5-6 POLICY ON INFORMATION SYSTEMS POLICIES AND PROCEDURES

A. Physical Security of Computer Assets

Employees will ensure that all computer assets (Computers, Monitors, laptop computers, printers, etc.) that are assigned to or regularly used by them are maintained and used in a manner consistent with the equipment's function and such that the possibility of damage and/or loss is minimized.

Desktop computer equipment will not be removed from SYCAMORE PARK DISTRICT premises without prior authorization from the Executive Director or his/her designee. Employees will not modify SYCAMORE PARK DISTRICT computer equipment in any manner including, but not limited to, attaching external disk drives, external hard drives, changing the amount of memory in a computer, and attaching/installing any peripheral device.

Some portable computing equipment (laptop computers, PDAs, Electronic organizers, etc.) will be maintained under the direct supervision of the employee/department to which it is issued.

Computers, as well as other electronic equipment should never be left in/near extreme temperatures. For this reason, as well as the possibility of theft, laptop computers and the like should not be stored overnight in a vehicle.

Any electrical or mechanical malfunction of equipment should be reported to the immediate supervisor or Executive Director without delay.

B. Maintenance of Computer Assets

Employees are individually responsible for keeping their PC; it's components and the surrounding desktop clean and in good repair. The desktop and floor should be kept clear of substances and debris that could accidentally spill on critical components such as the keyboard, mouse, printers, and the like.

C. Workstation/Laptop Maintenance

Employees should leave their Workstations powered on but log off their account each night. Laptop users will need to have them connected overnight on Thursdays whenever possible for updates to be applied.

D. Ownership of Information, Data, and Software

Definition of Data: Any computer information, including, but not limited to, information that has been entered into a computer, stored in a computer, or retrieved from a computer. Examples would include spreadsheet and database entries. All information and data generated or gathered by an employee, in the course of their employment and/or utilizing SYCAMORE PARK DISTRICT owned assets, shall be the exclusive property of SYCAMORE PARK DISTRICT. No information or data shall be transferred to, given to, or loaned to any other organization or outside individual except for those instances where it is in the approved course of business for SYCAMORE PARK DISTRICT.

All software purchased by, licensed by, or created by SYCAMORE PARK DISTRICT is the exclusive property of SYCAMORE PARK DISTRICT and may not be transferred to, given to, or loaned to any other organization or outside individual without the express written authorization of the Executive Director or his/her designee.

E. Access to Computer Information and Hardware

All computer related resources under the control of SYCAMORE PARK DISTRICT exist for the furtherance of SYCAMORE PARK DISTRICT business pursuits. SYCAMORE PARK DISTRICT may inspect or monitor any SYCAMORE PARK DISTRICT owned, leased, or controlled computer, computer device, network, computer facility, or storage device at any time for any reason. This includes the inspection of e-mail (incoming, outgoing, or stored) and the monitoring of Internet usage. SYCAMORE PARK DISTRICT may divulge any information found during such inspections or monitoring to any party it deems appropriate.

The use of encryption, the labeling of an e-mail or document as private, the deletion of an e-mail or document, or any other such process or action, shall not diminish SYCAMORE PARK DISTRICT's rights in any manner.

F. Information Security

Sensitive or Confidential information is any information in any form, that is a business advantage to SYCAMORE PARK DISTRICT in any way. This includes participant lists, pending contracts, claims and investigation files, legal documents, loss control materials and SYCAMORE PARK DISTRICT financial information. Information belonging to participants or prospective participants also applies.

A common method for gaining access to computer networks is for the hacker to impersonate a contracted information systems employee. They will call an employee with a story that they need the employee's ID and password. Once they have these, they are well on their way to breaking into the network. Contracted agents of any information systems departments will never call an employee and ask for a login ID and or password. Employees should never disclose their login or passwords to anyone except for the Executive Director. Employee IDs and/or passwords should not be written down and kept within the general area of the computer. Employees may not access, in any manner, unassigned computer equipment unless that person is specifically authorized to.

The loss of any computer equipment of any of the SYCAMORE PARK DISTRICT's information should be immediately reported to the Executive Director who will immediately ensure that all possible steps are taken to protect SYCAMORE PARK DISTRICT from further information loss and loss of assets.

All information created by, obtained by, or utilized by employees in the course of their employment is the exclusive property of the SYCAMORE PARK DISTRICT. Even when physically able to, employees will not access any information other that that which they are specifically authorized to and is necessary for the performance of their assigned duties. SYCAMORE PARK DISTRICT information may be utilized for the benefit of other organizations within reason, i.e., surveys, participant registration totals.

Extreme care should be taken when dissemination of information that is Sensitive or Confidential. In this case, it is required that the Executive Director be consulted for clarification on Sensitive Confidential matters. The Sensitive or Confidential information is encrypted in a computer file, or otherwise sealed in an envelope or appropriate container. The transmittal letter or e-mail text includes a warning to the recipient that the material is Sensitive or Confidential and is the property of SYCAMORE PARK DISTRICT. A copy of the transmittal letter or e-mail should be archived by the employee.

All employees will ensure that their computer files are properly backed up. SYCAMORE PARK DISTRICT work files (network drives) are backed up nightly, local hard drives are not.

All computers will have antivirus software installed. This software is to remain activated at all times.

G. Installation and Use of Software

Software piracy is utilizing software in violation of its licensing agreement. Without the prior written authorization of the Executive Director or his/her designee employees shall not install any software on SYCAMORE PARK DISTRICT owned computer equipment, install SYCAMORE PARK DISTRICT owned software on non-owned SYCAMORE PARK DISTRICT computer equipment or provide copies of SYCAMORE PARK DISTRICT owned or licensed software to anyone.

Employees will not engage in any acts of software piracy. The Executive Director shall ensure that all software installed or utilized on SYCAMORE PARK DISTRICT machines is properly licensed.

H. Personal Use of Computer Hardware/Software

Employees may utilize SYCAMORE PARK DISTRICT owned hardware and software for personal use within reason. Such use should not take place during normal business hours, except during lunch, occasional rest breaks or before/after personal flextime hours of work; should not interfere with SYCAMORE PARK DISTRICT needs or operation and should be purely personal and many not be for any commercial purpose. In addition, the employee must comply with all laws and regulations and usage should not include political activity, pornography, sexist material, racist material, or any illegal act or any other inappropriate behavior.

Examples of allowable use include typing a letter, making a meeting flyer, or updating a budget spreadsheet. Others include sending e-mail to a family member or friend or accessing the internet to search for material.

SYCAMORE PARK DISTRICT may purge files on its computer at anytime without notice. SYCAMORE PARK DISTRICT is not responsible for any personal files or outside project files that may be purged or lost.

B. Electronic Mail and Internet Usage

SYCAMORE PARK DISTRICT's e-mail system and internet access is intended to further the business purposes of SYCAMORE PARK DISTRICT. Personal use of the e-mail system and internet access is permissible within reason and should be limited to the time frames as indicated above (Personal Use of Computer).

All information created, sent, or received via SYCAMORE PARK DISTRICT computers, networks, internet access, and/or email system is the property of SYCAMORE PARK DISTRICT.

SYCAMORE PARK DISTRICT reserves the right to monitor, filter, and/or review, at any time, any all internet utilization and e-mail created, sent, or received via SYCAMORE PARK DISTRICT's computers, networks, internet access and/or e-mail systems. SYCAMORE PARK DISTRICT further reserves the right to reveal the contents of such e-mail and Internet access information to any party that it deems appropriate. The use of encryption, the labeling of communication as private, the deletion of communication, or any other such process or action, shall not diminish SYCAMORE PARK DISTRICT's rights in any manner. Employees have no right of personal privacy in any matter stored in, created, received, or sent over the SYCAMORE PARK DISTRICT e-mail system.

SYCAMORE PARK DISTRICT will disclose e-mail and internet access information to any party that it may be required to by law or regulation. This may include law enforcement search warrants and discovery requests in civil litigation.

Even though SYCAMORE PARK DISTRICT has the right to retrieve and read any e-mail messages, those messages should still be treated as confidential by other employees and accessed only by the intended recipient Employees are not authorized to retrieve or read any e-mail messages that are not sent to them. Any exception to this policy must receive the prior approval of the Executive Director or his/her designee.

Due to potential security breaches, employees will exercise extreme caution in executing any files attached to e-mail. If the attachment seems odd, is not clearly business related and/or expected from a known source, it should never be opened or executed. Employees should never download files from the Internet or accept e-mail attachments from outsiders without first scanning the material with virus checking software. If you are unsure of certain e-mails or attachments, contact the Executive Director.

Employees will not subscribe to any e-mail lists that are not directly relevant to their assigned duties. Employees will not post any comments or statements on any web page or send any messages to the Internet newsgroups without written authorization from the Executive Director or his/her designee. Employees should not enter any Internet chat rooms, chat channels, bulletin board services and the like unless this action is related to work. Employees should not download software form the Internet unless prior approval has been obtained from the Executive Director or his/her

designee. Management approval is required before anyone can post any information on commercial on-line systems or the Internet.

Any approved material that is posted should obtain all proper copyright and trademark notices. Extreme care should be taken when e-mailing information that is Sensitive or Confidential as discussed above (Information Security).

Each employee is responsible for ensuring that their use of SYCAMORE PARK DISTRICT's e-mail system and internet access is consistent with this policy, any other applicable SYCAMORE PARK DISTRICT policy, and appropriate business practices. SYCAMORE PARK DISTRICT's policies against sexual or other harassment apply fully to the e-mail system, and any violation of those policies is grounds for discipline up to and including dismissal. Therefore, e-mails shall not contain offensive jokes, pornography, sexist remarks, racist remarks, defamatory remarks, obscene remarks, anything of a commercial nature not pertaining to SYCAMORE PARK DISTRICT business, anything of a political nature, or any other classification protected by law. Further, the e-mail system shall not be used for any purpose in violation of law or regulation.

Chain Letter e-mail will not be created or forwarded. Employees will carefully review all e-mail prior to sending it to ensure that their meaning is clear and not subject to interpretation. E-mail messages should be composed in a professional manner. Comments that would be inappropriate in memorandums and letters are equally inappropriate in e-mails.

Employees should be mindful that internet sites collect information about visitors. This information will link the employee to SYCAMORE PARK DISTRICT. Employees will not visit any site that might in any way cause damage to SYCAMORE PARK DISTRICT's image or reputation. In the event that you unintentionally access such a site, please inform your immediate supervisor.

Employees should be aware that some of the material available on the internet is copyrighted or trademarked. Other than viewing publicly available material, employees will not use any material found on the Internet in any manner without first establishing that such use would not be in violation of a copyright or trademark. Internet sites usually make visitors aware of the law as well as options for securing permission to purchase/use images, etc.

Employees may not use SYCAMORE PARK DISTRICT's internet connection to download games or other entertainment software, including but not limited to wallpaper and screensavers, to play games over the internet, music, etc.

Employees will not reveal their e-mail passwords to anyone except for the Executive Director. Employees will not utilize or access e-mail accounts belonging to any other employee.

Users should routinely delete outdated or otherwise unnecessary e-mails and computer files.

Violation of the Information Systems Policies and Procedures may result in disciplinary action up to and including dismissal.

Adopted on:

Revised on:
November 2021