Chesterfield Public Library

Information Technology Policy and Procedures (ITPP) Manual

Approved by Library Trustees

January 17, 2023

Table of Contents

Information Technology (IT) Policy

It is a policy of the Chesterfield Public Library (CPL) to regulate the management and use of its information technology resources for legitimate operational reasons.

Information technology resources are broadly, but not exclusively, comprised of network services, computers, peripheral devices, end point devices (smart phones and tablets), software applications, web services, and cloud-based services like social media.

Library trustees have designed this policy to achieve the following operating objectives.

1. Assure continuity of library operations in support of patron and community needs.
2. Maintain a secure digital operating environment to protect library and patron interests from motivated threat actors operating in the cyber realm.
3. Establish guidelines for social media use consistent with the library's mission and standards.
4. Make known to library employees and patrons their responsibilities for maintaining and or using information technology resources.

The cybersecurity program framework and IT procedures outlined below will enable implementation of this policy. Library trustees and employees are responsible for implementation of the procedures and achievement of the policy objectives outlined above.

CPL trustees and the library director will review annually, or sooner when needed, the IT Policy and Procedures outlined in this document for relevancy and improvement.

Cybersecurity Program Framework

CPL will deploy an effective cybersecurity program as a means for assuring continuity of library operations and a secure digital operating environment. The National Institute for Standards and Technology (NIST) recommends five capabilities for assuring cybersecurity. They are 1) identify, 2) protect, 3) detect, 4) respond, and 5) recover. Trustees provide guidance for the deployment of these capabilities in the next five sections of this document. It is important to note that cybersecurity is not the responsibility of a single person. Library trustees, employees and patrons are collectively responsible for assuring cybersecurity.

#1 Identify

CPL needs the capability to visualize and describe its on premise information technology resources and broader digital operating environment.

In conjunction with the Trustees, the Library Director will be responsible for maintaining an inventory of all information technology resources used by the library during its operation.

#2 Protect

CPL needs the capability to convert its attack surface structure into a trust boundary at a level sufficient to meet security requirements.

A cyber-risk forms when there is a motivated threat actor, who desires an asset of value. The motivated threat actor needs to exploit a vulnerability to illicitly gain access to the asset of value. In general, a small community library is not a high value target. It is, however, a soft target of opportunity that a cyber-criminal may attack seeking illicit gain, a hacktivist promoting their cause, or a disgruntled insider like a patron or employee who wants to disrupt library operations.

Management of the library's attack surface is essential for cybersecurity. There are four elements in the library's attack surface structure. They are 1) information technology resources deployed for library mission achievement, 2) cyber-supply chain fulfilling library digital needs, 3) people (employees and patrons) using information technology resources, and 4) the library's physical facility where information technology resources are located. Conversion of attack surface risk into a trust boundary enables cybersecurity.

In conjunction with the Trustees, the Library Director will be responsible for developing and implementing procedures to effectively manage attack surface risk.

#3 Detect

CPL needs the capability to detect when a cybersecurity incident occurs through human observation or a technology alert.

It is important for library employees and patrons to say something if they see something. This may be either an indicator of risk or an indicator of compromise. An example of an indicator of risk is an abnormality like a web session with an unexpected pop-up window or a malformed email containing unusual information or a link. Another example is a phone call or message requesting information that is confidential in nature. An example of an indicator of compromise is abnormal data, strange information technology resource performance, or a non-responsive (dead) resource.

Note, there may be an automated incident detection capability with alert messages and logging capabilities depending on the sophistication of deployed library information technology resources. If present, CPL should consider utilizing it. It may be necessary for CPL to engage a subject matter expert specializing in computer and cybersecurity management if the library does not possess the skills to effectively manage it.

In conjunction with the Trustees, the Library Director will be responsible for developing and implementing procedures for detecting and reporting an attack.

#4 Respond

CPL needs a preplanned response capability to properly address cybersecurity incidents. It is not a question of if a cybersecurity incident will occur; instead, it is simply a question of when it will occur. Elements of a response plan include guidelines for 1) employee mitigation steps needed to stop the incident, 2) notification of relevant library personnel and trustees, and 3) initiation of the recovery phase for restoration of library services.

In conjunction with the Trustees, the Library Director will be responsible for the developing and implementing procedures required for a viable response capability.

#5 Recover

CPL needs a rapid recovery capability to minimize down time when a cybersecurity incident occurs.

There are four key elements in a recovery plan. They are 1) a work-around approach that can alternatively be used while library services are being recovered, 2) identification of a subject matter expert in computers and cybersecurity who can be employed to aid in the recovery effort, 3) deployment of a backup strategy for critical data, and 4) a replacement capability for operationally impaired hardware or software when required.

In conjunction with the Trustees, the Library Director will be responsible for developing and implementing procedures required for a viable recovery capability.

Information Technology Procedures

The following procedures will help the library achieve its stated information technology policy operating objectives.

Inventory of Library Owned Information Technology Resources

1. The Library Director will inventory information technology resources and record findings in an excel spreadsheet that is password protected.
2. The inventory file will have an obscure file name so as not to draw attention if discovered by a motivated threat actor.
3. The Library Director will make known to the Trustees the name of the file, its password, and where it is located.
4. Alternately the Library Director will print a hard copy of the spreadsheet file. The hard copy document will be stored in a locked fireproof file cabinet that is known to the trustees.
5. Inventory resource line items will show end-of-life dates or contract expiration dates when appropriate.

Management of Information Technology Resource Documents and Files

1. The Library Director will maintain a file containing all information technology resource documents.
2. The file will contain purchase / lease agreements, user manuals, warranty terms, and source files (IE recovery files).
3. The file will be stored in the same locked fireproof file cabinet containing the information technology resource inventory.

Management of Library Employee Login Credentials

1. The Library Director and employees will maintain an inventory of passwords utilized by employees using 3X5 notecards.
2. The note cards will show both current and prior passwords.
3. The Library Director will store the notecards in the same locked fireproof file cabinet containing the information technology resource inventory and related documents.

Procurement of New Information Technology Resources

1. The provenance of all information technology resources must be known. The Library Director will only purchase new network services, equipment, and or software from the OEM supplier or their authorized sales channel. Grey market or previously owned goods, while cheaper, may contain hidden cyber risks.
2. The Library Director should consider purchasing technical and cybersecurity support directly from the OEM supplier.
3. The OEM supplier must provide 24X7 technical and cybersecurity support services
4. The Library Director needs to evaluate a supplier's commitment to update their good or service in the presence of discovered vulnerabilities and constantly evolving threats.
5. The Library Director needs to ask the supplier if there is a product or service end of support or end of life notice issued. CPL should receive a reasonable period of support for their purchase.
6. The Library Director will maintain a file of in force supplier warranties and file them with the information technology resource inventory and passwords.
7. The Library Director will ensure that purchased information technology resources are fit for their intended use and interoperable with relevant resources that are already deployed.
8. Trustees must review and approve the purchase of new capital information technology resources recommended by the Library Director.

Disposal of Existing Information Technology Resources

1. The Library Director needs to ensure that existing information technology resources containing sensitive information are properly decommissioned.
2. Decommissioning requires degaussing or physical destruction of the actual device storing library information.
3. The library director may elect to use an external service specializing in decommissioning based on the sensitivity of the information on the resource.

Information Technology Resource Management

1. The Library Director, or their delegate, needs to update software when upgrades become available on a timely basis.
2. The Library Director, or their delegate, will ensure that all information technology resources with internet access will have an antivirus application installed.
3. The Library Director, or their delegate, will ensure that employees receive instructions on any licensing agreements relating to the software including any restrictions on the use of the software.
4. The Library Director, or their delegate, will ensure that back-ups of all critical information technology resources are current and available if needed.
5. The Library Director and employees are prohibited from bringing software from their home and installing it on library owned information technology resources.
6. The Library Director and employees are prohibited from taking home library owned information technology resources for their personal use.
7. Unauthorized software is prohibited from being used in the library by both employees and patrons.
8. Duplicating, acquiring or use of software copies is prohibited in the library by both employees and patrons.

Information Technology Resource – User Identify and Access Management

Every employee will have a unique password to access technology. Information technology resources shall not be left unattended in a state that affords an opportunity for unauthorized or inappropriate access to library records or otherwise compromises security. Each password must meet the following requirements:

1. Be at least eight characters in length
2. Have not been used in two previous passwords cycles
3. Does not contain the individual’s name, account name, or personal information
4. Upper case character
5. Lower case character
6. Numbers 0-9
7. Non-alphanumerical characters
8. Must not follow any discernible pattern

Passwords are an important aspect of computer security. Users are responsible for taking appropriate steps to select and secure their passwords and should not:

1. Reveal a password in an email message
2. Talk about a password in front of others
3. Hint at the format of a password (e.g., “my family name”)
4. Reveal a password on a questionnaire or other form
5. Use the “remember Password” feature.
6. Reveal a password over to the phone to anyone.
7. Share a password with patrons or family members
8. Write passwords down and store them in your desk. The Library Director will secure them in a locked file.
9. Store passwords in a file on any computer system
10. Fail to report a password or account suspected to have been compromised to the Library Director.

Passwords are not to be shared with other employees except the library director. The library director will keep a list of all passwords in a locked and secure place. The Chair of the Board of Trustees will keep a duplicate list off-site. No passwords will be stored on a desktop password management system.

Passwords will be changed when a password must be provided to a non-employee or when staff turnover occurs.

All user accounts are to be removed immediately upon employee termination.

Social Media Management

The Chesterfield Library Board of Trustees and the Library Director will have full administrative rights to all social media pages. Other staff that has been trained on social media protocol will have editor rights. Any posts on social media platforms of any kind by library staff must be approved by the Library Director prior to posting. The content of the library’s social media interface is to be accurate, appropriate, and current. Basic branding guidelines must be followed to ensure a consistent and cohesive library image.

The Library Director will maintain a record of the following details:

1. List of domain names
2. Dates of renewal for domain names

3. List of hosting service providers
4. Expiry dates of hosting
5. List of social media platforms.

The Library Director will maintain a list of all social media passwords in a locked fireproof file cabinet containing the information technology resource inventory, related documents, and user login credentials. The Chair of the Board of Trustees will work with the Library Director to maintain a duplicate list off-site.

Specific Social Media Requirements:

1. Any posts on social media platforms of any kind must be approved by the Library Director prior to posting. All social media accounts are created with the Approval of the Chesterfield Library Board of Trustees. The Library Director must approve and change the name, passwords, avatar, and any other settings of the social media accounts.
2. The Library Director and the Chair of the Library Board of Trustees shall be the only personnel to have administrative privileges.
3. All social media sites and content are subject to being edited or deleted by the Chesterfield Library Board of Trustees.
4. All social media accounts and business emails are the property of the library. All materials developed on library time or library resources are the property of the library.

Employees must:

1. Ensure that others know that your personal account or statements do not represent the library.
2. Avoid sharing intellectual, financial, or personal information. Confidentiality laws apply.
3. Avoid any defamatory, offensive, or derogatory content as it may be considered harassment. Please be respectful and polite.
4. Avoid speaking on matters outside your field of expertise.
5. Correct or remove any misleading or false content as quickly as possible.
6. Observe and abide by all copyright, trademark, and service mark restrictions in posting materials.

The Library Director has the right to monitor all social media postings. Disciplinary action leading up to and including termination of employees if the policy's guidelines are not followed. Non-conformity with this policy includes but is not limited to

1. Failing to obtain the library directors approval before postings
2. Disregarding job responsibilities and deadlines to use social media at work
3. Disclosing confidential information through personal accounts without consent

4. Directing offensive or threatening comments towards colleagues and members of the online community.
5. Making obscene or libelous comments
6. Using library accounts for political advocacy
7. Posting comments which discriminate based on race, appearance, religion, national origin, sex, gender, non-gender, disability, age, sexual orientation, creed, or ancestry.
8. Posting comments which are sexually harassing, including epithets, slurs, negative stereotyping, sexual rumors or innuendos, off-color jokes.

The library is a public space where members of the community come to use our resources and attend programs. Photographs and/or video may be taken at any time in order to promote the library, its events, staff, and resources. By participating in library programs, patrons' consent to having their image taken for library marketing purposes. Patrons may at any time contact library staff to request that their image (or that of minors in their care) not be used or removed from the library's online forum.

Similarly, patrons should have no expectation of privacy in posting on the library's sponsored social media platforms. By choosing to comment or post on the library's social media sites, patrons agree to give the library permission to use the content of any posting without compensation or liability. Any posts that violate this policy may be deleted.

Cybersecurity Incident Response Protocol

1. Once a cybersecurity incident is detected, do not turn off or unplug the information technology resource located on premise. Alternatively disconnect the resource from the on-premise intranet or internet while it is still powered on.
2. Other information technology resources connected to the intranet or internet should be left powered on and disconnected temporarily from the network too.
3. Notify the Library Director and Trustees as appropriate based on incident severity.
4. Leave the resource powered on until the Library Director has a chance to investigate
5. The Library Director may retain the services of a subject matter expert, who is knowledgeable in computers and cybersecurity.
6. Either the Library Director or retained subject matter expert will initiate the recovery process when it is appropriate to do so.
7. Note, once unplugged information technology resources loses temporary memory that may be useful for digital forensic purposes.

Employee Acceptable Use Policy for Library Owned Resources

The Library Director will allow employees to access their personal accounts while at work, but the Board of Trustees expect employees to act responsibly and ensure that productivity is not affected and accessing personal accounts occurs during break or at lunch.

Use of personal accounts should be restricted to minutes per workday and should not be used for any personal commercial or promotional purposes.

While employees are not required to use personally owned devices to complete their daily job duties, it is recognized that there are times when this may occur. Employees are required to have pre-approval from the Library Director prior to connecting any personally owned devices to library owned information technology resources.

Employee Bring Your Own Device Policy (BYOD)

Employees may use their personally owned end point devices (smart phone, tablet, or personal computer) when connected to the library public WiFi network. They are prohibited from using their personal end point devices for interacting with any other library owned information technology resources. Employees are responsible for maintaining cybersecurity hygiene on their endpoint devices.

Patron Acceptable Use Policy

1. The Chesterfield Public Library provides internet access through designated workstations and computers, as well as public wireless access. Computer access is available to all card holders in good standing on a first come, first served basis. Patrons without a library card may purchase a guest pass.
2. In the interest of serving all customers, the library reserves the right to set uniform time limits on public computers
3. Signing in to use public access computers is required.
4. Time limits per session are enforced if other patrons are waiting.
5. All illegal use including the viewing of child pornography, infringement of copyright, credit card fraud, hacking, and sending libelous and/or harassing emails is prohibited.

6. It is the responsibility of the user to respect copyright laws and licensing agreements and assume responsibility for payments of fees for any fee-based service.
7. Library staff members are not able to provide in-depth computer training but will answer questions and, as time permits, help users locate and use resources on the internet. Library staff support may be limited regarding personal devices.
8. Patrons may not store personal information, documents, or files on library computers. Patrons may not use thumb drives, DVD's, or C.D.'s on library P.C.'s. The library is not responsible for maintaining patron files, documents, or individual website logins.
9. Patrons may send materials to the printer before their session ends or they leave the computer. The library charges $0.10 to print a black and white page and $0.50 to print a color page. When a patron's session has ended their work is no longer available.
10. Parents or legal guardians, not library staff, are responsible for internet information selected and/or accessed by their children. The library will not serve in *loco parentis* to monitor children's access. The Chesterfield Public library does not use internet filtering software.
11. There are times when viewing otherwise legal materials may be inappropriate. Behavior which attracts the attention of others to sexually explicit images depicted on the screen or in copies made on the library printer is forbidden. The library staff reserves the right to address such use of the internet or behavior by requiring a patron to terminate his/her session.
12. The use of library computers, networks and internet access is a privilege and may be revoked for inappropriate conduct including, but not limited to:
    a. Displaying images, sounds, or messages in a way that will negatively affect those who find them objectionable, offensive, or disruptive.
    b. Altering, removing, or damaging configurations of software or hardware on library computers.
    c. Misrepresenting oneself, to gain unauthorized access to computer systems that the user has not been granted access to.
    d. Deliberately propagating any virus, worm, Trojan horse, trap-door program code, ransomware, or other code or file designed to disrupt, disable, impair, render inaccessible, or otherwise harm either the library's networks or systems or those of any other individual or entity.
    e. Disclosing, using, or disseminating personal information regarding minors.
    f. Seeking information on, obtaining copies of, or modifying files, data or passwords belonging to others. Patrons will respect the privacy of others.
13. Computer users shall agree to hold harmless the Chesterfield Public Library for any liability or damage claim arising from the disclosure of financial or other personal information over the library's public computer services. Users should be aware that use

of public computers is not a secure medium and that third parties may be able to obtain information regarding user’s activities.

14. The internet offers access to many valuable sources of information; however, some information found on the internet may be inaccurate, incomplete, dated, or offensive to some individuals. An informed patron must evaluate the validity and appropriateness of any information found.
15. The library is not responsible for equipment malfunction, loss of data, or any damages to the user’s peripheral equipment
16. Misuse or abuse of library resources or willful and malicious damage to equipment may result in the immediate suspension of library privileges and/or prosecution of criminal charges (RSA 202-A:24). Reinstatement of privileges requires a written request for an appointment with the Library Board of Trustees.
17. All registration and lending records of the Chesterfield Public Library are considered private and confidential as part of the library’s commitment to intellectual freedom and Library policies. This includes the use of Library computers and online resources that are accessed. The Chesterfield Public Library will not disclose the information except upon consent of the user, pursuant to subpoena or court order, or as otherwise required by law. All public computers are configured to reset to a clean slate after restarting, wiping all data from the previous session.