4.17 ELECTRONIC COMMUNICATIONS USE

This policy governs employee use of the Library's computers, networks, communications systems, phone systems and other IT resources (collectively "information systems"). All such information systems, and all communications and stored information transmitted, received, or contained in the Library's information systems are Library property and are to be used primarily for job-related purposes during working time. To ensure the proper use of information systems and business equipment, the Library may monitor the use of these systems and equipment from time to time. When using the Library's information systems, employees should note the following:

1. Information systems are owned/leased and maintained by the Library District, and electronic communications are the sole property of the District. Excessive personal use of information systems or distribution of personal messages by employees is prohibited. Personal software shall not be installed or stored on the District's information systems unless prior approval is obtained.

2. The use of personal passwords, assigned to or selected by the employee, is not grounds for an employee to claim privacy rights in the information systems or any data or content stored therein. The Library reserves the right to override personal passwords.

3. The Library will, or reserves the right to, monitor the use of information systems and to review or inspect all material stored therein. No communications are guaranteed to be private or confidential.

4. The Library's prohibition against sexual, racial, and other forms of harassment is extended to include the use of the Library's information systems. Harassing, vulgar, obscene, or threatening communications are strictly prohibited, as are sexually oriented messages or images. Employees who receive email or other information on their computers which they believe violate this policy should immediately report this activity to their supervisor.

5. Employees must respect all laws governing copyright, fair use of copyrighted material owned by others, trademarks, and other intellectual property, including the Library's own copyrights, trademarks, and brands.

6. Staff may make personal use of these resources on their own time, such as breaks, away from public areas; these resources may not be used for an employee's personal advertising or profit.

7. The security of the Library District's network must be a high priority for all users. If a staff member is aware of any security risk or abuse of the computer or Internet system, the staff member must alert their supervisor immediately.

8. Employees must be aware of the possibility that electronic messages that are believed to have been erased or deleted can frequently be retrieved by systems experts and can be used against an employee or the Library. Therefore, employees should be cautious and use the systems only in the appropriate manner and consult with systems experts to guarantee that information to be deleted is truly eliminated.

9. The Library District may use software to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by Library District networks. The failure of the

Library District to block a particular site does not render the site necessarily appropriate for access. In the event you encounter racially or ethnically offensive material or other inappropriate or sexually explicit material while browsing on the Internet, you must immediately disconnect from the site, regardless of whether the site was subject to Library District blocking software.

Violation of this policy can result in discipline, up to and including termination of employment.

Adopted by the Niles Public Library District Board of Trustees 7.1. 92
Revised 4.19.06; 1.20.2011; 11.18.2015; 1.18.2017