NATIONAL CLUB ASSOCIATION
50TH ANNIVERSARY
1961–2011

NCA CONNECT
NEWS. TRENDS. ANALYSIS.

VCT NCA's Official Strategic Communications Alliance Partner

In Policies We Trust

Protecting Your Club Through IT Policy

Published Wednesday, February 1, 2012
by Tom DeMayo

Technology. It saves time, keeps us focused on our business goals and ensures we remain competitive in the fast-paced world around us. It also can be misused if not implemented in a controlled manner.

Strong, clear technology usage policies can help maintain the confidentiality, promote the integrity and ensure the stability of a club's information and technology resources. When employees understand what the club expects of them, it can help minimize the club's risk exposure.

As I work with clients, big and small, it is apparent that IT policies, and sometimes policies in general, are where many organizations need the most help. Though clubs may have basic policies regarding Internet or e-mail usage, oftentimes these are just basic stock policies downloaded directly from the Internet.

In today's expanding technological landscape, it's important that clubs take the time to both develop comprehensive IT policies and actually enforce them in order to truly protect a club from risk.

As with any policy drafting process, when writing technology policy, clubs should consider certain key questions to ensure that the policy accomplishes its purpose:

1. Who is the audience?
2. What is the club trying to convey, and what are the ramifications of non-compliance?
3. Where can more information or assistance be accessed?
4. When is the policy effective?
5. Why are we implementing this policy?

These questions can help provide direction for your club's actual policy wording. When crafting the language of your club's policies, make sure that it's clear. One of the biggest mistakes businesses make is that the policies are not definitive and, appear open to interpretation. Words like "may" and "could" should be eliminated whenever possible. Policies should delineate the club's official position, instruct a user about user requirements, and convey that deliberate failure to conform to these policies will result in disciplinary action, up to and including, termination.

In terms of specific policy tenets, IT policies should clearly state that employees have no right to privacy and can have no expectation of privacy when using club-owned equipment and/or networks. The club should reserve the right to monitor, review, restrict, store and distribute employee communications at any time, without notification.

The more clearly a club conveys this reality to its employees, the better the business can protect itself from legal recourse should a disciplined or terminated employee file suit. Clubs should also consider implementing a log-on banner—a box employees will need to click before they can access the club's computers or network—to ensure employees re-acknowledge the club's right to monitor their technology usage and their lack of a right to privacy.

Though policies should be focus on protecting your club, they also need to be unbiased and sensitive to the civil liberties of your employees. When crafting your club's IT policies, do not be afraid to seek legal counsel. As technologies evolve, so do the associated legal complexities and challenges. Spending the money on legal consultation now will pale in comparison to the legal fees that could be spent as a result of poorly worded or planned policies.

Once your club has developed strong IT policies, written policies should be distributed to, and discussed with, new employees as part of the orientation process. Acknowledgement of receipt and a statement of agreement and understanding should be signed by the employees and stored in their respective personnel file. All policies should include the right of the employer to amend the policy at any time, as well as the recognition of e-mail as an acceptable means for the employer to disseminate updates and new policies.

Even once IT policies have been developed and distributed, the club's job doesn't end there. One in ten organizations that I've visited still used policies that were written more than ten years ago. Management needs to consider their IT policy as a living document. It will never be perfect, and there will always be room for improvement. Policies need to be reviewed and updated at least annually. At that time, organizations need to reflect on their policies and ask themselves the following questions:

1. Is this policy still relevant?
2. Is the wording of the policy reflective of our actual business practices?
3. Have there been any employee issues during the year that may warrant the need for a new policy?
4. Have new technologies been introduced that the organization needs to take a position on to protect its business?

Time spent now in developing clear, concise, definitive IT policies can avoid potential problems down the road. However, writing a policy, placing it in the employee handbook and forgetting about it is the biggest reason policies are not enforced, relevant, or all encompassing in the protection they provide.

For more information on areas that your club's IT policies should cover, as well as specific advice for each policy area, please see the accompanying article, "How to Draft Your Club's IT Policies."

Tom DeMayo is Manager of Information & Technology Services at PKF O'Connor Davies. He can be reached at tdemayo@pkfny.com.