**STATEMENT OF POLICY AND PROCEDURE**

Section: NLLS Employee(s) | Chapter: Code of Ethics | Page(s): 1

Subject: **INTERNET and COMPUTER USAGE** | Sec 1, 3J

Reviewed 2021/11/19 | Revised: 2022/05/04 | **Effective: 2017/05/13**

# SECTION 1 - 3.J

**INTERNET and COMPUTER USAGE**

1. Background

This policy outlines best practices and expectations regarding use of computers and other technology in the workplace.

1. General Principle
   1. The guiding principle for both computer and internet usage at Northern Lights Library System (NLLS) is that these are resources paid for and owned by the system, being used by employees on NLLS time.
   2. NLLS has no objection to employees using computer resources on their own time for routine and benign matters such as internet browsing, booking flights, checking email, doing online banking, or similar matters, however personal usage should be restricted to breaks, lunchtime, or before or after hours, and should be consistent with other guidelines in this policy.
2. Restricted Uses
   1. Northern Lights Library System (NLLS) reserves the right to restrict what software may be used on NLLS computers. Staff must seek the approval of Technology Services and Infrastructure (TSI) before installing new software on NLLS devices.
   2. The following are absolutely prohibited types of internet sites to be visited, ever, under any circumstances:
      1. Gambling sites
      2. Adult content sites
      3. Unapproved file sharing sites
      4. Other sites deemed to represent a security risk by NLLS IT employee(s)
   3. In addition, sites not related to NLLS business activities should be viewed with great discretion ~~with regard to~~ regarding content others may find offensive, sexist, racist, or otherwise inconsistent with a tolerant and inclusive workplace.
   4. Similar discretion shall be exercised with email correspondence, to ensure it is also consistent with the guidelines for internet usage.
   5. Technology Services and Infrastructure (TSI) employee(s), under the direction of the Executive Director, may be directed to restrict user rights for employee(s) found in violation of the above policy, and/or implement the required technical means to enforce this policy.
3. Email
   1. Professional business practices shall be adhered to in respect to the creation and content of email records.
   2. Emails are a record belonging to Northern Lights Library System (NLLS) and will be retained and backed up according to current industry best practices.
   3. If there is a need to include confidential information, mark your text as “confidential” in the subject line.
   4. As a NLLS record, emails are subject to FOIP (Freedom of Information and Protection of Privacy) legislation.
   5. NLLS staff must use email systems provided by NLLS and not personal email accounts for business purposes.
   6. Employee(s) will, as far as reasonably possible, not share their own email or that of other NLLS Employees with 3rd parties, unless required to do so for a legitimate business reason.
   7. Employee(s) will avoid adding their email to mailing lists of any kind, unless they fully trust the source, and have a business reason for being part of a mailing list. (Technical user groups and professional memberships are ~~an~~ examples of ~~an~~ acceptable mailing lists ~~to join~~).
   8. ~~Employee(s) will refrain from opening or forwarding "chain" emails that have been sent to or received by many people and will follow additional anti-spam guidance as provided by the IT TSI department.~~
   9. NLLS employee(s) shall refrain from doing mass mailings that are not work-related.~~, especially if they involve large file attachments such as video files, high resolution pictures, or similar high resource usage elements.~~
   10. Employee(s) will treat suspicious emails, and emails from unknown senders, as cautiously as possible, deleting mail from unknown senders and not interacting with attachments or links.
4. Privacy
   1. Anything created or stored on a NLLS computer and/or network device, is subject to the provisions of the Freedom of Information and Protection of Privacy Act (FOIP).
   2. NLLS will strive to maintain the privacy of its employees with respect to email and other content on computers assigned them for work.
   3. NLLS will not actively monitor email communication or other computer usage.
   4. In the case of a cyber-security threat, incident, internal investigation, or legal requirement TSI staff may be required to access and provide emails and other computer information to third-parties.
   5. ~~The Staff Network Policy must be adhered to by NLLS staff.~~

**NLLS Executive Board Chair**

March 4, 2022

**Date of Approval**

1