**PUEBLO CITY-COUNTY**
**Library District**

www.pueblolibrary.org

# Information Technology Policies and Procedures

# TABLE OF CONTENTS

## 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

*INFORMATION TECHNOLOGY–*                        *Adopted: 02-27-2025*
*Acceptable Use of Information Technology*                    *05.01.01*
*2 of 2*

**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.