JEFFERSON COUNTY
LIBRARY
DISTRICT

INFORMATION TECHNOLOGY SERVICES POLICY

ADOPTED MAY 8, 2024

PURPOSE

This policy establishes guidelines to help ensure the safety, security, availability, and integrity of the data and tools used by the Jefferson County Library District, as well as those offered to patrons. Responsibilities include:

- Provisioning digital tools required by staff and Trustees to fulfill the District's mission and adhere to District policies;
- Securing these tools to the greatest extent possible while still supporting staff activities to fulfill the District's mission;
- Maintaining data created and used by staff and Trustees in the fulfillment of the District's mission, including assuring its availability to staff for business purposes, public records requests, and archival purposes; and,
- Providing secure and accessible tools and services to patrons as needed to fulfill the District's mission.

DEFINITIONS

Information Owner: Staff responsible for a technology tool, allowing or disallowing access to that tool, and any information stored within that tool. This is not necessarily Information Technology staff or vendors assigned to IT support.

IT Services: Information Technology staff or vendors assigned to IT support.

District: the Jefferson County Library District, JCLD.

Tools: Within the context of this policy, the term "tools" refers to hardware, software, and services provided by JCLD, third-party vendors, and/or contractors, and which may fall under the maintenance, security, and support responsibility of IT Services.

Remote: Locations not owned or operated by JCLD.

On-Premises: Locations owned or operated by JCLD.

PURCHASE AND INSTALLATION OF IT HARDWARE AND SOFTWARE

To efficiently, securely, and sustainably provide necessary technology tools for staff, it is optimal to minimize the diversity of hardware and software tools deployed within the District. In consultation with IT Services, the Director or designee will approve purchases, procure hardware, software, and services, and engage contractors and vendors in accordance with this Policy. As the safety, efficiency, accessibility, and security of the District's technology environment is critical to the continued fulfillment of the District's mission, careful consideration is required during the selection process of any new tools. This consideration will weigh the costs and benefits of additional tools as they pertain to security, efficiency, and efficacy in fulfilling the tool's purpose.

IT Services will develop and maintain a list of tools that are "supported for use" by District staff. Staff use of tools outside of this list is prohibited unless *written* consent is obtained. Use of these tools must be critical to the fulfillment of the District's mission. This consent may be accompanied by limitations to the unsupported tool's allowed use or to the ability of IT Services to provide technical support regarding its use. The consent may be revoked at any time.

Information Owners, in close collaboration with IT Services, shall manage and maintain relationships with third-party vendors who provide hardware, software, and/or services ("tools") to JCLD. Prior to contracting with third parties for tools, JCLD shall require information from the vendor regarding:

- Compliance standards
- Service-level agreements
- Vendor liability in the event of a data breach
- Disaster recovery and redundancies implemented by the vendor
- Termination of contracts when security requirements are not met
- Auditing requirements
- Other security-related information about the vendor that is essential to JCLD's ability to provide services to the public

The District will comply with all software and hardware licensing requirements and restrictions.

STAFF USE OF TECHNOLOGY

Technology resources and tools are provided to employees and Trustees for use in the performance of their work. The equipment, data, and other tools used always remain the property of the Jefferson County Library District. Data on District computers, or stored on platforms owned, leased, or subscribed to by JCLD, is not private, whether personal or work-related, including email and voicemail.

IT Services will provide staff and Trustees with requirements, limitations, procedures, and guidelines for the proper use of tools in accordance with current security and efficiency practices.

JCLD reserves the right to monitor and audit computer or information use at any time without prior notice to employees. JCLD may monitor and audit for legitimate business reasons.

IT Services monitors inventory of all tools for proper and secure use. Staff tools may also be monitored for the purpose of securing patron data in accordance with the *Privacy and Confidentiality Policy*. Staff use of tools shall not jeopardize the data or operations of the District. Staff use of tools must never violate any other JCLD policy or procedure, nor shall such use be allowed if it is in violation of local, state, or federal law.

Staff shall not install any software on District computers unless *written* consent is obtained.

Minimal personal use of JCLD-provided tools is allowed during breaks, lunch hours, or other off-work time during an employee's scheduled workday. Employees may make limited personal use of printers or copiers during breaks, lunch hours, or other off-work time on the same terms and at the same rates that apply to patrons using these resources.

Volunteers or others who are not library employees may use District computer resources when authorized by a supervisor, but only for the purpose of performing library business JCLD has engaged them to perform on a paid or volunteer basis. Non-JCLD employees using District technology resources are subject to all restrictions set forth in this policy.

- **EMAIL USAGE**
  - JCLD email accounts are provided to staff and Trustees for JCLD business purposes only. Personal use of JCLD email accounts is prohibited. JCLD-provided email accounts shall not serve as an employee's primary personal email account. Employees and Trustees should be aware that JCLD-provided email accounts may be subject to public disclosure.
  - As email can be used for external communication, care must be taken by staff to assure the privacy of patron data as directed in the *Privacy and Confidentiality Policy*.
  - No action shall be taken to disable malware- or spam-filtering measures deployed by IT Services.
- **INTERNET USAGE**
  - Internet access is provided throughout JCLD facilities. Access should always be used diligently by patrons and staff, with consideration of best security practices in mind. Use of social media tools shall only occur in accordance with the *Social Media Policy*.
  - Procedures, guidelines, and limitations for Internet access will be provided by IT Services.

USER ACCOUNT MANAGEMENT

User accounts for technology tools and services are often required for staff access. These accounts will be secured according to best practices, using secure passwords and other authentication methods to prevent access by unknown parties. Information Owners shall maintain user accounts in a manner which preserves security and integrity of the data accessed by users. Procedures and guidelines, including password/authentication requirements and procedures for adding/removing accounts, will be provided by IT Services.

NETWORK SECURITY

Devices, software, and hardware required for providing access to tools shall be maintained according to documented best practices for operating system and software patching, software and firmware updates, and security updates. These practices will be documented in procedures updated regularly according to current conditions and practices.

Remote access to on-premises tools will be strictly limited and only granted in accordance with the *Telecommute Policy*.

PHYSICAL SECURITY

Physical access to tools, including systems required to provide on-premises services, shall be denied by physical means whenever possible. Such access will be managed to prevent access by unknown parties. This includes:

- Disconnecting unused network jacks from equipment that provides access to JCLD networks
- Limiting physical access to server and communications closets through the use of locked doors or locked cabinets whose keys are inventoried and tracked
- Limiting access to JCLD tools by non-staff by limiting the number of computers to the minimum required for daily operations
- Implementing security processes that prevent use by unknown parties (such as "locking" a computer when staff is not monitoring it).

DATA SECURITY

IT Services supports the Public Records Officer in maintaining the District's compliance with the Public Records Act (RCW 42.56). In so doing, IT Services provides tools such as storage to maintain both public records and data important to the operation of the District. IT Services also works with Information Owners to minimize the amount of data retained by the system to mitigate the risk of downtime and other operational losses in the case of security breaches.

IT Services also develops procedures that enhance the integrity, confidentiality, and security of operational and patron data. These procedures include: access to, or limitations to, tools and processes that pertain to creation, access, usage, modification, sharing, retention, archiving, or deleting of data. These procedures are provided to Information Owners for their own use in securing the data for which they are responsible.

IT Services implements technology access control procedures and audits data access as appropriate to maintain and secure the District's data. It will work with Information Owners to help them follow best practices not only with providing or limiting access to tools that fall under their purview, but also with maintaining, minimizing, and securing any data housed within those tools.

IT Services maintains a Disaster Recovery Plan to be used in instances of data breach, data loss, or accidental destruction. The Plan includes system restoration priority, data backup requirements, communications plans, and vendor contact information. It also includes a process for regular review and updates, as well as regular discussion and practice in the use of the Plan.

CYBERSECURITY PRACTICES

IT Services develops and implements practices and procedures that mitigate cybersecurity risks inherent in the use of technology tools. The mitigation techniques may include limiting, enabling, and monitoring of:

- Use of software, applications, and browser extensions
- Use of USB or portable storage media or peripheral devices such as printers or hard drives

Further mitigation may include:

- Regular data backups for the purposes of disaster recovery or business continuity
- Design and implementation of required training on IT security and best practices
- Password complexity requirements and alternative authentication methods
- Limitations for mobile device management
- Auditing the use of JCLD tools and data

IT Services coordinates regular cybersecurity audits, performed by third-party professionals, that assess the current state of the District's practices. Audits are iterative and provide opportunities for constant improvement. Recommendations for changes to procedures and processes as a result of the audit process will be assessed and implemented when possible, considering cost/benefit of each recommendation.

RESPONSIBILITY FOR PROCEDURES

The Technology and Collections Manager is responsible for establishing, maintaining, and ongoing monitoring of procedures that support this policy. The Technology and Collections Manager is also responsible for adherence to this policy and related procedures.