Privacy Policy

Overview

The DFPL seeks to protect the privacy of Library users, and this policy explains how the Library attempts to achieve this. Our general approach is to gather only the information we need to provide library services and not to share that information.

In the case of a public health emergency, the Library may be required to collect additional information in order to protect the health of its staff, patrons, and wider community. Please refer to the Public Health Emergency Policy for more details.

Library Records

The DFPL specifically recognizes its circulation records and other records identifying the names of users to be confidential in nature. Such records shall not be made available to any agency of federal, state, or local government except pursuant to such process, order, or subpoena as may be authorized under the authority of federal, state or local law which relates to civil, criminal, or administrative discovery procedures or legislative investigatory power. Library staff receiving a request to examine or obtain information relating to circulation or other records identifying the names of library users will immediately refer the request to the Library Director.

The Director, upon receipt of such process, order, or subpoena, shall consult with the Village attorney to determine if such process, order, or subpoena is in good form and if there is a showing of good cause for its issuance.

If the process, order, or subpoena is not in proper form or if good cause has not been shown, the DFPL will insist that such defects be cured before any records are released.

Any threats or unauthorized demands concerning circulation and other records identifying the names of library users shall be reported to the library attorney.

Any problems relating to the privacy of circulation and other records identifying the names of library users which are not provided for above shall be referred to the Library Director.

Westchester Library System

The DFPL partners with the Westchester Library System (WLS) to enhance the services we offer to our users. WLS provided services include the public catalog (ILS or Integrated Library System), public computers in our library, and wireless internet access. All of these services are offered under the auspices of the WLS Privacy Policy.

eContent and 3rd Party Services

We work with a number of partners to provide eContent (e.g., eBooks, eMusic, streaming movies). Before using these services, users should read the privacy policy of the company that is providing the service in question.

Adopted by the Library Board of Trustees, 6/18/20

We also work with a number of third party service providers and technologies, including infrastructure, database and other similar service providers ("Third Party Providers"), to help deliver some of the Library's online services to you. The Library may share your information with these Third Party Providers as necessary for those providers to provide services to the Library.

For your information and convenience, the Library also provides you access to third party collections, databases, widgets, applications, website, other similar services and collaborative features (collectively, "Third Party Platforms") through the Library's online platforms. When accessing Third Party Platforms through the Library website, be aware that any information shared with these platforms will be governed by their privacy policies and practices. The Library is not responsible for the privacy practices of the Third Party Platforms. The Library recommends that you read any applicable privacy notices and policies of any Third Party Platforms you access through the Library's online Services before accessing those Third Party Platforms.

Website & Cookies

Cookies are commonly used to provide useful features to website users. A cookie is a small text file that is sent to your browser from a website and stored on your computer's hard drive. Cookies cannot read data from your hard disk or read cookie files that were created by other websites—the website that creates a cookie is the only one that a browser will permit to access it. The cookie itself does not contain any personally identifiable information, but may be used to tell when your computer has accessed DFPL's website.

If you are concerned about the use of cookies, we suggest that you set your browser's options to notify you whenever a cookie is set or to disallow cookies altogether. You should be aware, however, that prohibiting the use of cookies may restrict your access to certain types of content or features.

Confidential Information Security

Confidential information security is defined as the administrative, technical, or physical safeguards the Dobbs Ferry Public Library ("Library") uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle confidential customer or staff information ("confidential information").

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. The Library has a responsibility to ensure that the accessing, handling, sharing and disposing of confidential information complies with applicable laws and regulations.

A. Responsibilities

The Library has set the following goals for every Library computer, piece of equipment or network with access to confidential information:

- Secure computing systems, equipment, and networks with confidential information

- Restrict physical and login access to authorized users
- Maintain up-to-date software patches and anti-virus software
- Ensure and maintain complete system backups
- Enable and use host-based firewalls if available
- Perform regular security scans on computing systems, equipment, and networks
- Provide training, or in the absence of live training, provide written training materials, to all staff, volunteers, trustees, and contract workers in the appropriate use of the network, awareness of the possible effects of misuse or unauthorized use of computer resources, and the consequences of any unauthorized use.

B. Authorized Users

Authorized users may be staff members, volunteers, trustees and contract workers. They are responsible for confidential information in their custody. Maintaining the confidentiality, integrity, availability, and regulatory compliance of confidential information stored, processed, or transmitted at the library is a requirement of all authorized users. All authorized users with access to confidential information will:

- Notify their manager immediately if confidential information, passwords, or other system access control mechanisms are lost, stolen, or disclosed or suspected of being lost, stolen, or disclosed.
- Restrict physical access to laptop computers when the user is physically away from the computer by locking the computer or using security cables or devices.
- Secure all staff computers by using a screen saver or built- in lock feature when the user physically walks away from the work space.
- Maintain possession or control of mobile devices to the extent possible to reduce the risk of theft and unauthorized access.
- Secure computers and mobile devices by requiring passwords (except for public computers with no confidential information).
- Use secure methods to transfer confidential information.
- Not intentionally damage, alter, or misuse any library owned or maintained computing systems, equipment, or networks.

C. Library Managers

Specific responsibilities of library managers include:

- Ensuring staff understand the danger of malicious software, how it is generally spread, and the technical controls used to protect against it.
- Informing the person responsible for IT support of the change in status of staff, volunteers, trustees or contract workers who use the library computer resources. This could include a position change (providing greater or more restricted access privileges) or termination of library employment.

Enforcement
When users fail to comply with this policy, the Library network may be exposed to the unacceptable risk of loss of confidentiality, integrity, or availability. Violations of security guidelines and procedures established to support this policy will be promptly investigated and

could result in disciplinary action up to and including termination of employment or termination of a non-employee's rights to use the computer resources.

Breach of Security

Any actual or suspected security breaches involving confidential information must be reported immediately to the Library Director. Incident response procedures will be initiated to identify the suspected breach, remediate the breach, and notify appropriate parties.

Disclaimer

The Library uses standard systems and communication methods beyond its direct control, and no guarantee can be made that transactions over the Internet or our local network, by mail or e-mail, by telephone or at a public service desk are infallibly secure and confidential. While utmost care is exercised to protect Library systems and servers from unauthorized access, no guarantee can be made that personal information is invulnerable.

APPENDIX TO PRIVACY POLICY

New York State Civil Practice Laws and Rules S.4509

Library records, which contain names or other personally identifying details regarding the users of public, free association, school, college and university libraries and library systems of this state, including but not limited to the circulation of library materials, computer database searches, interlibrary loan transactions, reference queries, requests for photocopies of library materials, title reserve requests, or the use of audio-visual materials, films or records, shall be confidential and shall not be disclosed except that such records may be disclosed to the extent necessary for the proper operation of such library and shall be disclosed upon request or consent of the user or pursuant to subpoena, court order or where otherwise required by statute.

Adopted by the Library Board of Trustees, 6/18/20