NATIONAL CLUB ASSOCIATION
50TH ANNIVERSARY
1961–2011

NCA CONNECT
NEWS. TRENDS. ANALYSIS.

VCT NCA's Official Strategic Communications Alliance Partner

How to Draft Your Club's IT Policies

Published Wednesday, February 1, 2012
by Tom DeMayo

To protect your club from liability, be sure to develop usage rules in the following areas when crafting your club's IT policies:

- E-Mail
- Internet
- Remote Access
- Passwords
- Removable Media
- Social Media

Specific policies your club should consider implementing include:

E-Mail/Internet:

- Prohibit employees from transmitting or viewing content that could violate equal opportunity or discrimination laws.
- Forbid employees from transmitting or viewing e-mail messages of a sexual nature or containing racial, ethnic or other slurs. If an employee sends out a lewd message with your club's name on it, the club could be held liable.
- Instruct employees never to open e-mail attachments or links from unknown senders.
- Inform employees that deleted e-mail will not ensure confidentiality. Messages can be restored and archived.
- Inform employees that the club's systems are not in place for their personal business ventures.
- Do not prohibit employees from sending personal e-mails. Be realistic, but set terms and conditions as to what is and is not acceptable.
- Only authorized personnel should be permitted to transmit club-wide e-mails.
- Do not permit employees to send chain letters, jokes and political correspondence.
- Prohibit the streaming of any video or media that is not needed for business purposes.
- Have a clause or separate section regarding e-mail retention.

Passwords:

- Clearly define what the minimum password requirements are for all business systems and applications, including length, complexity, lockout, change frequency, etc.
- Require that employees keep passwords protected. No yellow sticky notes attached to the monitor. No exception to this rule for family and friends as well.
- Inform employees that passwords may be reset by management to access their systems and files if needed.

Remote Access:

- Prohibit remote access from kiosks or insecure public locations.
- If possible, limit remote access to business-owned and controlled systems.
- Require active antivirus scanning on the system used to connect.
- Require the connecting machine to have recent operating system and application security updates installed.
- Require the user to close the session when they are done and not leave the session unattended for any length of time.

Removable Media (USB drives, external hard drives, iPods, etc.):

- Take a position on whether or not removable media is acceptable in your club. If employees have no legitimate business need for the use of removable media, ban it. Removable media can introduce viruses and can be the biggest source of confidential data loss. Also keep mind, as innocent as an iPod may seem, it is still a hard drive that can either infect or steal information from a network.
- If you allow USB drives, specify if encryption is required.

Social Media:

- Define what the club considers to be social media.
- Clarify the club's position on the use of the club name on personal social media pages.
- Specify whether or not club supplied e-mail addresses can be used to create social media accounts.
- Remind employees that they represent the club. You do not want a client or business associate to search an employee name and easily obtain images and/or content that may place into question the integrity and quality of the club.

For more information on drafting your club's IT policies, please see the accompanying article, In Policies We Trust.

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