

This article may not be reproduced without the author's permission.

ELECTRONIC COMMUNICATION: LEGAL AND PRACTICAL ISSUES TO CONSIDER IN THE INFORMATION AGE

Charles R. Gregg, Private Attorney, and Catherine Hansen-Stamp, Attorney

Reprinted with adaptations from *The CampLine* by permission of the American Camp Association.

©2006 American Camp Association

I. Introduction

Outdoor recreation and adventure programs are now intimately familiar with the World Wide Web. Your organization probably has a Web site, reaching out to anyone around the world who has access to the Internet. The Web has catapulted your business into the spotlight in a low cost and accessible way. You and your staff have integrated electronic communication into your business, using e-mail and other electronic communication to conduct business and communicate with clients, associations, and other individuals or entities that relate to your business.

However, with the onset of this information explosion come many questions and issues, both legal and practical. How accurate is the message you offer on your Web site and present in other electronic communications? What is the effect of an electronic signature, particularly when you are dealing with parents and their minor children? What are your obligations, if any, regarding electronic communication sent and received by participants while active in your program, in a program-sponsored chat room, or after the program ends? We will address these and other issues as we explore the legal and practical ramifications associated with use of the Web.¹

II. Pre-Program

The flow of information between an organization and its potential participants and their families is essential to a good operation. This information exchange includes information provided by the organization and received by it. The Web provides a convenient method to engage in this two-way communication. Words, photos, video clips, and other graphic images can project the organization's image and personality, describe its mission and activities, and serve as an effective and inexpensive marketing tool. In addition, online registration information, including health information and participant agreements, can be available online, allowing prospects to respond without licking a stamp!

The practical value of this electronic information exchange is clear. Search engines and links to and from other Web sites can cast a broad net, allowing your message to be spread quickly and efficiently to the market. Electronic re-

trieval of information allows the organization to collect vital information from participants—obtaining registration and health information, payment, participant agreements, and corresponding electronic signatures on these “documents,” with the appropriate software in place.

The legal implications of this electronic information exchange are more complex. We will examine two areas in this pre-program exchange of information.

III. Marketing Information Provided to Participants and the Public

Your information, presented electronically or otherwise to the outside world, is a powerful tool. However, in the push to spread a positive marketing message, it is important to keep in mind the value of an accurate and balanced message.

An organization that presents a fair and accurate message to its participants will maximize the opportunity to educate and prepare them for the experience, avoiding surprises, disappointment, and unfulfilled expectations. If incidents occur, participants and their families who are psychologically prepared for the experience and who have been presented with a fair picture of the experience may be less likely to be critical of the organization, or to file a lawsuit.

On the other hand, electronic or other communication that contains exaggeration or guarantees, or inaccurate, unbalanced, and inconsistent information does not serve the interests of the would-be participant and can be extremely damaging to the organization, particularly in the event of an injury or loss. The bottom line is, representations and assurances in electronic form are as binding on an organization, and as likely to produce trouble—legal or otherwise—as those contained in written letters or brochures.

IV. Information Provided To and Collected From Participants and Their Families

Using the Web to collect information from and about your participants is a valuable tool. Organizations can provide registration information, including terms of enrollment, health information, questionnaires, and participant agreements on their Web site. Organizations can collect payment

and information without asking families to mail in a paper copy. Everyone is familiar with “clicking yes” to contract terms involving the purchase of products on the Web.

Electronic delivery and collection of information allow organizations a convenient and efficient way to deal with this traditionally paper-driven process and increase organizations’ ability to provide a quality experience. With appropriate software, electronically signed or delivered documents can easily and effectively be electronically stored or relayed to appropriate staff.

The legal issues related to collection of electronic information are more complex. The organization probably intends that important portions of this information exchange will serve as binding contracts. For example, the registration information may contain terms of agreement, including organization policy on refunds, cancellation, and registration. Health information and participant agreements may require participant or participant-parent acknowledgment or agreement. These documents may require signatures which you want and expect to be evidence of a binding agreement.

The Federal E-Sign Act² was created to legitimize electronic contracts. Among other things, the act provides that a contract cannot be found unenforceable simply because it is in electronic form. Of course, to be considered binding or enforceable, the contract, electronic or otherwise, must meet other basic contract requirements.

An important requirement of a legally binding contract is that there be successful contract formation—that is, there must be an offer by the organization and a valid acceptance or assent by the signing party. Developing case law in various jurisdictions reflects that electronic acceptance by the signer is a critical issue. Among other things, the individual clicking “yes” to contract terms should be provided with clear and unambiguous instructions on the nature of the contract and the process for acceptance of its terms. The signer should clearly understand that he/she is entering into a legally binding contract. The terms of the contract should be available to the signer on the Web, in conjunction with acceptance of those terms.

Another important issue is contract authentication—that is, verification that the individual electronically signing the document is who he or she purports to be. This is critical in the event the organization needs to rely on the electronic document to enforce its contractual rights. Consider the issues with minors, who are not legally competent to enter into a legally binding contract³. Although there may be some value in having the minor sign certain documents, the parent/s of the minor are usually required to sign documents such as registrations, health forms, and participant agreements. Even if the participant is an adult, authentication is important in the electronic context. Important safeguards can include seeking personal information from the signer and seeking e-mail verification from the signer following the organization’s receipt of electronically signed contracts.

Another issue is accurate information collection and

record keeping. An organization’s software or database should record accurate and important information in the electronic collection process and should have adequate storage and retrieval capabilities. In the case of binding contracts, critical information includes the who, when and what: 1) who signed the contract (contact information); 2) time and date of the electronic signature; and 3) the document or version of the document entered into.

Consider specific issues related to individual documents. For example, in addition to meeting the requirements for a binding contract, documents containing release or other liability shifting (exculpatory) language are subject to a second level of scrutiny by the courts. In most states, these documents are enforced only on a case-by-case basis and only if certain criteria are met. Consider too, that state law varies regarding whether a parent can legally release their minor child’s right to sue in the event of injury or incident at the organization. Thus, the presentation and content of this type of document, whether electronic or paper, must address these and any additional jurisdiction specific issues.

In light of the particular importance and sensitivity of these participant agreements, many organizations may choose to collect signed written documents rather than relying on electronic collection. A transition strategy may be to offer participants the option of completing either a written form or an online electronic version.

Although some of the issues organizations face in addressing the enforceability of binding electronic contracts are similar to those affecting more traditional forms of contracts, the Web presents a new twist regarding contract enforceability. Organizations should work with their legal counsel and Web designer or computer consultant to assess legal and technological issues as they consider increasing the online information exchange.

V. During Your Program

The matters of access to the Internet, entitlement to Internet messages received by the organization, and other electronic matters are best handled by establishing and publishing the organization’s requirements and expectations early in the relationship with the participant and family.

The organization may set the terms of a participant’s admission to the organization’s program, regulate what he or she brings to the program and how he or she behaves while in the program, and dismiss participants for a violation of organization rules. Accordingly, the organization can and should make clear, including the consequences of violations, its policies regarding digital cameras (including cell phones with that capability), access to and use of the Internet, and entitlement to personal messages received by the organization.

Internet issues will force a thoughtful consideration of where a line might be drawn between positive and negative experimentation with a participant’s freedom within a program. Internet opportunities abound which challenge

participant privacy and other issues. The organization must be aware of these issues and address them in a manner that is consistent with the organization's culture and values. The issue may be an iPod containing music which some might regard as suggestive and sexually provocative. It may be e-mails from parents or friends, received directly by the participant or by an organization's computer, BlackBerry or similar device, including material that organization management considers inappropriate for the participant. These and other Internet issues can have significant legal ramifications for the organization and its community. An organization's failure to proactively address these issues may, following an incident, result in anger, confusion, and even claims of a violation of some legal duty. This can include, for example, illegal interception of communications intended for the participant, invasion of privacy, or intentional or negligent infliction of emotional distress.

Each organization will have its own policies regarding participant use of electronic and wireless devices. Some organizations prohibit such devices. However, an organization which allows participants to bring equipment capable of making and transmitting photographs, may, preferably, with proper prior announcement, confiscate that equipment until the end of the program if it finds it is being abused. Organizations may have an "Internet Café" from which communications can be sent and received. Rules governing such a place, and the messages sent and received, must be clear and strictly enforced.

The organization cannot afford to appear to be a partner or collaborator with a participant or staff member who sends, electronically or otherwise, inappropriate messages or photo images of other participants. In addition to other clear rules or policies, the basic agreement between the organization and participant may include a statement that the organization is not responsible for publication of photos or other images taken by co-participants without appropriate consent and authority.

An organization may distribute none, all, some, or only filtered e-mails that come into the organization computer intended for a participant. The organization, working with the variety of special service providers and software programs (eOrganization, etc.), may negotiate methods for screening and rejecting unwarranted material, including a message of receipt and rejection. The organization office may receive all e-mails, review them, and select what e-mails will be sent to the participant. If the organization distributes e-mails, it should make it clear that their confidentiality cannot be guaranteed, thereby preserving an announced opportunity to screen. The organization office may refuse to receive and distribute any e-mails, or accept and deliver e-mails only from specified persons.

An attorney for the American Camp Association recently addressed the legality of an interception of e-mails directed to a camper, while at camp. Citing federal law (18 U.S.C.A. 2511), counsel opines that if the computer that receives the

e-mail is the property of the organization, the organization may do what it chooses with those e-mails. Mail is not being intercepted illegally and privacy rights are not being violated.⁴

Again, the organization's policies and practices in these areas should be made clear to the participants and their families in advance of the commencement of the program, to avoid surprises, disappointments, or later charges by a parent that the organization is interfering with an intended communication, privacy issues, and so forth.

To what extent interested persons are advised of such matters we will leave to the organization. But the organization is clearly within its legal rights to set the terms of admission and participation, including confiscation of offending property.

VI. Post-Program

Issues with the Internet continue after the program ends. We all have heard stories of chat rooms, blogs or other Web based arenas in which the organization experiences are shared and the organization community is extended, perhaps with expectations for the following summer. While such chat rooms can be productive in strengthening organization relationships, including staff to students, some of these relationships and communications may not serve the organization or participants well. In addition, comments may be made at these sites about program experiences which, accurate or not, may be detrimental to the image the organization wishes to project. The organization must not give the appearance of endorsing or promoting communications like these on the Web; yet it is next to impossible to monitor or control communications on the variety of sites that exist. The organization, on its own Web site or in other materials, can announce expectations for transactions in a chat room or blog controlled by the organization. It can also address issues about the use of other Internet sites (MySpace, etc.) and some of the problems associated with extending the organization's relationships beyond the controlled environment of the program itself. Even before activities begin, the organization should disclaim and be very clear about its lack of responsibility for—in fact its lack of ability to—monitor activities on a site other than a dedicated site it has created.

An organization's "captive" private chat room site, for example, should state clearly to participants and their families that the purpose of the chat room is to provide a forum for participants, and perhaps staff, to talk to one another. The organization can explain that it has no responsibility for, and does not expect to monitor, the site or to act upon matters that might be discussed there. If the organization does choose to monitor or control the site, it should describe the limits of its responsibilities, and penalties for misuse. An organization cannot afford to appear to be a sponsor of a communication that may offer inaccurate, offensive, or illegal material. The organization can be held responsible for what occurs on these sites if the organization might fairly be regarded as endorsing, promoting, or taking

on the responsibility for what is said and done.

At a private site it is quite easy for the organization to provide a disclaimer, even a “pop-up,” that will announce, periodically, the limits of the organization’s responsibility and its expectations for what is to take place. The site could be passworded to limit access to those people who have received sufficient warnings and a declaration of expectations. A private site may be an attractive alternative to the independent free-wheeling conversations that might take place otherwise. However, the organization surely will understand that regardless of its best intentions in sponsoring or offering a private site, some of the participants and alums will be attracted to other offerings on the Internet.

Some overly aggressive past participants or staff members may attempt to draw attention to their personal Internet offerings by including the organization logo or trademark patched in from the organization’s Web site or elsewhere. While this may be well intentioned, such use might cause parties to the communication to believe that the organization has a level of involvement in the communication that it does not have. Unauthorized use of the organization’s trademarks, including its logo, is illegal. An explanation and warning about such use can be included in a statement or disclaimer on the organization’s Web site.

The American Camp Association has some excellent publications addressing these issues, including those informing parents about sexual predators on the Internet and other dangers of unsupervised Internet conversations. See, for example, www.wiredsafety.org. See also “Their Space or Yours? Internet Issues Come to Organization” by Stephen G. Wallace, M.S. Ed., in the March 2006 issue of *Inside ACA* on www.ACAorganizations.org/inside or “Cyber-Shadows, Protecting Teens From the Dark Side of the Online World” by Stephen G. Wallace, M.S. Ed. on www.OrganizationParents.org. Recommendations made by the authors may not be suitable for all organizations, including the prospect of visiting Web sites and monitoring compliance. Undertaking to do so, and potentially publishing that intention, may create certain expectations that will be difficult to fulfill.

VII. Conclusion

Running a quality program includes thinking ahead on developing issues, and none are developing more quickly than cyber technology. Address these issues thoughtfully—before, during and after your program. Understand the issues, and work with professionals: legal counsel, computer consultants, staff, and your participants and their families to address and minimize problems presented in our electronic age.

**This article contains general information only and is not intended to provide specific legal advice. Organizations should consult with a licensed attorney experienced in recreation and adventure law regarding application of state and federal laws and issues specific to their business or operation.*

©Charles R. Gregg and Catherine Hansen-Stamp

Charles (Reb) Gregg is a practicing attorney in Houston, Texas, specializing in outdoor recreation matters and general litigation. He is an active speaker and author in the field of managing the risks of legal liability. He serves as general counsel to The Association for Challenge Course Technology and serves as counsel to numerous other education and adventure programs, including camps, schools, and others. Reb is a member of the Wilderness Risk Managers Committee and the Accreditation Committee of the Association for Experiential Education. He serves on the board of SCA, and is president of The Friends of Big Bend National Park. He can be reached at (713) 982-8415 or e-mail rgregg@gregglaw.net; www.rebgregg.com.

Catherine Hansen-Stamp is an attorney in private practice in Golden, Colorado. She consults with and advises recreation and adventure providers and related organizations on legal liability and risk management issues. She speaks and writes on these issues both regionally and nationally and has presented at the WRMC since its inception in 1994. She is a member of the Wyoming and Colorado Bar Associations. Hansen-Stamp can be reached at (303) 232-7049, or e-mail reclaw@hansenstampattorney.com; www.hansenstampattorney.com.

¹ Staff internet and electronic issues are not within the scope of this article. However, these issues are important and relevant, and include issues with staff postings on personal Web sites; review of electronic information available on prospective employees; restrictions on staff access to the Internet during the organization session; and staff contact with the organization after the session closes.

² Electronic Signatures in Global and National Commerce Act at 15 U.S.C. 7001, et seq. State laws may establish other or additional requirements for the enforceability of electronic documents (*and see* 15 U.S.C. 7002).

³ Other issues, including a minor’s ability to potentially ratify or disaffirm release language or other terms of a contract, are beyond the scope of this article.

⁴ Attorney Jason A. McNeil

WRMC 2008 Conference Proceedings



This article may not be reproduced without the author’s permission.