PERSONNEL
USE OF NJSBA COMPUTERS,
SOFTWARE, E-MAIL AND INTERNET

Use of NJSBA's Computer System

Suspected employee use of NJSBA's computer system for reasons deemed unacceptable under the NJSBA policy may result in the employees Department Director requesting the Executive Director, in writing, to monitor the employees' use of the NJSBA computer system, including internet usage. If approved, the Executive Director will provide specific directives to the Director, Human Resources to monitor the employees' use of the NJSBA computer system for a specific period of time. The Director, Human Resources will provide a written summary of the employees' computer activity inclusive of the internet to the Executive Director and the employees Department Director.

Random Monitoring

As outlined in the policy, the Association retains the right to monitor and record internet use. Abuse of the NJSBA computer system is grounds for disciplinary action and may also be punishable under state and federal law. The Executive Director may provide specific directives to the Director, Human Resources to randomly monitor employee use of the NJSBA computer system including the internet. The Director, Human Resources will provide the Executive Director a written summary of the employees computer use, including the internet.

Periodic Password Resets

Every 60 days the network server will prompt employees to change their password when attempting to log into the network. Employees will be responsible for selecting and maintaining their password each time it is changed. User passwords should be protected and kept in a secure place and should not be listed on the employee's computer monitor, telephone, on scrap paper, etc. These passwords should not be shared with anyone, except when the NJSBA IT department requests it for purposes of upgrading or enhancing the employee's computer or when the Department Director requests it for the purposes aligned with carrying out the duties/functions of the Association in the absence of the employee.

Information Technology User Password Responsibility

While performing daily tasks, employees of the NJSBA Information Technology Department may, either inadvertently or by necessity, have access to or be able to read confidential personnel information. IT staff are required to keep confidential all such information. These instances are only to occur as part of the IT Department's job-related duties. Any additional means of an IT Department staff member accessing an employee's computer, LAN account, e-mail or Internet files would be in violation of policy GO/4146.6, unless authorized and approved by the Executive Director.

NJSBA User Data Storage

Employees must save all NJSBA documents and files to the appropriate network drive. This will prevent the breach of any confidential material, as well as ensure the integrity of all data in the event that an employee's

desktop computer is not functioning.

Use of Association e-mail

The following procedures govern the use of Association e-mail:

A. All messages shall pertain to legitimate NJSBA concerns.

B. Staff shall not send or forward any messages that contain material that a reasonable person may find obscene, defamatory, racist, sexist, or promote illegal or unethical activity.

C. Staff shall not send or forward chain letters, junk mail, jokes, pictures or any other material unrelated to NJSBA business.

D. A staff member will seek approval from his/her director before sending an email to all staff.

E. When replying to an e-mail, staff shall respond to the individual sender whenever possible and avoid sending a “reply to all.”

F. A staff member shall consult with his/her director if unsure whether a particular e-mail conforms to these guidelines.

Issued: January, 2000

Revised: January, 2001
November 19, 2002
July 14, 2005
February 22, 2006
March 2008