PUEBLO CITY-COUNTY
Library District

www.pueblolibrary.org

Information Technology Policies and Procedures

PUEBLO CITY-COUNTY
Library District

TABLE OF CONTENTS

PUEBLO CITY-COUNTY Library District

INFORMATION TECHNOLOGY

05.01.01 Acceptable Use of Information Technology

Pueblo City-County Library District (PCCLD) requires the responsible and secure use of all information technology (IT) resources, including computers, networks, software, and mobile devices, provided by PCCLD. PCCLD intends to protect the confidentiality, integrity, and availability of systems and data, and to promote the efficient and effective use of IT resources by employees, contractors, and authorized users. PCCLD seeks to align with the National Institute of Standards of Technology (NIST) Cybersecurity Framework, specifically the Identify (ID), Protect (PR), and Detect (DE) functions, and to mitigate the risks associated with inappropriate use of IT systems.

This policy applies to all employees, contractors, and authorized users of the PCCLD's IT resources, including desktops, laptops, tablets, mobile devices, networks, software, and cloud services, whether accessed on-site or remotely.

Acceptable Use
PCCLD's IT resources are to be used solely for authorized purposes related to the performance of job duties or allowed patron activities. Acceptable use includes:

- Accessing and using library systems, databases, and software to complete job-related tasks.
- Communicating with colleagues, library patrons, and external parties through authorized channels for library business purposes.
- Accessing educational or professional development resources directly related to job responsibilities.
- Patron use of library equipment, systems, databases, software, internet resources.

Unacceptable Use
The following activities are strictly prohibited:

- Accessing, downloading, or transmitting offensive, illegal, or unauthorized content (e.g., pornography, gambling, and malware, etc.)

- Installing unauthorized software, games, or other personal applications.

- Using IT resources for personal financial gain or illegal activities (e.g., fraud, hacking, etc.)Sharing login credentials or allowing unauthorized access to library systems.
- Using IT resources to harass, intimidate, discriminate against others or violate library rules of conduct or employee guidelines.
- Circumventing security protocols or accessing restricted areas of the network or data systems.

See Also:
02.09.06	Communication Systems
03.01.02	Internet Access and Wireless Use
03.01.02.F1	Internet Access Agreement Form
03.01.02.F2	Internet Consent Form - Permission for Minors
03.01.03	Public Computers and Other Equipment Use
03.01.03.G1	Public Computers and Other Equipment Use Guidelines

PUEBLO CITY-COUNTY
Library District

INFORMATION TECHNOLOGY

05.01.01.G1 Acceptable Use of Information Technology Guidelines

Responsibilities

Staff are required to adhere to basic security hygiene practices, including:

- Using strong, unique passwords for all accounts and changing passwords regularly.
- Locking workstations when not in use.
- Reporting suspected security incidents (e.g., phishing attempts, malware infections) to the IT department immediately.
- Ensuring data is stored securely and is not shared or transmitted without authorization.

Privacy and Confidentiality

Employees must ensure that patron information and other sensitive data are kept confidential. Access to confidential information should only occur on a need-to-know basis, in accordance with library policies and regulations.

Monitoring and Enforcement

The Library District reserves the right to monitor the use of its IT resources to ensure compliance with this policy. Monitoring will be done in accordance with relevant privacy and legal guidelines. Any detected violations will be addressed promptly in alignment with PCCLD policies.

PUEBLO CITY-COUNTY Library District

INFORMATION TECHNOLOGY

05.02.01 Asset Management

Pueblo City-County Library District (PCCLD) requires the responsible and secure use of IT assets through effective practices that ensure tracking, maintaining, and safeguarding assets. This policy applies to all hardware and software assets used in the PCCLD environment, including but not limited to laptops, desktops, servers, mobile devices, printers, scanners, and networking equipment.

IT assets meeting the capitalization threshold for financial accounting standards must be managed in conjunction with the PCCLD Finance Department. All other assets shall be inventoried and monitored in line with established library procedures.

See Also: 04.01.05 Management of Fixed Assets
04.01.06 Disposal of Fixed Assets
04.01.06.P1 Disposal of Fixed Assets Procedure

PUEBLO CITY-COUNTY Library District

INFORMATION TECHNOLOGY

05.02.01.P1 Asset Management Procedures

Asset Classification

IT Assets are classified into the following categories:

- Hardware: Desktops, laptops, servers, printers, networking equipment
- Software: OS, applications, licensed software
- Peripheral Devices: Monitors, keyboards, mice, etc.

Acquisition and Tagging

All IT assets must be entered into the designated inventory system (Snipe-IT) upon receipt. Assets must be tagged with a unique barcode/QR code. Asset information must include make, model, serial number, assigned user, and location. Assets individually valued at $5,000 or more are capitalized and tagged by the Finance Department (separately from and in addition to the IT process).

Lifecycle Management

Assets must be evaluated annually for functionality, support status, and replacement needs in accordance with the established library asset replacement plan. Replacement cycle typically spans every 5 years or as needed. Retired assets must be removed from inventory and securely wiped before disposal. Disposals of capitalized assets (recorded by the PCCLD Finance Department) must be approved for disposal by the library board of trustees prior to disposal.

Asset Transfers and Assignments

Asset transfers must be approved by the Director of IT, or their designee, and documented in the inventory system. Assignments must be validated through asset acceptance documentation. Changes must be reflected in inventory within 48 hours of the asset transfer or relocation.

Auditing and Reconciliation

Periodic audits to reconcile inventory data are required (annually at minimum) or upon request by the CFO or Executive Director. Any missing or damaged equipment must be reported and investigated. Annual audit findings must be submitted to the CFO and Director's Office.

Enforcement

Failure to follow this policy and procedures may result in disciplinary action. Unauthorized transfer, disposal, or misuse of IT assets is strictly prohibited.

PUEBLO CITY-COUNTY
Library District

INFORMATION TECHNOLOGY

05.03.01 Software Licensing and Management

Pueblo City-County Library District (PCCLD) requires the responsible, lawful, and secure use of all software utilized within the organization. This policy establishes requirements for the acquisition, licensing, installation, and management of software in order to ensure compliance with licensing agreements, support operational needs, control costs, and reduce cybersecurity and legal risks associated with unauthorized or unmanaged software.

This policy applies to all employees, contractors, and authorized users of PCCLD technology resources, and to all software installed on or accessed through PCCLD-owned or managed devices, servers, systems, and cloud-based platforms.

All software used within the PCCLD environment must be properly licensed, approved, and managed by the IT Department. Software may only be acquired through authorized procurement processes and must align with organizational business needs, security requirements, and technical standards.

The IT Department is responsible for installing, maintaining, and management of software. Software licensing vetting and management will be completed through various means including but not limited to advisory oversight. PCCLD reserves the right to conduct software audits and to remove or restrict access to software that is found to be unlicensed, unsupported, insecure, or otherwise non-compliant with this policy.

Unauthorized, unlicensed, or personally obtained software is strictly prohibited from being installed or used on PCCLD systems.

Failure to comply with this policy may result in the removal of unauthorized software and may lead to disciplinary action in accordance with PCCLD policies and employee guidelines.

PUEBLO CITY-COUNTY Library District

INFORMATION TECHNOLOGY

05.03.01.P1 Software Licensing and Management Procedures

Software Request and Intake

All software must be formally requested prior to acquisition or installation. Requests must be submitted using the PCCLD Software Vetting Checklist and Intake Form and must include business justification, intended use, user scope, data classification, and deployment type. No software may be installed, purchased, or subscribed to outside this process.

Vendor and Security Review

The IT Department is responsible for reviewing vendor background, software security posture, and known vulnerabilities. This includes evaluation of vendor reputation, patch practices, support lifecycle, and publicly disclosed security issues. Software presenting unacceptable security or privacy risk may be denied or require documented risk acceptance.

Licensing Review

The IT Department evaluates software licensing models and terms, including usage limitations, audit rights, renewal requirements, and financial exposure. Licenses with unclear terms or aggressive audit enforcement may be escalated for additional review.

CAB Review and Approval

All software requests and IT findings are reviewed by the Change Advisory Board (CAB). The CAB makes recommendations on approval, denial, conditional approval, or risk acceptance. Approved software may only be deployed by the IT Department.

Testing and Pilot (When Applicable)

For high-impact or high-risk software, the IT Department may require limited pilot deployment, security testing, or compatibility validation prior to full approval.

Inventory and Ongoing Management

The IT Department maintains a centralized inventory of approved software and licenses. License usage and compliance are monitored periodically. Software renewals, vendor changes, and emerging risks are reviewed as part of ongoing management.

Exceptions and Enforcement

Exceptions to these procedures must be documented and reviewed/approved by the CAB, the Director of IT or Executive Director (or designee). Unauthorized or unmanaged software is subject to removal. Failure to comply with these procedures may result in disciplinary action.

PUEBLO CITY-COUNTY Library District

INFORMATION TECHNOLOGY

05.03.01.F1 Software Vetting Checklist & Intake Form

Requester Information

Requesting Department: _____

Requester Name & Title: _____

Date of Request: _____

Urgency / Timeline: _____

Software Overview

Software Name: _____

Vendor Name: _____

Website / Documentation URL: _____

Type (SaaS / On-Prem / Open Source / Other): _____

Business Justification

Primary Business Use Case:

Users / Departments Impacted: _____

Is this replacing an existing tool? If yes, which? _____

_____

Data & Security Review

Data Classification Involved: _____

Authentication Method: _____

Encryption at Rest and In Transit? (Yes/No): _____

Known CVEs or Security History Reviewed? (Yes/No): ___

Vendor & Risk Review

Vendor Longevity and Stability Reviewed? (Yes/No): ___

Patch and Update Cadence: _____

Incident or Breach History? (Yes/No/Details): _____

Licensing & Audit Considerations

License Model: _____

Audit Rights Present? (Yes/No): _____

True-Up or Reconciliation Required? (Yes/No): _____

Auto-Renewal Clauses? (Yes/No): _____

IT Decision

Decision (Approved / Denied / Risk Accepted): _____

Conditions or Notes:

Approving Authority: _____

Approval Date: _____