Access to Electronic Resources
Policy Number: LS 306
Effective: April 2021

Purpose

Tampa-Hillsborough County Public Library provides access to a wide range of electronic resources. This policy governs how these resources are to be utilized and managed.

Policy

The Internet enables the Library to provide information beyond the confines of its own collection. The Tampa-Hillsborough County Public Library Board (the Library Board) upholds and affirms the right of each individual to have access to constitutionally protected material. Users are encouraged to be good information consumers by carefully evaluating material accessed via the Internet. The Library subscribes to a variety of online databases. Identification, selection, and review of these databases are managed as outlined in the library's Materials Selection Policy.

While the Library cannot control or monitor all material available on the Internet, the Library Board has determined to guard against providing access to visual depictions which are not constitutionally protected, to protect children from access to visual depictions which are obscene, child pornography, or harmful to minors as such terms have been defined in the Children's Internet Protection Act and approved by the courts.

Customers are responsible for using the Library computers in accordance with this policy and the Library Code of Conduct. The Library Board has elected to use filtering software in conjunction with firewall technology to manage Internet access on all library computers. Library customers may request that library staff review any website, either blocked by the filter or not. Customer Request for Review of a Website forms are made available to customers at all Public Service Desks. (See LS307, Request for Review of a Website).

Parents are responsible for monitoring their own children's use of library materials and electronic resources. In order to assist parents, the library offers an internet safety training program for children. The safety program teaches children how to safely navigate the Internet and to recognize dangers that may be encountered online. Completion of this training program is required before anyone under 17 years of age may access the Internet

on library computers. This requirement will only be waived on the request of parents via a signed authorization form.

Confidentiality of library registration and circulation records are governed by Florida Statutes Chapter 257.261. In accordance with this law, computer sign-in sheets are shredded as soon as all customers listed have been served or at the end of the day, whichever occurs first. The Library is not responsible for the content found on other websites, for any failure in transmission of online applications or forms to other agencies, or for accurate submission of forms or information. The Library cannot guarantee that other agencies receive forms or information submitted from library computers or act on them appropriately. No agreement or contract is created between the customer and the Library or its staff. The Library uses best efforts to ensure network security. Nevertheless, the customer assumes all responsibility for the use of the library's network and networked resources, including interference with the customer's data, laptop computer, or other devices.

The Library is not liable for the loss or compromise of any confidential or sensitive, or any other information, or for any and all damages resulting from that loss. The Library computers are equipped with software that erases all customer entries and activities when the computer is restarted after each use.

In accordance with Florida Statutes, Chapters 847.011(1)a and 847.0133(1), displaying obscene materials to minors may be a violation of the law and could result in penalties up to and including imprisonment. In accordance with Florida Statutes, Chapter 815, damaging or altering a computer or computer system, network, program, or software may be a violation of law and could result in penalties up to and including imprisonment.

Procedure

Workstations providing public access to the Internet are to be located in areas of the floor where activity can be easily monitored by staff. Internet session lengths shall be limited to one hour per session. Customers may have additional sessions if no other customers are waiting or have placed a reservation for use of the Internet computer. Customers shall be granted a maximum of three (3) hours per day access on the Internet. Customers will be given the option to extend a session, only when no one else is waiting, for a total daily maximum of 3 hours (see LS 308, Time Management Software on Internet Computers).

When all Internet computers are in use, customers may use the Reservation Station to reserve an Internet computer for the next available time. Such reservation shall be honored

only if the customer is present at the time requested to access the Internet computer. If the customer arrives after the reserved time and no Internet computer is available, the customer must wait for the next available Internet computer or make another reservation (see LS308, Time Management Software for Internet Computers).

Computer sessions are non-transferable. The customer who schedules the computer must be the one to use it. Customers must use their personal library card number and enter their PIN to log on to an Internet computer, or place a reservation for the use of an Internet computer. No more than two people may work together on the same computer at the same time. A group of two users must abide by the same time limits as a single user.

Customers may be asked to comply with sign-in and time limitations for other Library computers based upon the number of available computers and demand for their use. Branch Supervisors should discuss proposed limitations with their Regional Manager before implementation. Any limitations imposed should be clearly posted and uniformly enforced.

Sign-In Sheets:
A library branch may choose to keep a daily log of guest pass distribution. Branch Supervisors should discuss this option with their Regional Manager before implementation. Staff will enter the name of customers on the sign-in sheet. The first name and initial of the last name is the maximum amount of information that should be listed. Library customers are not permitted to view the names of others on the sheet. Sign-in sheets are to be shredded as soon as they are full or at the end of each day, whichever occurs first.

If law enforcement authorities ask to see sign-in sheets or computer log files, library staff must immediately notify the Library Director's Office and/or Regional Manager. Library staff must set aside the sign-in sheets requested by law enforcement authorities while guidance is sought from the County Attorney's Office. If law enforcement officers provide a subpoena, it must be immediately faxed to the Library Director's Office and forwarded to the County Attorney's Office.