

**AMERICAN ARABIC BENEVOLENT ASSOCIATION**  
**PO Box 320037**  
**West Roxbury, MA 02132**

**COMMUNICATION & TECHNOLOGY POLICY**

---

The following policy is hereby adopted this \_\_\_\_\_ day of \_\_\_\_\_ 2006, which addresses employee use of the American Arabic Benevolent Association's communication and computer systems.

The American Arabic Benevolent Association (hereinafter referred to as "AABA") and any AABA affiliated or controlled companies are subject to this approved Communication & Technology Policy.

Communications and computer systems are vital to conducting company business. The AABA's communications and computer systems are any equipment, hardware, software or networks owned, provided or used by or on behalf of the AABA that store or transmit voice or non-voice data. This includes telephones, cellular/wireless telephones, voice mail, computers, e-mail, facsimiles, pagers and AABA Intranet or Internet access. [see **Attachment A** for additional clarifications]

**1. Access, Maintenance and Protection**

Employees will safeguard the confidentiality and integrity of the AABA systems (including access codes, password logons, password protected screensavers, log-on IDs) from improper destruction, access, alteration, and disclosure. Employees will only access or use these systems when authorized.

**2. Unlawful and Inappropriate Use**

Employees will never use the AABA systems (such as the Intranet or Internet) to engage in activities that are unlawful, violate the AABA policies or in any way that would:

- a. Be disruptive, cause offense to others, or harm morale.
- b. Be considered harassing or discriminatory or create a hostile work environment.
- c. Result in the corporation's liability, embarrassment, or loss of reputation.

**3. Protection and integrity of Data**

Employees will maintain the integrity of the AABA information and data stored on the AABA systems by:

- a. Only introducing accurate and truthful data into the AABA's system that serves a legitimate AABA purpose.
- b. Only acquiring, using, altering, disposing of, or destroying data or information with proper authorization.
- c. Protecting data and information stored on or communicated across the AABA's systems and not accessing this data or information unless authorized.

- d. Protecting data and information communicated over internal or public networks (for example, the Internet) to avoid compromising or disclosing sensitive information or communication.

#### **4. *Communicating Unauthorized Messages***

Employees will not use the AABA systems to communicate inappropriate/unauthorized messages, data, or information.

#### **5. *Personal or Unauthorized Use***

Employees understand that while the AABA systems are intended for business purposes, limited personal use is permissible, as long as the use does not:

- a. Interfere with work responsibilities.
- b. Lead to inappropriate costs to the AABA.
- c. Involve interests in personal outside business and/or other non-authorized organizations and activities (which may include, but not be limited to selling personal property/items or soliciting for or promoting commercial ventures, charitable, religious, or political activities or causes).

#### **6. *Virus Protection***

Employees will check all electronic media, such as software, diskettes, CD-ROMs, and files for viruses when acquired through public networks (for example, the Internet) or from outside parties, using virus detection programs, prior to installation or use. If the employee suspects a virus, he/she will not use the applicable computer system and equipment until the virus is removed and will report the matter immediately to his/her supervisor and/or the AABA's IT Director.

#### **7. *Properly Licensed Software***

Employees will only use approved and properly licensed software, as determined by the authorized AABA IT Director and will use it according to the applicable software owner's license agreements.

#### **8. *AABA Monitoring***

The AABA communication and computer systems, including, but not limited to, computer networks, data files, e-mail, and voice mail, may be monitored and/or accessed by the AABA to protect against fraud and abuse, to ensure the integrity of the technology, detect unauthorized access or use, and for other business purposes.

#### **9. *Inappropriate use of e-mail includes, but is not limited to, sending or forwarding:***

- a. Messages, including jokes or any language, that may be considered discriminatory, harassing, unlawful, defamatory, obscene, offensive, insensitive, or otherwise inappropriate (including messages about age, race, gender, disability, sexual orientation, national origin or similar matters).
- b. Pornographic or sexually explicit materials.
- c. Chain letters or gambling.
- d. Information related to religious materials, activities or causes, including inspirational messages unless authorized by the AABA.
- e. Charitable solicitations.
- f. Auction-related information or materials unless sanctioned by the AABA.

- g. Games or other software or copyrighted materials without a legitimate AABA purpose.
- h. Messages that disparage other companies or services they render.
- i. Large personal files containing graphics materials or audio files (such as photographs and music].
- j. Materials related to personal commercial ventures or solicitations for personal gain (for example, messages that could be considered pyramid schemes).
- k. Information related to political materials, activities, or causes unless sanctioned or permitted by the AABA.
- l. Unauthorized or inappropriate mass distribution of communication.

**10. *Inappropriate use of the Internet includes, but is not limited to, sending or forwarding information about, or downloading (from):***

- a. Sexually explicit, harassing, or pornographic sites.
- b. “Hate sites” or sites that can be considered offensive or insensitive.
- c. Auction or gambling sites.
- d. Non-AABA business related chat sites.
- e. Underground or other security sites which contain malicious software and/or instructions for compromising.
- f. Games, software, audio, or other materials that the AABA is not licensed or legally permitted to use or transmit or that are inappropriate to the AABA business.
- g. Offensive or insensitive materials, such as sexually or racially oriented topics.
- h. Intentional importation of viruses.

A violation of any of the above may be grounds for disciplinary action up to and including dismissal.

Policy Adopted by the American Arabic Benevolent Association, Inc. Board of Directors:

SIGNED:

Kenneth J. Raffol – President	/     / DATE
Camille Sarrouf, Sr., Esq - Clerk	/     / DATE
Rosanne Solomon – Recording Secretary	/     / DATE

## ATTACHMENT A

### **Definitions:**

Authorized/Authorization – written or verbal approval/permission from a Supervisor or other management individual.

Properly Licensed Software – software installed by an authorized individual, as determined by the AABA’s IT Director, for use on the AABA’s computer system.

Improper/Inappropriate – not suitable for, or consistent with, the purposes or circumstances intended by a Supervisor or with AABA policy.

Sensitive Information/Communication – data files, e-mails, voice messages pertaining to work or operations of a delicate nature.

Unauthorized – not justified by proper authority

### **Q&A Samples:**

Q1. My friends and family occasionally communicate with each other over e-mail. Is it appropriate for me to use the AABA’s computer to participate?

A1. Generally the AABA systems are intended for business purposes. Limited personal use of e-mail and the Internet may be allowed if approved by your Supervisor and it conforms to the AABA standards indicated in the Policy. Inappropriate use may overload the AABA’s systems, tie up needed resources, and damage the AABA’s reputation.

---

Q2. I received permission from my Supervisor to use the AABA’s computer for personal use. May I download games to my computer?

A2. Authorized limited personal use still requires you to comply with all AABA standards regarding inappropriate use of e-mail and the Internet.

---

Q3. A friend came to my office to visit and asked for my password so he could log in and use my computer to look up some AABA information. Is this ok?

A3. Employees must safeguard the confidentiality and integrity of AABA information and data stored, including password logons, from improper access.

---

Q4. I received data from another organization, as requested by my Supervisor, and stored the information on the AABA’s computer system. May I open up the file and print it out for him?

A4. Employees will maintain the integrity of AABA information and data stored on AABA systems by protecting data and information stored on the AABA's system and not accessing this data unless authorized.

---

Q5. I bought some software for my home computer and have the license. May I load it on my assigned AABA computer after I have checked that there is no virus?

A5. An employee will only use approved and properly licensed software. While employees are to check software using virus detection programs prior to installation, only the AABA's IT Director may approve the use or installation of any software on the AABA's systems.

**EMPLOYEE ACKNOWLEDGEMENT FORM**

I acknowledge that I have received and read the AABA’s “COMMUNICATION & TECHNOLOGY POLICY”, along with Attachment A. I understand my responsibilities concerning the use and access of the AABA’s communication and computer systems.

\_\_\_\_\_  
Employee Name [please print]

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Witnessing Supervisor [please print]

\_\_\_\_\_  
Witnessing Signature

\_\_\_\_\_  
Date