RESOLUTION NO. 2019 –02

A RESOLUTION OF THE TOWN COUNCIL OF THE TOWN OF RIDGWAY, COLORADO, ADOPTING A POLICY CONCERNING THE DESTRUCTION, DISPOSAL AND PROTECTION OF RECORDS CONTAINING PERSONAL IDENTIFYING INFORMATION

WHEREAS, during the 2018 legislative session, the state of Colorado adopted House Bill 18-1128, which was enacted as C.R.S. § 6-1-713, 713.5, 716 for certain covered entities and § 24-73-101, *et seq.* (the "Act") for government entities, and went into effect on September 1, 2018; and

WHEREAS, the Act requires all "governmental entities," which includes home rule towns, to adopt and maintain a written policy for the destruction or disposal of paper and electronic documents containing "Personal Identifying Information;" and

WHEREAS, the Act also sets forth requirements regarding the protection of Personal Identifying Information and procedures to follow in the event of a breach; and

WHEREAS, in order to ensure compliance with the Act, the Town Council of the Town of Ridgway ("Town") desires to adopt a policy concerning the destruction, disposal and protection of Personal Identifying Information that shall apply to all employees and elected officials of the Town.

NOW, THEREFORE, BE IT RESOLVED THAT THE BOARD OF TRUSTEES HEREBY ADOPTS THE TOWN OF RIDGWAY POLICY CONCERNING THE DESTRUCTION, DISPOSAL AND PROTECTION OF RECORDS CONTAINING PERSONAL IDENTIFYING INFORMATION, AS SET FORTH BELOW:

Section 1. The Town hereby adopts the attached Policy Concerning the Destruction, Disposal and Protection of Records Containing Personal Identifying Information attached hereto and incorporated herein as Exhibit A.

INTRODUCED, READ, PASSED, AND ADOPTED THIS ____ DAY OF _____, 2019.

TOWN OF RIDGWAY, COLORADO

By: _____
JOHN CLARK, Mayor

ATTEST:

By: _____
PAM KRAFT, Town Clerk

EXHIBIT A

POLICY CONCERNING THE DESTRUCTION, DISPOSAL AND PROTECTION OF RECORDS CONTAINING PERSONAL IDENTIFYING INFORMATION

ARTICLE I. PURPOSE

The purpose of this Policy Concerning the Destruction, Disposal and Protection of Records Containing Personal Identifying Information ("**Policy**") is to provide guidance to Town of Ridgway employees, department heads and elected officials (collectively referred to herein as the "**Town Parties**") for the proper handling of Personal Identifying Information, as required by C.R.S. § 24-73-101, *et. seq.* (the "**Act**").

This Policy shall establish a written policy for the destruction or proper disposal of paper and electronic records containing Personal Identifying Information (defined below) and set forth requirements regarding the protection of Personal Identifying Information, and procedures should a breach regarding Personal Identifying Information occur.

This Policy shall apply to all Town Parties.

ARTICLE II. DEFINITIONS

1. **"Biometric Data"** means unique biometric data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account.

2. **"Departments"** means all current Town departments and any department added after the adoption of this Policy.

3. **"Determination that a Security Breach Occurred"** means the point in time at which there is sufficient evidence to conclude that a security breach has taken place.

4. **"Encrypted"** means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

5. **"Medical Information"** means any information about a consumer's medical or mental health treatment or diagnosis by a health care professional.

6. **"Notice"** means:

    a. Written notice to the postal address listed in the Town records;
    b. Telephonic notice;

c. Electronic notice, if a primary means of communication by the Town with a Colorado resident is by electronic means or the notice provided is consistent with the provisions regarding electronic records and signatures set forth in the federal "Electronic Signatures in Global and National Commerce Act," 15 U.S.C. sec. 7001 *et seq.;* or
d. Substitute notice, if the Town demonstrates that the cost of providing notice will exceed two hundred fifty thousand dollars, the affected class of persons to be notified exceeds two hundred fifty thousand Colorado residents, or the Town does not have sufficient contact information to provide notice. Substitute notice consists of all of the following:
    i. E-mail notice if the Town has e-mail addresses for the members of the affected class of Colorado residents;
    ii. Conspicuous posting of the notice on the Town website; and
    iii. Notification to major statewide media.

7. "Personal Identifying Information" means 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 C.R.S. § 24-73-103(1)(a); an employer, student, or military identification number; or a financial transaction device, as defined in C.R.S. § 18-5-701(3), or date and place of birth, mother's maiden name, criminal, medical records, financial records, and educational transcripts (see 2 C.F.R. § 200.82).

8. "Personal Information" means:

    a. A Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable: social security number; driver's license number or identification card number; student, military, or passport identification number; medical information; health insurance identification number; or Biometric data, as defined above;
    b. A Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account; or
    c. A Colorado resident's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.
    d. "Personal Information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

9. "Security Breach" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of Personal Information

maintained by the Town. Good faith acquisition of Personal Information by an employee or agent of the Town for the purposes of the Town is not a security breach if the Personal Information is not used for a purpose unrelated to the lawful government purpose or is not subject to further unauthorized disclosure.

10. **"Third-Party Service Provider"** means an entity that has been contracted to maintain, store, or process Personal Identifying Information on behalf of the Town.

The definitions set forth in the Act are hereby incorporated into this Policy to the extent not set forth above. In the event of any conflict between a definition in the Act and a definition in this Policy, the definition in the Act shall control.

ARTICLE III. DISPOSAL OF PERSONAL IDENTIFYING INFORMATION

Section 1. Disposal and Destruction. Unless otherwise required by state or federal law or regulation, after a record has met the minimum retention period as defined in the Town's Records Retention Schedule, as amended from time to time, paper or electronic records within the custody or control of the Town that contain Personal Identifying Information will be destroyed by either shredding, erasing, or otherwise modifying the Personal Identifying Information to make the Personal Identifying Information unreadable or indecipherable through any means. Each Town department shall implement procedures and policies to address the specific nature of its records to ensure compliance with this Policy and the Act. The Town shall not be responsible for ensuring destruction of Personal Identifying Information by any Town Party that is required by state or federal agencies to use one or more software programs, which may include storage of data, located on servers not within the immediate control of the Town.

Section 2. Litigation Holds. A "**Litigation Hold**" refers to a period of time when Town Parties have a duty to preserve certain records that may be pertinent to anticipated, pending or ongoing litigation. Such period of time commences when the litigation involving the Town is initiated or reasonably anticipated or foreseeable. During such period, Town Parties shall preserve all records directly or indirectly related to such pending or threatened litigation and suspend deletion, destruction or disposal of such records. A Litigation Hold overrides a record that is eligible for destruction under the Town Records Retention Schedule or Article III of this Policy.

ARTICLE IV. PROTECTION OF PERSONAL IDENTIFYING INFORMATION

Section 1. Protection by the Town. The Town shall protect Personal Identifying Information from unauthorized access, use, modification, disclosure, or destruction. Each department shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the Personal Identifying Information given the nature and size of the Town.

Section 2. Third Party Service Providers. The Town shall require any Third-Party Service Provider it engages to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the Personal Identifying Information disclosed to the Third-Party

Service Provider and reasonably designed to help protect the Personal Identifying Information from unauthorized access, use, modification, disclosure, or destruction. Each department shall ensure that in all contracts with Third Party Service Providers that either do, or could result in, the exchange of personal identifying information, contain contractual terms to ensure such Third Party Service Providers are subject to and abiding by the terms of the Act and this Policy.

It shall not be considered a disclosure of Personal Identifying Information to a Third-Party Service Provider if the Town retains primary responsibility for implementing and maintaining reasonable security procedures and practices appropriate to the nature of the Personal Identifying Information and the Town implements and maintains technical controls reasonably designed to help protect the Personal Identifying Information from unauthorized access, modification, disclosure, or destruction; or effectively eliminate the Third-Party Service Provider's ability to access the Personal Identifying Information, notwithstanding the Third-Party Service Provider's physical possession of the Personal Identifying Information.

ARTICLE V. INTERNAL NOTIFICATION AND INVESTIGATION OF SUSPECTED SECURITY BREACH OF PERSONAL INFORMATION

If any Town Party suspects that a Security Breach may have occurred, it must immediately notify the Town Manager and conduct a good faith and prompt investigation to determine the likelihood that Personal Information has been or will be misused.

Unless the investigation determines that the misuse of information regarding a Colorado resident has not occurred and is not reasonably likely to occur, the Town shall give Notice to the affected Colorado residents, as provided in Article VI and take further action as necessary under Article VII. If the investigation determines that the misuse of information regarding a Colorado resident has not occurred and is not reasonably likely to occur, the Town shall not take further action pursuant to this Policy.

ARTICLE VI. NOTICE OF BREACH IF MISUSE OF INFORMATION HAS OCCURRED OR IS REASONABLY LIKELY TO OCCUR

If the Town determines that a Security Breach occurred, the Town shall provide Notice to affected Colorado residents as set forth in this Article VI.

Section 1. Timing of Notice. Notice shall be in the most expedient time possible and without unreasonable delay, but no later than thirty (30) days after the date of determination that a Security Breach occurred. Provision of Notice shall be consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the Security Breach and to restore the reasonable integrity of the computerized data system.

Section 2. Content of Notice. If the Town is required to provide Notice, it shall provide the following information to all affected Colorado residents:

1. The date, estimated date, or estimated date range of the Security Breach;
2. A description of the Personal Information that was acquired or reasonably believed to have been acquired as part of the Security Breach;
3. Information that the resident can use to contact the Town to inquire about the Security Breach;
4. The toll-free numbers, addresses, and websites for consumer reporting agencies;
5. The toll-free number, address, and website for the Federal Trade Commission; and
6. A statement that the resident can obtain information from the Federal Trade Commission and credit reporting agencies about fraud alerts and security freezes.

If the investigation determines that the type of Personal Information that was misused or is reasonably likely to be misused is a Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account, the Town shall, in addition to the Notice otherwise required above, in the most expedient time possible and without unreasonable delay, but not later than thirty (30) days after the date of determination that a security breach occurred, consistent with the legitimate needs of law enforcement and consistent with any measure necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system:

1. Direct the person whose Personal Information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose Personal Information has been breached uses the same username or e-mail address and password or security question or answer.

2. If the Security Breach pertains to the log-in credentials of an email account furnished by the Town, rather than giving notice via email, the Town may comply with this section by providing notice by other methods specified under "Notice" in Article II or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an internet protocol address or online location from which the Town knows the resident customarily accesses the account.

The breach of encrypted or otherwise secured Personal Information must be disclosed in accordance with this section if the confidential process, encryption key, or other means to decipher the secured information was also acquired in the Security Breach or was reasonably believed to have been acquired.

Section 3. Costs. The Town shall not charge the cost of providing such Notice to individuals.

Section 4. Third-Party Service Providers. If the Town uses a Third-Party Service Provider to maintain computerized data that includes Personal Information, the Town shall require that the Third-Party Service Provider give notice to and cooperate with the Town in the event of a Security Breach that compromises such computerized data. Compliance shall include notifying the Town

of any Security Breach in the most expedient time and without unreasonable delay following discovery of a Security Breach, if misuse of Personal Information about a Colorado resident occurred or is likely to occur. Cooperation includes sharing with the Town information relevant to the Security Breach; except that such cooperation does not require the disclosure of confidential business information or trade secrets.

Section 5. Delay by Law Enforcement. Notice required by this section may be delayed if a law enforcement agency determines that such Notice will impede a criminal investigation and the law enforcement agency has directed the Town not to send the Notice required by this section.

ARTICLE VII. FURTHER REPORTING REQUIREMENTS

Section 1. Notice to Colorado Attorney General. If the Security Breach is reasonably believed to have affected five hundred (500) Colorado residents or more, the Town shall provide notice of such Security Breach to the Colorado Attorney General in the most expedient time possible and without unreasonable delay, but not later than thirty (30) days after determination of that a Security Breach occurred.

Section 2. Notice to Consumer Reporting Agencies. In the event the Town is required to provide Notice, as defined in Article II, to more than one thousand (1,000) Colorado residents, the Town shall also notify, in the most expedient time possible and without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by the federal "Fair Credit Reporting Act", 15 U.S.C. sec. 1681a (p), of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified. The Town is not required to provide to the consumer reporting agency the names or other Personal Information of Security Breach Notice recipients.

ARTICLE VIII. WAIVER

Any waiver of these notification rights or responsibilities is void as against public policy. The Town shall not elicit or accept any waiver of these notification rights or responsibilities.