APPENDIX A

ACCEPTABLE USE OF DISTRICT TECHNOLOGY

[Note: Substitute the word "volunteer" for "employee" and "volunteer services" for "employee job duties."]

The District's computer equipment, software, operating systems, storage media, internet connection, electronic mail (e-mail), cell phones, pagers and portable radios are all important technology assets and resources for the District. These important technology assets and resources are provided for use consistent with the District's business operations. The Board of Directors have adopted this "Acceptable Use of District Technology" regulation, which may be amended from time to time. Each employee is expected to use the District's technology assets and resources in a manner consistent with Section 17 of the *Carbon County Fire Protection District Personnel and Benefits Manual (2023)* and this regulation.

From time to time the District Chief, in conjunction with the District's contracted Information Technology provider may provide guidances and directives to District employees so as to maintain the operation and security of the District's technology assets and resources. Employees are expected to conduct themselves in accordance with those guidances and directives.

A. District's Computer Equipment, Software, Operating Systems, Storage Media, Cell Phones, Pagers, Portable Radios.

Employees are expected to respect, protect, and use the District's computer equipment, software, operating systems, storage media, and cell phones, pagers and portable radios at all times, in a manner so as to not damage or compromise these District assets and resources in any fashion. Employees who receive District technology equipment are responsible for that equipment. Each employee who receives District technology equipment is required to sign and comply with the terms of the *District Equipment Agreement*, a copy of which is attached as Exhibit A-1.

The introduction of viruses or malicious tampering with any computer equipment, software, operating systems, storage media and cell phones , pagers and portable radios is strictly prohibited. Employees are not to remove or disable anti-virus or security software or re-configure settings and firewalls unless authorized to do so, in writing, by the District Chief and/or the District's contracted Information Technology provider.

No personal or non-District provided devices, including but not limited to phones, flash drives, music player, discs, or anything else than can, interface with electronics either physically or wirelessly, shall be connected to District equipment (including computers, laptops, printers, copiers, tablets, and any other electronics), District networks (including ethernet, Wi-Fi, Bluetooth, etc.), District infrastructure, or District facilities unless specific written permission from the District Commissioners and/or the Information Technology Director is received prior to any

connection. Conversely, no District-provided equipment such as District-issued flash drives, printers, etc., shall be connected to other non-District provided equipment or devices. Specific exemptions may be authorized by the District Chief and/or District's contracted Information Technology provider for law enforcement purposes or other required government uses. Guest network access shall only be used for non-District provided devices that require temporary, short term internet access for government business purposes, such as presentations to the Board of Directors.

Employees must not store personal files such as music, video, photographs or games on the District's computer equipment or cell phones.

B. <u>Internet Use Guidelines</u>.

Use of the District's internet connection and services by all employees must be consistent with this acceptable use policy. It is expected that District employees will exercise good judgment and remain productive at work while using the internet. District internet users are required:

- To respect the privacy of other users. For example, users shall not intentionally seek information on, obtain copies of or modify files or data of other users, unless explicit permission to do so has been obtained;

- To respect the legal protection provided to software programs and data by copyrights and licenses;

- To protect data from unauthorized use or disclosure as required by state and federal laws and the requirements of District's business and governmental purposes;

- To limit <u>personal</u> use of the Internet connection and services to an absolute minimum.

It is not acceptable to use District's internet facilities:

- For activities unrelated to the District's business and governmental purposes;

- To access, post or participate in any type of social media unless during break periods, a part of the employee's job duties, or with the permission of the department head;

- For activities unrelated to official assignments and/or job responsibilities;

- For any illegal purposes, including any unauthorized or illegal acts like hacking, fraud, buying or selling illegal goods;

- To transmit threatening, obscene, or harassing materials or correspondence;
- For unauthorized distribution of District's data and information or confidential information;
- To interfere with or disrupt network users, services, or equipment;
- For private purposes such as marketing or business transactions;
- For solicitation of any kind, including profit and nonprofit;
- For revealing or publicizing proprietary or confidential information to unauthorized recipients;
- For representing personal opinions as those of the District or any of its elected officials.
- For uploading or downloading commercial software in violation of its copyright;
- For uploading or downloading pornographic or obscene materials, images or software;
- For intentionally interfering with the normal operation of any District internet service;
- To visit or connect to suspicious or potentially dangerous sites;
- To connect to or engage in conduct that introduce viruses or malware to infect or damage the District's computer equipment, software, operating systems, and storage media.

C. **E-Mail Use**.

- Every District employee and elected official is responsible for ensuring that the electronic mail system is used in accordance with this use policy. The e-mail system is part of the business equipment and technology owned by the District and should be used only for its business and governmental purposes. Personal business should not be conducted by means of the e-mail system and personal use should be kept to an absolute minimum. All of the guidelines developed for the use of the District internet connection and services apply to the use of e-mail.
- Neither elected officials, nor District employees, have a personal right of privacy in any matter created on, received through, or sent from the District e-mail system.

The District, its elected officials, department heads, Board of Directors and others, in its/their discretion, reserve the right to monitor and read, retrieve, print, and/or delete any matter created on, received through or sent from the District e-mail system.

- Employees should be aware that even when a message has been erased, it still might be possible to retrieve it from a backup system. Therefore, employees should not rely on the erasure of messages to assume a message is private.

- Even if an employee has a password for the e-mail system, it is impossible to ensure the confidentiality of any message created on, received through, or sent from the District e-mail system. Any employee password used must be known to the employee's department head as a need to access this information may occur during an employee's absence. Employees are not to share their passwords with persons other than the District Chief or Board of Directors.

- No e-mail messages should be created or sent that may constitute intimidating, hostile or offensive material on the basis of race, color, sex or gender, sexual orientation, gender identity or expression, national origin, religion, disability status, age, political affiliation, protected veteran status, genetics, or any other characteristic protected by federal or state laws. The District's policy against sexual harassment and harassment based on other protected characteristics applies fully to the e-mail system.

- Care should be exercised at all times in drafting e-mails as e-mail is as permanent and admissible in courts as paper communications. E-mails, both internal and external, can be subject to production and release under the Wyoming Public Records Act and under court discovery rules.

If an employee has any questions about what constitutes acceptable use of District technology, the employee should ask the District Chief for further guidance and clarification. Any employee who becomes aware of misuse of the District's computer equipment, software, operating systems, and storage media, internet connection or electronic mail (e-mail) should promptly notify the District Chief or any member of the Board of Directors.

D. **Notice of NO Privacy or Confidentiality for Employees.**

Pursuant to the Electronics Communications Privacy Act of 1986 (18 U.S.C. 2510 et seq.), as amended from time to time, notice is hereby given that there are NO facilities provided by this system for sending or receiving PRIVATE or CONFIDENTIAL electronic communications. The Carbon County Fire Protection District, its elected officials, District Chief, Board of Directors, employees and others have access to all e-mail and user access requests, and may monitor messages and the District's systems, as necessary to assure

efficient performance or appropriate or inappropriate use. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

Attachment: Exhibit A-1: District Equipment Agreement

Section 25 of the Carbon County Fire Protection District Volunteer Handbook concerning Acceptable Use of District Technology provides: Each volunteer will be provided a copy of the District's Acceptable Use of District Technology regulation as may be approved by the Board of Directors from time to time for its employees which criteria and procedures are applicable, substituting the word "volunteer" for "employee." Each volunteer is required to read and sign the Acceptable Use of District Technology regulation; it is the responsibility of each volunteer to be familiar with these procedures. The signing and compliance with the District's Acceptable Use of District Technology regulation does not make any volunteer a District employee. Nothing contained in this Section shall in any way abrogate the status of the District's volunteers as volunteers.

_____ _____

Date Signature of Volunteer

_____ _____

Date District Chief or Designee