Cy-Fair Sports Association Acceptable Use Policy

Use of the Cy-Fair Sports Association (CFSA) Systems requires responsible judgment, supervisory discretion and compliance with applicable laws and regulations. Users must be aware of information technology security and other privacy concerns. Users must also be aware of and follow management directives for use of the CFSA Systems. Internet services provided by CFSA, like other CFSA equipment and resources that are part of the CFSA Systems, are to be used only for authorized purposes as determined by CFSA management. To this end, the restrictions outlined below regarding use of the CFSA Systems during official working hours and non-working hours should be followed by CFSA employees and volunteers using Internet services, Instant Message (IM) and telecommunications equipment provided by CFSA.

CFSA strives to maintain a workplace free of harassment and sensitive to the diversity of its employees and volunteers. Therefore, CFSA prohibits the use of computers and the e-mail system in ways that are disruptive, offensive to others, or harmful to morale. Harassment of any kind is prohibited. Messages with derogatory or inflammatory remarks about an individual's or group's race, religion, national origin, physical attributes, or sexual preference will not be permitted. For example, the display or transmission of sexually explicit images, messages, and cartoons is not allowed. Other such misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassment or showing disrespect for others.

Employees and volunteers should notify the VP of Information Technology and the President upon learning of violations of this policy. Employees and volunteers who violate this policy will be subject to disciplinary action, up to and including termination of employment or volunteer duties. The following specific statements reflect official guidance on CFSA employees' and volunteers' use of the CFSA Systems:

1. Users are individually responsible for understanding and respecting the security policies of the systems (computers and networks) they are using. Users are individually responsible for all use of resources assigned to them, and hence sharing of accounts and access to resources is strictly prohibited. Given the extreme vulnerability to viruses and other malicious software users are exposed to by use of the Internet, employees and volunteers must ensure that processes and procedures to minimize risk from malicious programs are in place. Virus checking software must be used in conjunction with Internet use.
2. The use of the CFSA Systems provided by CFSA during nonworking hours is not limited to official purposes only. However, employees and volunteers may not make excessive use of CFSA printers or supplies in conjunction with personal Internet and e-mail activities. Activities for which CFSA Systems may not be used, during working or non-working hours include, but are not limited to, the following:

    a) the pursuit of private commercial business activities or profit-making ventures (i.e., employees/volunteers may not operate a non-CFSA related business with the use of the CFSA Systems);
    b) matters directed toward the success or failure of a political party, candidate for partisan political office, or partisan political group;

c) use of profanity or inappropriate language in e-mail;
d) use of a CFSA user account by anyone but the authorized owner of the account;
e) sending or posting discriminatory, harassing, or threatening messages or images;
f) sending or posting confidential material, trade secrets, or proprietary information outside of CFSA;
g) engaging in unauthorized transactions that may incur a cost to CFSA or initiate unwanted Internet services and transmissions;
h) sending or posting messages or material that could damage CFSA's image or reputation;
i) participating in the viewing or exchange of pornography or obscene materials;
j) sending or posting messages that defame or slander other individuals;
k) attempting to break into the computer system of another organization or person;
l) refusing to cooperate with a security investigation;
m) sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities;
n) using the Internet for religious activities or any sort of gambling;
o) jeopardizing the security of CFSA's electronic communications systems;
p) sending or posting messages that disparage another organization's products or services;
q) passing off personal views as representing those of CFSA;
r) sending anonymous e-mail messages;
s) any violation of statute or regulation;
t) utilizing proxy avoidance software or websites to hide or mask internet activity;
u) disabling software or services installed or enabled by the IT Department;
v) cancelling or otherwise blocking the installation of security patches and updates;
w) installing Peer-to-Peer (P2P) software or utilizing P2P websites/networks.

3. The equipment, services, and technology provided to access the Internet remain at all times the property of CFSA. As such, CFSA reserves the right to monitor Internet traffic, and retrieve and read any data composed, sent, or received through our online connections and stored in our computer systems.
4. Modifying or otherwise altering CFSA provided hardware and equipment, including laptops, Desktops, and communications devices is prohibited.

Revision History

12/23/15 Document created, Will Morse
03/03/16 Document reviewed, Scott Huntsman