
Smiths Falls Public Library



Policy Type: **Operational**

Policy Number: **OP-22**

Policy Title: **Cybersecurity**

Policy Approval Date:
November 25, 2025

Last Review Date:

The Smiths Falls Public Library recognizes that it must do everything possible to protect itself against the growing issue of cybersecurity threats while acknowledging that the library is a small organization with limited resources.

The Smiths Falls Public Library employs the following cybersecurity strategies:

1. The library does not host its own server.
2. Therefore, the chance of the library's systems being completely down in a cyberattack is unlikely.
3. Important data is housed as follows:
 - a) Our ILS, Insignia, hosts our entire catalogue and all customer records.
 - b) Our email is hosted by Vianet.
 - c) Our website host is hosted by an individual webhost.
 - d) Our phone system is hosted by net2phone.
 - e) Sensitive records are protected by the Town of Smiths Falls.
 - f) Various other databases for the public are hosted by the providers (eg. OverDrive).
4. Public computers are wiped clean upon restart.
5. Staff engage in regular cybersecurity-related training, often provided by the Town of Smiths Falls.
6. Shared passwords are securely stored in a secured, analog location for all staff. Individual passwords are also stored in secure locations. On balance, for a small, in-person organization this approach has fewer risks than using an online password manager.
7. As the library could never meet any ransom demand, we focus on data preservation by:
 - a) Staff back up all their computer and email files on a biweekly basis to external devices. In the case of the CEO files, two separate external devices are maintained with one external device kept off-site overnight.
 - b) The aforementioned external devices are marked and kept in locked locations.