



Conway Public Library Cybersecurity Policy

Purpose

The purpose of the policy will be to develop standards for the protection of information the library collects and keeps from the public, the intellectual property created by the staff for the operation of the library, how the library works with third party vendors who use library data, and the training of staff on cybersecurity.

Information Provided to the Library by the Public

The Library will request and store as little data as possible from the public, with the sole purpose being for the following reasons. The purpose of collecting personal information from the public is to establish who is eligible for a free library card, contact the patron if they have an item waiting for checkout, and to inform them about upcoming events and news.

Library Intellectual Property

The Library will take every reasonable precaution to ensure that any confidential information that is kept by the Library for any purpose is safeguarded from unauthorized access.

Working with Third Party Vendors

Many of the systems used by Library staff and members of the public are managed by third party vendors. Some of these systems involve authentication through our Integrated Library System. Library staff will work with vendors to ensure that only the bare minimum amount of information necessary to use the service in question will be shared.

The Library may choose not to work with a vendor if in the opinion of the staff they are not effectively protecting patron data.

Password Management

Library staff shall implement a password management system and will follow industry best practices for password strength.

Compliance and Enforcement

It is the responsibility of all staff members to protect the technology and information assets of the library including devices, computer software, files and data, from unauthorized access, theft, or destruction. The library reserves the right to examine or monitor any or all computer systems and devices under its control as deemed necessary to ensure the security of such systems or to enable forensic efforts to be initiated in the event of a breach.



Staff Training

Staff shall attend at least one computer security training per year.

Annual Review

The Trustees shall review this policy annually for the next three years.

Adoption

Adopted by the Trustees May 16th, 2023