all applicable high-risk issues, approved responses and actions, as well as the chain of escalation and command for each.

When a Community Technology seeks a Socially Safe Seal it must complete several lengthy questionnaires and certify as to their accuracy. WiredTrust reviewers review the disclosures looking for risks, practices and policies (both internal and external), methods of operations and consistency. They may also conduct independent tests and probes of the Community Technology. Once the audit is complete, the applicant is advised of the outcome of the audit and what needs to be changed, added or deleted to bring the Community Technology into compliance with its standards.

Certain changes to the participant’s practices, policies and programs must be communicated to WiredTrust throughout the term of the Socially Safe Seal (which is one year, the “Seal Term”). These relate to items that change the risk factors, or how those risks are addressed, as well as those involved with the Community Technology. The audit, the one year Socially Safe Seal applicable to the Community Technology (assuming its requirements are satisfied, and handling affirmative reports of changes during the Seal Term are included in the first year fee.

The Community Technology must retain user data for at least 6 months and assign someone within the enterprise to address law enforcement inquiries and celebrity/VIP inquiries and, if applicable, parent and school inquiries. Contact information for inquiries from each of the special stakeholder groups – law enforcement and celebrities/VIPs and, if applicable, schools and parents must be made available to those communities through WiredTrust.

And for Community Technologies of a certain size that permit or facilitate the posting or sharing of user-generated-content or collect PII (personally identifiable information), or IP information, emergency inquiry email addresses and phones and fax lines must be manned 24/7.

In some cases there are clear best practice mandates. These include having someone or a group assigned to handle all law enforcement inquiries, addressing high-risk reports within 24 hours of receipt and retaining all data for at least 6 months. In others, the Community Technologies can set their own policies, as long as they have considered the issues and articulated their policies internally and externally and are consistent in their application. The privacy policy, terms of service and any code of conduct must be consistent with the other articulated policies, as well.

For example, if a Technology Community has a substantial user-base of teens 16 and under, they must have an internal parents' policy and related guide for parents. The decision about what the policy provides, such as whether information will be provided to parents upon inquiry, or whether an account, profile or post will be removed upon the request of a parent is within the Technology Communities' reasonable discretion. They may decide not to address parents' inquiries directly, asking them to work with their child directly. In such a case adding a line to the posted privacy policy that "information will only be provided to users." Or they can be responsive at varying levels to their inquiries. This is the Community Technology's choice. As long as the Technology Communities have considered the issues and are consistent in setting, enforcing and articulating their policy regarding parents' inquiries, it satisfies WiredTrust's best practices standards.

The same applies to school policies. School inquiries usually relate to a campaign of cyberbullying among students, or harassment of teachers and school personnel by students who create fake accounts or post hateful or defamatory information about them. There may be bomb or suicide threats made, which require quick and reliable information. The Community Technology can remove accounts, profiles or posts reported by the school, or not. They can provide information to the school, upon inquiry or not. The process can be as formal or informal as the Community Technology decides. The decision is theirs, as long as it is reasonable and reflected in the formal and informal policies and procedures.

Privacy settings must be available for all communication technologies and user-generated-content posts and profiles. How many privacy selections and communication settings the Community Technology uses and how they work is discretionary. But all must permit blocking of specific users and a setting that permits users to block all incoming "friend" requests or communications from others generally. WiredTrust calls this the "do not disturb" setting. Abuse reporting buttons must be available on all pages, but the abuse-reporting interface is up to the Community Technology to choose.

Risk management is knowing the risks, the likelihood of each and how to eliminate or reduce their occurrences. WiredTrust's audits help you understand the risks of most Community Technologies and be proactive in avoiding them or lessening their frequency. Education of users and, in the case of sites for minors, parents, caregivers and educational institutions is a crucial component of risk management. So, Socially Safe Seal holders must have cybersafety content on their publically-facing pages teaching the users how and what to report as abusive and when they should ask for help.

Socially Safe Seal participants are part of a very elite community. This community wants to handle data responsibly, maintain standards that lead the industry in safety, privacy and responsible use and keep their communities safe and secure. Being able to display the Socially Safe Seal applicable to their model helps them communicate that commitment to everyone who accesses their services, products, games, sites and networks.

Note: This document and the Socially Safe Seal Program requirements are copyrighted and protected by international intellectual property laws. In addition, they are subject to change at any time and from time to time. For the Socially Safe Seal requirements in place currently and applicable to any Community Technology, please contact WiredTrust directly through WiredTrust.com. This document was last updated September 14, 2009.