RESOLUTION
OF THE
BOARD OF DIRECTORS
OF THE
ASPEN PARK METROPOLITAN DISTRICT

Adopting a Personal Data Privacy Policy

WHEREAS, the Aspen Park Metropolitan District (the "**District**") is a quasi-municipal corporation and political subdivision of the State of Colorado and a duly organized and existing special district pursuant to Title 32, Colorado Revised Statues; and

WHEREAS, the Colorado General Assembly adopted House Bill 18-1128 concerning strengthening protections for consumer data privacy (the "**Bill**") with an effective date of September 1, 2018; and

WHEREAS, the Bill added Article 73 to Title 24, Colorado Revised Statutes known as "Security Breaches and Personal Information" ("**Article 73**") which requires each Governmental Entity in the state that maintains paper or electronic documents during the course of business that contain Personal Identifying Information to develop a written policy for the destruction or proper disposal of such paper and electronic documents; and

WHEREAS, § 24-73-101(4)(a), C.R.S., defines a "Governmental Entity" as the state and any state agency or institution, including the judicial department, county, city and county, incorporated city or town, school district, special improvement district, authority, and every other kind of district, instrumentality, or political subdivision of the state organized pursuant to law. "Governmental Entity" includes entities governed by home rule charters; and

WHEREAS, the District is a Governmental Entity under Article 73 as it is a political subdivision of the state organized pursuant to law; and

WHEREAS, § 24-73-101(4)(b), C.R.S., defines "Personal Identifying Information" as a social security number; a personal identification number; a password; a pass code; an official state or government-issued driver's license or identification card number; a government passport number; biometric data, as defined in § 24-73-103(1)(a), C.R.S.; an employer, student, or military identification number; or a financial transaction device, as defined in § 18-5-701(3), C.R.S.; and

WHEREAS, the District may maintain paper or electronic documents that contain Personal Identifying Information; and

WHEREAS, the District has developed and desires to adopt a written policy for the destruction or proper disposal of paper and electronic documents containing Personal Identifying Information, in conformance with Article 73.

NOW, THEREFORE, BE IT RESOLVED BY THE BOARD AS FOLLOWS:

1. Adoption of Personal Data Privacy Policy. The District hereby adopts the Personal Data Privacy Policy set forth in **Exhibit A**, attached hereto and incorporated herein.

2. Preambles Incorporated. The preambles to this Resolution are hereby incorporated into this Resolution as if set out fully herein.

3. Severability. If any part, section, subsection, sentence, clause or phrase of this Resolution is for any reason held to be invalid, such invalidity shall not affect the validity of the remaining provisions.

4. Effective Date. This Resolution shall become effective as of September 1, 2018, shall be enforced immediately thereafter and shall supersede any previous policy related to disposal of paper and electronic documents containing Personal Identifying Information. This Resolution shall be implemented and administered by the District to conform with all requirements of Article 73, as modified from time to time.

[Signature page follows.]

ADOPTED this 21st day of May, 2019

ASPEN PARK METROPOLITAN DISTRICT, a quasi-municipal corporation and political subdivision of the State of Colorado

Officer of the District

ATTEST:

APPROVED AS TO FORM:

WHITE BEAR ANKELE TANAKA & WALDRON
Attorneys At Law

Heather L. Hart

General Counsel to the District

Signature page to Resolution Adopting Personal Data Privacy Policy

EXHIBIT A

Personal Data Privacy Policy

The purpose of this Personal Data Privacy Policy is to comply with § 24-73-101 (1), C.R.S., which requires a Governmental Entity that maintains paper or electronic documents during the course of business that contain Personal Identifying Information to develop a written policy for the destruction or proper disposal of such paper and electronic documents.

Section 1. Definitions

(1) "District" means the Aspen Park Metropolitan District

(2) "Personal Identifying Information" means the following, which the District may collect over the course of normal business:

a. A social security number;
b. A personal identification number;
c. A password;
d. A pass code;
e. An official state or government-issued driver's license or identification card number;
f. A government passport number;
g. Biometric data, as defined in § 24-73-103(1)(a), C.R.S.;
h. An employer, student or military identification number; or
i. A financial transaction device, as defined in § 18-5-701(3), C.R.S.

(3) "Third-Party Service Provider" means an entity that has been contracted by the District to maintain, store, or process Personal Identifying Information on behalf of the District.

(4) All defined terms in section 5 shall be defined as in § 24-73-103, C.R.S.

Section 2. Security Procedures and Practices

(1) The District will store paper documents containing Personal Identifying Information in a locked cabinet or locked office. Only employees or individuals who must use Personal Identifying Information to conduct District business will have access to the storage location.

(2) The District will take appropriate measures to protect Personal Identifying Information stored as digital media. These protections may include password access, firewalls and encryption software. Only those employees or individuals who must use the Personal Identifying Information to conduct District business will have access to the electronic storage system(s).

(3) In the event an employee's or individual's responsibilities in relation to the District change such that the employee or individual no longer must use Personal Identifying Information to conduct District business, the District shall take reasonable measures to terminate that employee's or individual's access to Personal Identifying Information, such as replacing locks on any storage cabinet or locked office where Personal Identifying Information is stored in paper format, or denying the employee or individual access to Personal Identifying Information stored digitally by changing passwords or access settings.

(4) In the event the District discloses Personal Identifying Information to a Third-Party Service Provider, the District will require the Third-Party Service Provider to implement and maintain reasonable security procedures and practices that are:

a. Appropriate to the nature of the Personal Identifying Information disclosed to the Third-Party Service Provider;

b. Are reasonably designed to help protect the Personal Identifying Information from unauthorized access, use, modification, disclosure, or destruction; and

c. Are in accordance with the policies and procedures set forth in this Policy.

Section 3. Records Management and Destruction

(1) Records maintaining Personal Identifying Information should be retained in accordance with the District's Records Retention Policy. All paper or electronic documents containing Personal Identifying Information that are no longer needed, shall be destroyed by the District in accordance with the District's Records Retention Policy, and in accordance with the retention periods set forth therein, based on the type of record. When destroyed, all records containing Personal Identifying Information must be disposed of by shredding, erasing or otherwise modifying the Personal Identifying Information in the paper or electronic documents in a manner that renders the Personal Identifying Information unreadable or indecipherable through any means.

Section 4. Open Records Disclosure

(1) The District is governed by the Colorado Open Records Act ("CORA"). Any records maintained by the District may be subject to inspection and copying by members of the public, unless an exemption in the law exists. In the event the District must release records containing Personal Identifying Information, sensitive data will be redacted or otherwise removed to protect the privacy of the individual(s).

(2) The District will not otherwise release Personal Identifying Information unless legally required to do so in connection with legal proceedings or law enforcement

investigations. The District will not sell Personal Identifying Information to any outside organization.

Section 5. Notification of Security Breach

(1) In the event the District becomes aware that a Security Breach may have occurred, the District will conduct in good faith a prompt investigation to determine the likelihood that Personal Information, as defined in § 24-73-103(1)(g)(i)(A) has been or will be misused. The District will notify the affected Colorado residents in accordance with the notice requirements set forth in § 24-73-103, C.R.S., unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur.