



YMCA

We build strong kids,
strong families, strong communities.

THE GREATER DAYTONA BEACH AREA YMCA



COMPUTER AND SECURITY GUIDELINES

Updated 01-17-07

SECTION I: Use of Personal Computers (PC), Laptops & ICA Workstations

1. YMCA employees are encouraged to use the computer system in accordance with the YMCA's mission and policies.
2. Computer privileges are extended to all full-time staff, administrative part-time staff and by special request to other designated staff.
3. Each YMCA facility has a designated number of stations available for staff use, and the distribution is determined by the Branch Executive Director.
4. Each employee has a particular Security Policy applied to their login, which limits their access to certain applications on the system (discussed in more detail later in this policy document).
5. Each employee using the YMCA computer system is responsible for the proper use of the computer. Proper use includes but is not limited to:
 - a. No beverages or food near the components
 - b. No unplugging of components unless instructed to do so by IS staff
 - c. Proper logging on and off procedures
 - d. No excessive or destructive force applied to any of the components
 - e. Proper application of the Security Policy that is included in this policy document
6. Only YMCA work-related tasks should be performed on the equipment. All personal tasks should be kept to a minimum and only done with the permission of your supervisor. This includes but is not limited non-work-specific e-mail, school work, internet surfing, stock trading, and conducting any other kind of personal business on-line.
7. No one may modify or destroy any hardware, software or data.
8. All employees must use the printer and printing supplies conscientiously. Each user should perform periodic cleaning of the User Directory, i.e. deleting outdated files, old emails and unknown files.

SECTION II: Security Policy Related to End Users

1. Each employee receives a personal password-protected login, which determines his or her access to the system.
2. Employees are **NEVER** to give their password to any other person. Every file your login accesses, edits, deletes, etc. is tracked! If an audit is performed, it is YOUR login that is assigned the responsibility, and therefore YOU become responsible, whether you were using it at the time or not.
3. There are four (4) available Policies assigned by level of authority: IS (Information Systems) Administrator, Executive/Manager, Office/Program Director, and Front Desk.
4. It is unacceptable for any employee to violate U.S. or Florida law, including but not limited to copyright laws and licensing agreements. ***Violation of these laws is grounds for immediate dismissal.***

5. Employees may **NOT**:
 - a. Download text files, software, executable files, and databases to disk drives.
 - b. Download viruses – follow the guidelines for opening attachments and floppy use contained in this policy.
 - c. Harass other employees, volunteers, members or guests, including the intrusive display of graphics and offensive text or sending unwanted email.
 - d. Attempt to evade the YMCA system security.
6. YMCA IS Administrator reserves the right to:
 - a. Delete any files or email from the system.
 - b. Impose time limitations on the idle time of an employee's login.
 - c. Monitor any employee's activity and use of data, files, internet or email.
 - d. Alter any employee's security, permissions or privileges without prior notice.

Section III: The Greater Daytona Area YMCAs Internet and Email Use Guidelines

1. Access to the Internet is limited to Executives, Managers and specially approved staff.
2. It is provided for the benefit of the organization and its members.
3. Every full-time and other approved employees have access to Email. This allows employees to connect to information resources around the world.
4. Every employee with access has a responsibility to maintain and enhance the organization's public image and to use the internet and email systems in a productive manner.
5. **Acceptable Uses** of Internet and Email:
 - a. Employees accessing the Internet are representing the company. All communications will be professional.
 - b. Employees are responsible for ensuring that the Internet and Email systems are used in an effective, ethical and lawful manner.
 - c. Internet Relay Chat channels may **ONLY** be used to conduct official company business, or to gain technical or analytical advice.
 - d. Databases may be accessed for information as needed.
 - e. Email should be used for business and professional communications. Keep personal use to a minimum.
6. **Unacceptable Uses** of Internet and Email:
 - a. To prevent computer viruses from being transmitted through the system, **no** unauthorized downloading of any software is allowed. **All** software downloads will be done through the IS department.
 - b. Personal email accounts (i.e. Yahoo, Hotmail, etc.) are not to be accessed across the internet.
 - c. Copyrighted materials belonging to entities other than the YMCA may not be transmitted by staff members on the Internet. One copy of copyrighted material may be downloaded for your own personal use in research. Users are not permitted to copy, transfer, rename, add or delete information or programs belonging to other users unless given express

permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action up to and including dismissal from the YMCA and/or legal action by the copyright owner.

7. ***All Users agree not to engage in any activity:***

- a. Which may cause harm to any of the material or software components that make up the Internet; and
- b. Which attempts to compromise or thwart the security of any account, host or network on the Internet; and
- c. Which interferes with activities of any user, group, host or network on the Internet, including, but not limited to:
 - i. The transmission of material harmful to other systems, such as a virus, Trojan horse or worm attempting to circumvent authentication or security of any Internet host, network or account
 - ii. Forging email
 - iii. Sending large numbers of unsolicited mail messages
 - iv. Forwarding or posting "chain letters"
 - v. Repeated posting of inappropriate messages to a group of users (spamming)
 - vi. Attempting to masquerade, cancel, or otherwise interfere with email other than one's own
 - vii. Engaging in any activity which aims to reduce the effectiveness of an Internet service
 - viii. Engaging in harassment, whether through language, volume or size of emails.

8. YMCA IS Staff reserve the right to:

- a. Revoke any staff person's Internet or email access.
- b. Monitor any employee's activity on the Internet and through email.
- c. Remove History, Temporary Files, Cookies, Favorites, Deleted, Sent and Archived emails after a certain period of time or of a certain size.

Section IV: YMCA BLOG and PERSONAL WEB PAGE Guidelines

1. Our YMCA believes in fostering a thriving online community and acknowledges blogging as a valuable component of shared media.
2. Any employee who blogs should be aware that all the information published on a blog or public website (including personal pages on sites such as MySpace, Friendster, and to a degree Face-book) is public accessible. Posting information on these pages is conceptually similar to sending a letter to the editor in a newspaper; once published, it is openly accessible.
3. Employees are advised to be mindful that the information they post on the internet will likely be seen by members of the YMCA community and could reflect poorly on your character.
4. As an organization that holds personal character in the highest regard, the YMCA is obligated to take actions to preserve its core values.
5. As such, the YMCA may terminate staff members for publishing public web pages and blogs that are contrary to the YMCA's mission or are detrimental to its community.

6. Employees' non-disclosure obligations and legal responsibilities are listed in the following five (5) paragraphs. Failure to abide by these guidelines may result in disciplinary action, up to and including dismissal from YMCA employment.
 - a. **Legal Liability** – When you choose to go public with your opinions via a blog, you are legally responsible for your commentary. Individual bloggers can be held personally liable for any commentary deemed to be defamatory, obscene, proprietary, or libelous (whether pertaining to the YMCA, individuals, or any other entity). For these reasons, bloggers should exercise caution with regards to exaggeration, colorful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterizations. In essence, you blog (or post on the blogs of others) at your own risk. Outside parties can pursue legal action against you for postings.
 - b. **YMCA Privileged Information** – Any confidential, proprietary, or trade secret information is obviously off-limits for your blog. The YMCA logo and trademarks are off-limits per our YMCA and Y-USA's brand guidelines. Anything related to YMCA members, programs, policy, strategy, financials, products, etc. that has not been made public cannot appear in your blog under any circumstances. Disclosing confidential or proprietary information can negatively impact our YMCA and may result in regulatory violations for the YMCA.
 - c. **YMCA Code of Conduct** – All of our employees are required to sign the YMCA Code of Conduct. *Blogs that violate the YMCA Code of Conduct will result in disciplinary action up to and including dismissal.*
 - d. **Unsanctioned Contact** – Specifically, in the YMCA Code of Conduct, employees agree to no contact with YMCA-related children apart from YMCA programs. If you receive e-mail or blog entries from any children whom you know from YMCA programming, you should contact your supervisor. Any response to the children is in violation of your no-contact promise to the YMCA and may result in disciplinary action up to and including dismissal. If you do receive such a communication, you should determine how the child obtained your e-mail or blog address and correct the deficiency and block further correspondence.
 - e. **Press Inquiries** – Blog postings may generate media coverage. If a member of the media contacts you about a YMCA-related blog posting or requests YMCA information of any kind, contact the President/CEO or the Vice President of Operations at the Corporate Office. You must clarify whether specific information has been publicly disclosed before you blog about it.

Section V: VIOLATIONS of Usage, Security, Internet & Email Policy

1. Any Greater Daytona Beach Area YMCA employee violating any portion of this policy will be advised of the appropriate section and directed to comply.
2. The YMCA leadership and IS Administrator reserve the right to terminate network access for employees who repeat a violation after a previous warning.
3. The YMCA leadership and IS Administrator reserve the right to prohibit violators from future access to or use of the YMCA's system.

4. The YMCA leadership and IS Administrator stress that any extreme misuse of equipment, software, email, internet or data could be grounds for dismissal, *even on the first occurrence*.

Section VI: Virus & Email Attachments

1. More than 53,000 virus threats exist today. In the war against viruses, information and communication are our weapons. The IS department will do its best to keep all users informed.
2. However, the YMCA and IS department rely on each employee/IS user to help keep the system free of viruses, bugs, worms, Trojan horses and other “critters”.
3. ***Be Aware:***
 - i. Some viruses can sit on a file for months and then be activated on a certain date.
 - ii. We used to be able to say, "Don't open any attachment that ends in .EXE." However, now they are sending viruses attached to files with ".txt", ".vbs", ".doc". They can figure out a way to destroy your data, consume your email address book, or wreak havoc with our whole computer system.
 - iii. We have a comprehensive Anti-Virus program, but it can only find and remove viruses once it has been updated. We update once a day, but any new viruses in that 24-hour period could get onto our system!
4. ***Things Each Employee can do to Help Prevent Viruses From Hurting Us:***
 - i. ***Never*** open an email attachment that you do not know what it is ***EXACTLY***...it could be from someone you know, yet the virus has infiltrated that person's address book. Forward any suspicious attachment to “**! Computer Problems !**”.
 - ii. ***Never*** bring in a file from a disk or CD where the disk or CD has not been scanned first. Most of the non-email viruses have been introduced into our system by disks from home or other sources. “**! Computer Problems!**” email can assist with Virus Scanning.
 - iii. If you get a warning that you have a virus – **STOP!** Call the IS Administrator immediately and describe the warning. It may not be too late to prevent it from entering or damaging our system!
 - iv. If you have ***any questions or concerns*** about the integrity of your computer, internet or email, call the IS Administrator immediately.



YMCA

We build strong kids,
strong families, strong communities.

The Greater Daytona Beach Area YMCA Acknowledgement of Receipt of the Computer & Security Guidelines

Employee's Name (please print): _____

Title: _____ Branch: _____

I acknowledge that I have received the Computer and Security Guidelines, including guidelines on the use of Blogs and Personal Web Pages, and that I have read and understand this acknowledgement. I understand that I have the opportunity to ask my supervisor, the Human Resources Director, and/or the Information Systems Administrator questions about both, and I fully understand that I am responsible for reading, understanding and adhering to the contents of both as they relate to my use of computers and the YMCA's information systems, as well as my employment with the Greater Daytona Beach Area YMCA. I understand that violations of proper computer use, as set forth in this document, can be grounds for disciplinary action, up to and including dismissal.

Employee's Signature

____/____/____
Date

This signed receipt will be retained in the Association's Human Resources Office as part of the employee's official personnel file.