Basalt Regional Library District

Electronic Access Policy

It is the policy of the Basalt Regional Library District's (BRLD) Board of Trustees to provide Internet access to its patrons and guests.

BRLD understands the important role the Internet and electronic resources play in today's society. Therefore, BRLD maintains public computers, wireless Internet service, and reputable databases for the convenience of our guests and patrons.

BRLD adheres to the USA Patriot Act, the Children's Internet Protection Act (CIPA), and the Child Online Protection Act (COPA).

1. Each Internet accessible computer has security software which will automatically delete any changes made during a user's session once the computer is rebooted or shut down at the end of the session. Patrons are advised to save files to the cloud or onto a flash drive.
2. Patrons must have a BRLD library card if they wish to use an Internet accessible computer. Guests may request a "Guest Pass."
3. Computer users may use the computer in blocks of one-hour sessions. Library staff has the authority to grant or deny extended computer time on an individual basis if computers are available.
4. All public computer stations and network connections (including wireless) in the library are filtered according to Federal and State law. Filters are software programs that block access to material that may be considered offensive. No filter is 100 percent effective. Parents or legal guardians of minors must assume responsibility for their children's use of the computers.
5. The information resources available through the Internet exist beyond the scope of BRLD's Collection Development policy. BRLD is not responsible for the accuracy or validity of information found on the Internet. Patrons should consider the source and timeliness of all information retrieved through the Internet. BRLD subscribes to several reputable databases that are available to our patrons.
6. Unauthorized Use: Illegal activities or any other activities intended to disrupt the network services or equipment are prohibited. Unauthorized use includes, but is not limited to, the following:
    a. Disrupting or causing damage to library programs, data, or equipment
    b. Disassembling computers or disconnecting network or power cables from computer or wall
    c. Unauthorized monitoring of electronic communications
    d. Unauthorized entering of other machines accessible via the library's networks

e. Intentionally propagating computer worms, viruses or other malicious software
f. Interfering with another patron's privacy or use of a library terminal
g. Fraudulently obtaining access to Internet sites including falsification of age, and unauthorized use of computer accounts, access codes or network identification numbers
h. Unauthorized use or copying of information posted on the Internet
i. Distributing unsolicited advertising or spam
j. Violating software licensing agreements and/or copyright laws

Unauthorized access of a computer, computer network, computer system, or any part thereof, or exceeding authorized access to a computer, computer network, computer system, or any part thereof, is a crime under Colorado law (Colorado Revised Statutes, Sec. 18-5.5-102). Unauthorized use may result in the loss of library privileges. Violators may also be subject to criminal prosecution or other legal action.

7. Patrons of BRLD shall be prohibited from invading the privacy of any computer user. Each patron must comply with the BRLD's Behavior Policy and should be considerate of all library users and library staff. Computer users must be aware that the U.S.A. Patriot Act gives authorities the legal right to access information from computers in the library. In the event of a request for information from a law enforcement agency, the Executive Director will contact BRLD legal counsel for advice on how to respond to the request.
8. The American Library Association's Freedom to Read Statement (attached hereto as Exhibit B) and the Library Bill of Rights (attached hereto as Exhibit C) are adopted policies of the Board of Trustees.
9. The library will not be responsible for any information (i.e. credit card) that is compromised, or for any damage caused to your hardware or software due to electric surges, security issues, or consequences caused by viruses or hacking.

Review Date: April 2015, March 2022