BIG FLATS POLICY ON MANAGING PERSONAL, PRIVATE OR SENSITIVE INFORMATION

1. Personal, private or sensitive information is any information where unauthorized access, disclosure, modification, destruction or disruption of access to or use of such information could significantly impact an organization, its employees, its customers, citizens or third parties. PPSI includes, but is not limited to:

A. information concerning a person which, because of name, number, personal mark or other identifier, can be used to identify that person, in combination with their social security number (SSAN), driver's license number, mother's maiden name or financial account identifiers or other information which would permit access to a person's financial resources or credit;

B. information that is used to authenticate the identity of a person (e.g., password, SSAN, PIN);

C. security related information (e.g., system and network designs, data storage locations, vulnerability reports, risk assessments);

D. information that identifies specific structural, operational or technical information, such as maps, mechanical or architectural drawings, floor plans, operational plans or procedures, or other detailed information relating to electric, natural gas, steam, water supplies, nuclear or telecommunications systems or infrastructure, including associated facilities; and

E. other information that is protected from disclosure by law or relates to subjects and areas of concern. For further information, see Cyber Security Policy & Standard PS08-001: Information Classification and Control, Office of Cyber Security & Critical Infrastructure Coordination, last revised December 4, 2008.

2. The storage electronically or otherwise of social security numbers as employee identifiers on paper and electronic correspondence is to be avoided. The same applies to information obtained from individuals who come onto Town property to obtain marriage licenses, hunting licenses. This includes information on credit cards, driver's licenses, checking accounts, and any other personal, private and sensitive information (PPSI). If any of that information is obtained in the course of having to identify an individual, then it should be shredded or in some way securely disposed of as soon as possible. It is advisable to use the last 4 digits of a SSAN and discard the rest of that number. Only in unusual circumstances, such as in the bookkeeping payroll department, should any of that information be retained and if it is retained, for example

for town employment purposes, then it must be stored in a secure manner. If it must be physically stored then it should be placed in a place secured by a lock with the key or combination held only by the Town Clerk, the Deputy Clerk, the Bookkeeper and/or the Town Supervisor. If it is electronically stored than the employee needing that information shall ensure that it is not accessible by others and is secured by a password, etc. If a notary public needs to store identifying information, then the notary public shall ensure that that information is securely stored.

When a form/permit/or receipt is provided to an individual it can be noted that the individual paid by cash or check and the check number can be noted but not the account routing information.

No one should ask for credit card account number to be sent through mail unless required for a form or permit or some other document. Any email containing a credit card account number should be shredded as soon as possible. An individual can provide an account number if needed via the phone so it can be keyed in or the individual can go online and if something they need requires an account number, they can enter that themselves.

The collection and retention of PPSI is to be the least amount necessary to conduct the Town's business.

3. Employees shall receive training in the storage and safeguarding of PPSI. The training can include communicating Town policies and procedures; discussing new scams that are being used to steal information and other social engineering reminders; providing updates on privacy items in the news, such as recent government data security breaches and how they occurred; and reminding employees about the need to limit the type of sensitive information collected, accessed, or displayed to that which is essential for the function to be performed. Also, training could emphasize the importance of establishing limits for downloads of sensitive information into spreadsheets or other formats to workstations, laptops, or storage devices – unless the data is encrypted or under strict controls – and establishing effective methods for disposing of devices or data that contain sensitive information.

4. The Town shall establish a procedure for town-wide data classification. The Town shall regularly review its holdings of previously collected PPSI in order to determine whether continuing to collect such information is still relevant or necessary for meeting its business purpose and if the legal retention period for this information has been satisfied. Data that is no longer necessary or has exceeded the legal retention period should be disposed of properly.

5. Unless otherwise required by law, an employer shall not publicly post or display an employee's or any individual's social security number; visibly print a social security number on any identification badge or card, including any time card; place a social security number in files with unrestricted access; or communicate an employee's personal identifying information (which includes social security numbers) to the general public.

An individual shall never be required to use his/her SSAN to access the Town's website or any part thereof, unless a password or unique personal identification number or other authentication is also required to access the Town's website.

An individual's SSAN, except the last four digits thereof, shall not be included on any materials mailed to that individual or in any mail copied to third parties, unless State or Federal law requires the SSAN to be on the document being mailed. Mailing includes texting, email or any electronic communication. However, not withstanding the above, SSANs may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the SSAN. Any SSAN that can be mailed may not be printed in whole or in part on a postcard or other mailer not requiring an envelope, nor shall the SSAN be visible on the envelope or without the envelope having been opened.

A SSAN shall not be encoded or embedded in or on a card or document, including, but not limited to, using a bar code, magnetic strip, or other technology, in place of removing the SSAN as required herein.

6. The use of credit card information shall follow the Payment Card Industry Data Security Standard (PCI DSS) which was adopted by the credit card organizations that process, store or transmit sensitive cardholder information such as primary account numbers and three or four character authorization codes. The utilization of this standard is aimed at protecting cardholder data and preventing its unauthorized use, whether the data is printed or stored locally, or transmitted over a public network to a remote server or service provider. See https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf.

7. If credit cards are accepted for payment and the card information is submitted by email, mail or in writing then the PPSI including the credit card type, expiration date, three or four character authorization code, payer name as it appears on the credit card, primary account number, and signature, in addition to the preprinted information relating to the bill being paid once used to achieve payment shall be completely blacked out completely and shall be destroyed if no longer needed. Any such information stored by the Town shall be periodically reviewed to remove no longer needed information. The three or four character authorization codes should never be stored under any circumstances.

8. Every effort shall be made to ensure that any PPSI is not on the Town's web site.

9. The Town Board shall establish a procedure, if necessary to go beyond what is set forth above, classifying data and assigning levels of sensitivity there to and set forth the security safeguards to be applied to each classification. For example classifications can be public data, internal use only data, confidential data and/or personal and restricted confidential data.

The internal controls that can be established over data are generally based on the potential harm that could result to individuals and/or the Town if the information were to be inappropriately accessed, used or disclosed.

10. The Town Board or the Town Supervisor must establish a disaster recovery plan including policies and procedures to back up data and systems on a regular basis to ensure data is not lost if the system were to become compromised. There also should be formal policies and procedures for the addition, deletion, updating and monitoring of network user accounts.

11. If the network is accessible to employees and officer then user IDs should be set up. User IDs enable the system to recognize specific user accounts and grant the appropriately authorized access rights and provide user accountability for computer transactions. Each individual on the network should be assigned a unique user ID. If user IDs are not affiliated with a specific user, but shared among multiple users, Town officials will be unable to determine responsibility for system activities. Access authorizations should be monitored and adjusted on an ongoing basis to accommodate new and departing employees and changes in users' responsibilities and related access needs. Usage of the network should be periodically reviewed.

12. The Town's internal control system should include a formal disaster recovery plan to address the possible loss of computer equipment and data, and establish procedures for recovery in the event of such a loss.

13. Policies and procedures should be established to require data to be backed up (i.e., a copy made) on a routine basis and the backup copies be stored in an environmentally and physically secure off-site location. To establish the validity of this process, backup data must be tested and restored on a periodic basis.