STATEMENT OF POLICY AND PROCEDURE

Section: NLLS Employee(s) | Chapter: Service Points | Page(s): 1
Subject: **STAFF NETWORK USAGE POLICY** | Sec 1, 3Z
Reviewed: NEW | Revised: NEW | **Effective: 2022/03/04**

SECTION 1 - 3.Z

STAFF NETWORK USAGE POLICY

All staff-use computers within the Northern Lights Library System (NLLS), and its member libraries, operate on a network isolated from unrestricted internet traffic, public-use computers, and public wireless connections. It is imperative to the security of NLLS, and our TRAC partners, that the technologies connected to this network, referred to as the Staff Network, operate on the NLLS Domain (NL.ORG), or via an isolated network lock-out. It is further imperative that unauthorized devices not be permitted to connect to this network. Employees are required to use password management software provided by NLLS to ensure the appropriate distribution of access, and secure storage, of passwords critical to our operations.

Connection of Computers to the Staff Network

1. All computers connected to the Staff Network must operate on NL.ORG.
2. It is not permitted to connect computers that do not operate on NL.ORG to the Staff Network without the express permission of NLLS. This includes computers owned by the library that do not yet operate on NL.ORG (ex. public access computers), and personal computers belonging to library staff members or the public.
3. Exceptions will be made in extenuating circumstances, such as the need for an external contractor to connect to the Staff Network. In cases such as these, the owner of the external computer should be associated with a trusted provider or be able to demonstrate that their computer is free of viruses.
4. If a computer is found to be connected to the Staff Network and not operating on NL.ORG, NLLS staff will endeavour to contact the individual responsible for the connected device and remotely restrict it from connecting to the Staff Network. Library Managers will need to find alternative ways of obtaining internet access until the computer is compliant with this policy.

Connection of Other Technologies to the Staff Network

1. If a technology is acquired that must connect to the staff network to function, such as a traffic counting device, or security cameras, NLLS staff must be contacted prior to connection to build the appropriate isolated network lock-out on the Staff Network.
2. NLLS maintains the right to refuse to connect a piece of technology to the Staff Network if it is reasonably believed to have a likelihood of compromising the network. Due to this, it is recommended that Library Managers contact NLLS staff prior to purchasing new technologies.

Connection of Devices to the Staff Wireless Network

1. The Staff Wireless Network (Library Staff) is reserved for the use of NLLS approved devices requiring a wireless connection. If an unapproved device is found to be connected to the Staff Wireless Network, the Library Manager will be contacted by NLLS and asked to obtain approval for the device or connect the device to the Library BYOD wireless network.
2. Staff members who choose to bring their personal devices to work and need a wireless connection are invited to connect to the Library BYOD wireless network. This network is not to be used by members of the public, who instead must use the public wireless network (Public Library Wireless).

NLLS Executive Board Chair

March 4, 2022

Date of Approval