PUEBLO CITY-COUNTY Library District

www.pueblolibrary.org

Information Technology Policies and Procedures

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

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.