21.01 Computing Devices

Policy:

It is the policy of Licking/Knox Goodwill Industries, Inc. to provide portable mass storage and computing devices to approved staff members to assist employees in completion of their job duties.

Procedure:

Definition - Portable mass storage and computing devices are defined as an electronic device capable of copying or saving data to or from a computer. Examples include, but is not limited to, laptops, notebooks, tablets, PDAs, MP3 players, memory cards, floppy disks, zip disks, CDs, DVDs, cellular devices, USB Flash Drives (also known as zip drives, thumb drives, jump sticks, or USB keys) and desktop computers.

Personal Devices - Personal portable mass storage and computing devices brought to the workplace may not be connected to any Licking/Knox Goodwill, computer, network, or Internet connection.

- Employees may use their personal computing or mass storage devices while on rest or lunch breaks as long as the devices do not interfere with employee job duties or responsibilities and are not connected to Goodwill systems.
- Goodwill will not be liable for the loss of personal devices brought in to the workplace.

Company Provided Devices - Portable mass storage and computing devices issued to employees by the agency are to be used for company business only. Under no circumstances may agency-owned devices be borrowed by non-employees or contract customers. Devices may not be shared between contracts or employees.

- Employees in possession of company owned portable mass storage and computing devices are expected to protect the equipment from loss, damage or theft. Issued equipment is the sole responsibility of the authorized employee.
- All devices shall be inventoried and must be returned upon resignation, termination of employment, extended time off, or transfer to another position. Employees unable to present the device in good working condition are expected to report this information to the Director of Facilities.
- Transfer of any equipment must follow Policy & Procedure 11.20, *Fixed Assets-Inventory*.
- Devices in need of service or repair must follow Policy & Procedure 21.09, *Technology Repair and Disposal.*
- It is the responsibility of individual users to back-up their data to the fileserver on a regular basis. Portable mass storage devices have a higher failure rate than a laptop or desktop computer. Data recovery can be costly and sometimes impossible. This service may only be ordered at the discretion of the Director of Communications, the division director and the CEO/President.

Security of Data –

- All individuals using USB Flash Drives are required to password protect their data. Drives which are not capable of password protection should be replaced.
- Passwords for USB Flash Drives, computers and telephones must be provided to the Director of Facilities. All passwords should be changed in accordance with Section 21 Policy, *Passwords*.
- Unattended workstations must be secured by logging off or locking. Office doors must be closed and secured when unoccupied for any length of time.
- Mobile devices containing confidential information, including tablets, notebooks, laptops and cellular phones, must be physically secured and password-protected at all times.
- All company computing devices will be equipped with continually executing and approved virus-scanning software that includes a current virus database.
- Email attachments received from unknown users must be thoroughly scanned by approved virus-scanning software before opening.
- Taking work home on a company provided USB Flash Drive is discouraged. Any such use should be of an incidental nature and must be approved by the appropriate division director or CEO/President.
- Freeware, copyrighted, or licensed software is not permitted to be copied or installed to any portable mass storage or computing device by the user. All software is to be installed and maintained by a member of the Technology Committee.
- Any employee attempting to make illegal copies of software or confidential documents is subject to disciplinary action up to and including termination.
- Computing devices must be secured with password-protected screensavers with an automatic activation feature set at 15 minutes or less.