Village of Millbrook

Electronic Devices & Information Technology (I/T) Policy

A. Phone Usage Guidelines
B. Email Usage Guidelines
C. Social Media Usage Guidelines
D. Use of Electronic Devices during Board Meetings
E. Computer Systems Usage Guidelines
F. Computer Back Up Procedure- *updated 1.14.2020*
G. Breach Procedure

Adopted:

Village of Millbrook

Electronic Devices & I/T Policy

A. Phone Usage Guidelines

Telephone and cell phone usage must adhere to the following guidelines:

- An employee must answer promptly and speak in a clear, friendly and courteous tone;
- An employee must give the name of the department or office and one's own name. If the call is not for the employee who answers, the employee must transfer the caller to the correct party or take a message recording all pertinent information;
- If the call must be place on hold, the employee who answered the call must return to the line frequently to confirm that the call is being transferred;
- During office hours, each employee is responsible for there being at least one employee in the department or office to answer telephones. If the department or office has a limited staff, arrangements must be made with another department or office for telephone coverage or an answering device must be in operation;
- Collect calls may not be accepted without the approval of the Department Head or Mayor;
- An employee may make personal telephone calls, however, such calls should be limited in duration and frequency and must not interfere with the performance of the employee's job duties;
- An employee may not make or receive personal calls on a Village provided telephone or cell phone that will result in additional charges to the Village, except in an emergency and/or with prior approval from the Department Head. The employee must reimburse the Village for the cost of the call.

B. Email Policies and Procedures

1. General Policies

1.1 Ownership of Email

The Village legally owns all emails that employees and officials create and receive when conducting Village business, regardless of where employees and officials create and receive the emails. Employees and officials have no promise of personal privacy when using email on behalf of the Village.

- All email users of Village email accounts will acknowledge that they understand the Village's policy on email ownership each time they log into the Village's system.
- Email users who work at home (the Village Planning Board/ZBA secretary, Board members, Mayor, Building Inspector/CEO, Public Works Supervisor) should have separate email accounts for Village-related emails or, at minimum, should maintain Village emails separately from personal emails.

1.2 Training

- The Village Clerk will ensure training on the email system for all new Village officials and employees, and will also provide ongoing training, especially after upgrades or transitions to new email programs.
- New employees will not have access to and use of a Village email account until they are trained on the Village's email policies and procedures.

2. Managing Email

The Village manages most email as general correspondence and follows the retention periods for general correspondence in the Records Retention and Disposition Schedule MU-1. The Village manages and preserves emails with a retention period of longer than six years in a central file directory on the Village's main server, and ensures email with a retention period of six years or less is destroyed after six years.

2.1 Classifying Email

- Email users are responsible for classifying emails, on receipt or before transmission, as either not records or as permanent records. Non-records and permanent records are defined as follows:
- Emails that are not records include listserv messages distributed to many recipients, spam, broadcast messages received by officials and employees, and personal messages. A user may destroy non-records immediately.
- Permanent emails document significant policy, decision making, events, or legal issues, or pertain to legal precedents.

- Users must remove permanent emails from their individual email accounts and store them in the shared file directory on the Village's main server.
- The Village's email archiving appliance will capture all emails, including permanent emails, and will prevent modification or deletion of archived email.

2.2 Managing Retention and Disposition

- Permanent emails will be managed and preserved in the shared file directory, along with the Village's other electronic records (see below under "Preservation").
- The Village Clerk will ensure that emails generated ruing a certain year are purged from the email archiving appliance after six years.
- Email users who work at home should create two subfolders for permanent and non-permanent (six-year) emails, and delete all non-records. They should then periodically forward the two subfolders to the Village Clerk, who will file the permanent emails in the shared file directory. It is not necessary for the Clerk to manage the non-permanent emails, because the system will automatically collect the emails from the Clerk's account and manage the emails as six-year records.
- In rare instances, email users may receive or send an email or attachment that either does not qualify as correspondence or that they wish to save for longer than six years but not permanently. In such cases, they must forward the email to the Village Clerk, who will apply the appropriate retention period and file the email in the shared directory. (Users of personal accounts should also follow this procedure.)
- The email server deletes all messages from individual accounts in the Village email server after ninety days. (Users of personal accounts are strongly encouraged to purge these accounts of Village-related email according to the same schedule, after forwarding copies of record emails to the Village Clerk as described above.)
- Email users may store non-permanent records that they need for daily use on their own computer hard drives. The Village Clerk will prompt email users to review files on their personal drives annually, and to delete those saved emails that have passed their legal retention periods.
- Destruction of emails on the archiving appliance may be halted under certain circumstances (see Section 4. "E-Discovery").

2.3 Backups

- The Village Clerk will ensure that backups of emails on the email server and the archiving appliance are destroyed according to the retention period stipulated for backups in the Records Retention and Disposition Schedule MU-1.

2.4 Preservation

- Emails with retention periods greater than six years will be preserved with other electronic files in the Village's shared file directory.
- Emails will be stored in Rich Text format (.rft) on the email archiving appliance and in the shared directory.

- Emails stored in the archiving appliance are compressed, but the vendor of the appliance has assured the Village that the emails can be decompressed if needed without data loss (as documented in the Village's contract with the vendor).
- The Village Clerk, with assistance from the Village's computer support vendor, will monitor new versions of email software and the archiving appliance to determine whether upgrades are necessary.
- Backups of the email system and archive are to be used for disaster recovery and retention purposes.
- The Village Clerk, with assistance from the Village's computer support vendor, will ensure the ongoing integrity of media used to store emails, as stipulated in the Regulations of the Commissioner of Education (Part 185, 8NYCRR), if the emails are stored offline to removable storage media.

3. Access to Email

- Emails must be accessible for the duration of their retention periods. Emails are public records that are open and accessible to the public under the same conditions as all other Village records.
- Email users have access to the emails in their individual accounts in the Village system for ninety days. If they need access to some emails for longer than ninety days, they must save those emails on their personal hard drives.
- Permanent emails are files in the directory first by Village department and thereafter by subject or document type. Users have read-only access to emails in the shared directory, with some important exceptions. Access to certain emails relating to ongoing law enforcement investigations, court actions, and personnel matters may be restricted by law to specific individuals in Village government. The Village Clerk will maintain a list of types of emails where access is severely restricted.
- The Village Clerk, as records access officer, will respond to all FOIL requests involving email and , if necessary, will confer with legal counsel about an appropriate response (especially if a request is denied).

4. E-Discovery

Village staff and officials must be aware that all email messages, including personal communications, may be subject to discovery proceedings in legal actions, and all must respond appropriately to an impending legal action involving email

- Legal counsel will work with the Village Clerk to establish procedures for preserving evidence relating to imminent or ongoing legal actions.

- If a Village staff member or official becomes aware of potential litigation, it is his or her responsibility to notify legal counsel immediately. Counsel will determine what action, if any, needs to be taken.
- Legal counsel will work with the presiding judge and opposing counsel to narrow the parameters of a records search as much as possible.
- The Village Clerk, working with the Village's computer support vendor, will ensure that records of potential relevance in the archive remain accessible for the full extent of the proceeding, which may require moving relevant email records to removable storage media.
- All measures taken in response to an e-discovery actin will apply to Village-related emails that are retained by email users working on home computers.

5. Appropriate Use

Appropriate use will be handled as a security issue. Violation of the Village's appropriate use policy can threaten the Village's computer system, make the Village vulnerable to legal action, and cause irreparable damage to the Village's reputation.

5.1 Responsibility for Appropriate Use & System

- All email users are expected to know the difference between appropriate and inappropriate use of email. This appropriate use policy applies to anyone who is representing the Village, even if that person is using a personal account on a home computer.
- All users will be prompted to acknowledge their personal responsibility for using email appropriately every time they log into their Village email accounts.

5.2 Inappropriate Uses of Email

Email is provided as a tool to assist Village employees and officials in their day-to-day work, facilitating communication with each other, our constituency, and other stakeholders. The Village email system is intended for official communications only, and it is everyone's responsibility to limit personal use of the system.

It is not acceptable to use the Village of Millbrook's email for:

- Any illegal purpose
- Transmitting threatening, obscene, or harassing materials or messages
- Distributing confidential Village data and information
- Interfering with or disrupting network users, services, or equipment
- Private purposes, such as marketing or business transactions
- Installing copyrighted software or computer files illegally
- Promoting religious and political causes

- Unauthorized not-for-profit business activities
- Private advertising of products or services
- Modifying, obtaining, or seeking information about files or data belonging to other users, without explicit permission to do so

5.3 Enforcing Appropriate Use

- The Village has the right to address instances of email misuse through disciplinary action or termination, if necessary.
- Messages relating to or in support of illegal activities must be reported to the appropriate authorities.
- The Village Clerk has access rights to all email on the archiving appliance to monitor and ensure system security.
- The Village Board will review alleged violations of the email appropriate use policy on a case-by-case basis.

6. Technical Security

The Village's computer support vendor has primary responsibility for overseeing the technical security of the Village's email management system.

- The Village's computer support vendor is responsible for providing and maintaining up-to-date anti-virus software, firewalls, and spam filters to protect the overall system from malicious email messages and other forms of sabotage.
- In the event that email users receive unsolicited email (spam) or email with unexpected and suspect attachments, they must delete these emails and report them to the Village Clerk, who will confer with the Village's computer vendor to assess the security risk.
- Users should exercise similar care when linking to external websites from unsolicited messages.
- Email users must employ passwords to access their email in the Village email system and must change their passwords periodically.
- As a general rule, email users must not share their passwords with other Village officials or employees. In cases of planned or emergency absences, other personnel may be allowed to access the absent person's email, with prior approval from the Village Clerk.

7. Staff Departure

- If a staff member or official separates from the Village, the Village Clerk will place a hold on the email account of that individual until the account and computer can be reviewed for record content.

- Any Village emails maintained on a home computer by a former employee must be transferred to the Village Clerk for review and disposition.

8. Training

- All Village employees and officials will be trained in established email use and management policies.
- Training will be provided to all Village email users within the first ten days of employment or appointment, and to all employees when the policy is revised or the Village changes its current email management system.

  The Village Clerk will provide or arrange for training that will address the following topics:
- Identifying records, permanent records, and general records management practices
- Responsibilities of employees in records and email management
- Costs to the Village and the individual of not managing email
- Use of the Village email application and its relationship to non-system Village email
- Appropriate use of Village email accounts
- Responding to legal actions and FOIL requests

  Training materials can also be obtained by contacting the Village Clerk.

Other Responsibilities

The person or persons responsible for certain functions associated with managing email are indicated throughout this email policy in boldface. Other responsible parties (and their respective responsibilities) are listed below.

1. Village Mayor and Village Board

- Ensure an adequate budget allowance for maintaining the email management system
- Promote, support, and enforce this email policy
- Review alleged violations of the email appropriate use policy on a case-by-case basis and adopt disciplinary measures as needed

2. Village Counsel

- Reviews and approves contracts with vendors to ensure they are consistent with Village law and with the Village's internal procurement practices

C. Social Media Usage Guidelines

Definition of Social Media
For the purposes of this policy Social Media is defined as content created by individuals using technologies through the Internet including, but not limited to, instant messaging, texting, paging and social media networking sites which include Facebook, blogs (a shortened term for web log), MySpace, RSS, YouTube, FourSquare, Twitter, Linkedin, Delicious, Flicker, Pinterest and any other information sharing services, websites and/or blogs.

Guidelines
All Village social media pages shall be approved by the Mayor or the Board of Trustees or their designees. All social media content shall adhere to all applicable laws, regulations and policies including the records management and retention requirements set by law and regulation.

No information, videos or pictures gathered while on Village of Millbrook business (this includes meetings, details, trainings or anything obtained on Village property or at Village functions) may be shared or posted in any format without the approval and written consent of the Mayor or the Board of Trustees.

Under this restriction, employees are prohibited from disseminating or transmitting in any fashion photographs or images of individuals conducting Village business. Any such transmission may violate New York State Laws and/or the HIPPA privacy rights of such individuals and may result in a criminal and/or civil proceeding being commenced against employees violating this provision of the policy.

Speech that impairs or impedes the performance of the Village, undermines discipline and harmony among co-workers or negatively affects the public perception of the Village may be sanctioned.
As a basic constitutional concept of law, a public employee may comment on a matter of public concern. However, airing personal workplace grievances does not raise a matter of public concern.

Conduct of Employees

Employees must follow the following guidelines when discussing the Village of Millbrook on any Social Media:

- Do not make any disparaging or false statements or use profane language.
- Do not make any statements or other forms of speech that ridicule, malign, disparage or otherwise express bias against any race, religion or protected class of individual.
- Make clear that you are expressing your personal opinion and not that of the Village of Millbrook.
- Do not share confidential or proprietary information.
- Do not violate Village of Millbrook policies including the Code of Ethics.
- Do not display Department or Village logos, uniforms or similar identifying items without prior written permission.
- Do not publish any materials that could reasonably be considered to represent the views or positions of the Village of Millbrook without authorization.
- Do not publish sexual content or links to sexual content.
- Do not engage in or encourage illegal activity.
- Do not publish information that may tend to compromise the safety or security of the public or public systems.
- Do not publish content that violates a legal activity.
- Do not publish content that violates a legal ownership interest of any other party.
- Prior permission must be obtained from the Mayor or Board of Trustees before images and/or video of incidents can be taken.
- Do not publish images and/or video of residents and graphic images that are defamatory, obscene, slanderous or unlawful; and/or tend to interfere with the maintenance of proper discipline; and/or damages or impair the reputation and/or efficiency of the Village or employees.

Any employee engaging in social media or social networking activities, will maintain a level of professionalism in both on-duty and off-duty conduct that is consistent with the honorable mission of the Village.

Use of Social Media While on Duty

1. Employees may not use social media while operating Village owned equipment.

Photography and Videography

1. The use of cameras (still and video) shall not interfere with your role as an employee
2. Do NOT take or distribute photos on any medium where an individual conducting Village business, or license plate could be identified.
3. NEVER take graphic or revealing photographs.

4. Photographs on the computers are the property of the Village of Millbrook and are not to be copied, mailed, emailed, or printed without prior authorization from the Mayor or the Board of Trustees.
5. Law firms and/or civilian agencies requesting photographs of a sensitive nature shall be required to make a formal request via the courts and serve the Village of Millbrook with a subpoena before said photographs will be released.

Information Distribution

It is the role of the Mayor or the Board of Trustees or the Fire Chief to distribute information to the press and public. No other member shall be allowed to distribute information to9 the press or public without expressed consent by the Mayor or the Board of Trustees. This includes but is not limited to written, auditory, and/or visual messages communicated via or on Village of Millbrook resources or via personal devices, such as cell phones, PDAs, etc., and/or social media. Any written auditory, and/or visual messages communicated by an employee that are relative to the Village of Millbrook are the sole property of the Village of Millbrook.

A. The following information may NOT be released:
   1. Personal employee or resident information that would violate their right to privacy.
   2. Anything not in compliance with FOIL regulations.
   3. Anything regarding Village policies or procedures. (Any questions of this nature should be referred to the Mayor or the Board of Trustees)

The Village of Millbrook owns the rights to all data and files in any owned computer, network, cell phone or other information system. The Village of Millbrook also reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use of the internet and of computer equipment used to create, view, or access email and internet content. Employees must be aware that the electronic messages sent and received using Village of Millbrook equipment are not private and are subject to viewing, downloading, inspection, release, and archiving by Department Heads or liaisons at all times. The Village of Millbrook has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with policy and state and federal laws.

Inappropriate use of the Internet and instant technology while on Village business may result in disciplinary actions, up to and including termination/expulsion of an employee of the Village of Millbrook.

Village of Millbrook computer equipment is to be used for Village/department business purposes in a professional and businesslike manner.

D. Use of Electronic Devices by Village Board Members during Board Meetings

All Village Board members may use any electronic devices at all Village Board Meetings and executive sessions only when relevant to the business discussion. The volume shall be turned off and/or set to vibrate on all such electronic devices during such meetings of the Village Board.

Village of Millbrook

Electronic Devices & I/T Policy

E. Computer Systems Usage Guidelines

Policy Statement - The purpose of this policy is to provide guidance for the use of Village owned computer systems and Internet/Email service.

Computer Systems

Property – All computer systems, hardware, software, and files are the property of the Village of Millbrook. This includes the messages created, transmitted, and stored on such systems and equipment.

Authority – Department Heads have the authority to inspect the contents of any computer equipment, data/files, or electronic mail ("Email") of their subordinates in the normal course of their supervisory responsibilities. In addition, the data/files of Department Heads may be inspected by the Village Mayor in the normal course of duty. There is no guarantee of privacy when using Village-owned computer systems and equipment. The right of access to such may be exercised, for example, but not limited to, for the following reasons:

- Complying with an investigation into suspected criminal acts.
- Recovering from system failures or other emergencies.
- Investigation into suspected breaches of security or violation of Village policies.
- Evaluating the effectiveness of electronic mail or to find lost messages.
- Providing assistance when employees are out of the office or otherwise unavailable.

Usage – All computer systems, hardware, and software provided to an employee are provided for the purpose of aiding that employee in the performance of the employee's job functions. All hardware and software used is to be supplies by the Village of Millbrook. No unauthorized or unlicensed hardware or software may be used or installed on any Village owned computers. Any hardware or software necessary to perform job duties should be requested of the employee's Department Head.

Prohibited Uses – In addition to the guidelines set forth above, the following uses of Village owned computers and equipment are prohibited. This list is meant to be illustrative, and not exhaustive.

- Any illegal activity;
- Threats or harassment;
- Slander or defamation
- Transferring of obscene or suggestive messages or graphical images;
- Any unauthorized commercial activity;
- Accessing or attempting to access the data/files of another person;
- Using or aiding in the unauthorized use of another person's password;

- Harming or destroying data/files (other than editing or deleting information in the normal course of one's job duties);
- Use of non-business software;
- Use of entertainment software, such as games and puzzles;
- Installation or use of any hardware or software, not owned by the Village;
- Installation or use of Village owned hardware or software for any use that is not Village related business;
- Installation or use of any unauthorized or unlicensed hardware or software;
- Installation of any software containing viruses.

Internet/Electronic Mail Requirements

Eligibility – Internet/Email service may be provided to employees who can demonstrate a work-related reason to have access. Approval must be given by the employee's Department Head or Mayor.

Proper Usage – In addition to the prohibitions set forth in the above paragraphs, any activities prohibited for any other general computer user are also prohibited with respect to internet/Email service usage. Employees are expected to communicate in a manner that will reflect positively on both themselves and the Village of Millbrook. Additionally, it is the responsibility of the employee to adhere to the following guidelines:

- Email must be used in a professional manner.
- Messages must not be threatening, insulting, obscene, abusive, or derogatory.
- Messages must not include remarks that constitute sexual harassment.
- Chain letters are illegal and must not be transmitted through Email.
- Employees are responsible for saving any Email that they want to keep permanently.
- Messages must not involve personal sales or solicitation or be associate with any for-profit outside business activity.
- Messages must not involve personal not-for-profit solicitations.
- Messages must not potentially embarrass the Village of Millbrook.
- Files must be housecleaned at least once a month, deleting any old Email and/or downloaded information that has been saved.
- Passwords should not be given to anyone other than the employee's Department Head or Mayor.
- Internet must not be used for the propagation of computer viruses.
- Internet must not be used for personal recreational activities (e.g. online games).
- Participation in non-business internet chat groups is prohibited.
- As a security precaution, a workstation must not be left signed onto Email or the Internet an unattended for a long period of time (or overnight). Each employee must log off the network when not in use and power down at the end of the day.
- Employee Internet/Email usage may be subject to filtering and will be monitored.

- Employees should be aware that deletion of any Email messages or file does not truly eliminate that message or file from the system. All Email messages are stored on a central back up system in the normal course of date management.

Reliability – Users should be aware that because the internet is a collection of computer networks with no single central authority over information consistency, data is subject to inaccuracies. The Village is not responsible for loss or damage to a user's data or for the reliability of information that is obtained via the Internet service. Also, this information must be used in accordance with applicable copyright laws.

Security – There is no guarantee of privacy of data/files, including email, on Village owned computers. As stated herein, all files and internet usage are subject to inspection and/or monitoring by the Village. Any employee who is required to have a password must submit that password to the employee's Department Head.

Reporting of Violations – Anyone with information as to a violation of this policy is to report said information to the employee's Department Head. Once the employee's Department Head is informed of the violation, a formal process, consistent with the Employee Handbook and/or applicable law, will begin.

Electronic Devices & I/T Policy

F. Computer Back Up Procedure Introduction

The Village Clerk is responsible under the guidance of the N.Y.S. Archives Department for ensuring that all personal and identifiable data is recoverable in the event of accident loss or damage or technical obsolescence – the rapid advancement of computer technology that can render records inaccessible due to lack of planning.

Electronic records are to have a filing system that mirrors the Village's paper files. A series of electronic folders and subfolders will be created on the server, arranged hierarchically from the general to the specific in a series of directories. For easy retrieval, develop naming conventions that are logical, consistent, and allow sensible sorting. For example, create Village Board of Trustees minutes electronically, use the name of the records series followed by the month, day and year, indicated numerically so that the file sort in chronological sequence: "Minutes 1-1-2013".

The policy was last reviewed on January 14, 2020 and will be reviewed annually at the Re-Organizational Meeting by the Board of Trustees.

Frequency and Timing of Backups

A full back up of Village data is taken every day including:

All records and all actively running officially license Municipal software,
Email, applications, system software, configuration files, etc.
All files on the server of the network are scheduled to backup automatically at a designated time daily.

For laptops and desktop computers a separate backup routine is required. Weekly backup with user determined "important" files or data to be stored on the file system "Village Share" that is backed up daily.

- Calendar, appointments
- Municipal software programs
- Files held elsewhere on the network
- Other relevant software

Backup Rotation

The Village Clerk and Deputy Clerk is responsible for:

1. Remote backup and changing back up written instructions
2. Checking that all backup processes used have been successful
3. Managing a backup failure

The rotation should include clear deputizing arrangements for cover in the event of staff absence (both planned and unplanned).

Storage of Backup Drives
The backup drives when removed from the server are stored securely in a locked fire-proof media safe in the Village Hall

Management of Backup Drives
Drives are clearly labeled. They are to be used in strict rotation to ensure backups are up to date. Drives should be replaced every 4-5 years.

Verification of Backup Status

The Village Clerk must check the backup status on the system first thing each morning and report any failures to the Mayor and IT contractor.

Backup Log

A daily backup log (see attached template) is issued to keep a report of backups, their status, and housekeeping of the backup system. These logs are stored in a fire-proof safe in the Village Clerk's Office.

Housekeeping of the Backup System

Regular upgrades of the backup system are carried out to ensure it is kept in good working

Managing Backup Failure

In the event of an unsuccessful backup, the staff responsible for checking the backup must immediately:

1. Note any messages/information on the server
2. monitor Contact the system supplier to report the
3. failure Report the failure to the Mayor
4. Record the failure in the backup log and any actions taken as a result
5. If the backup fails repeatedly, it may be necessary to perform a manual backup. This takes time and must be performed when all users are logged out.

Security

In addition to fire, flood, and vandalism, computer users must contend with viruses, hackers and hard drive crashes. The physical security of computers will be increased by locking doors and installing fire detection systems. In addition, the Village must implement and update virus protection software and firewalls and use a system of passwords to protect the Village's information.

Archive
Yearly backup taken and stored offsite- safe deposit box at the bank. The backups will be two drives, one drive will be Calendar year and the other one will be of the Fiscal year.

G. Citizen Cyber Security Policy (Breach Procedure)

For purposes of this Citizen Cyber Security Policy, the terms "personal information" and "private information" shall have the meanings prescribed by sections 202 and 208 of the State Technology Law. New York State *values* the protection of private information of individuals. This Policy requires notification to impacted New York residents and non-residents of the individual's private information in compliance with the Information Breach and Notification Act and this Policy.

The Village of Millbrook (Village) is required to notify an individual when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Notification Breach Policy.

The Village, after consulting with its Information Technology Vendor to determine the scope of the breach, and restoration measures, shall notify an individual when it has been determined that there has been a breach of data. A compromise of private information shall mean the unauthorized acquisition of unencrypted electronic data with private information.

Such notice shall be directly given to affected persons by one of the following methods:

1. Written notice;
2. Electronic notice, provided that the person whom notice is required has expressly consented to receiving such electronic notification.
3. Telephone notification provided that a log of each such notification is kept by the Village.

The Village shall provide notification to the Attorney General, appropriate credit bureaus and the Consumer Protection Board, via official incident reporting forms.

VILLAGE OF MILLBROOK

35 MERRITT AVENUE PO BOX 349 MILLBROOK NY 12545 TEL: 845-677-3939 FAX: 845-677-3972

Date:

Millbrook, N.Y. 12545

Dear:

We are writing to notify you that on , we discovered that, on , our Village computer system was breached which contained some of your personal information, which may have included your name, phone numbers and social security number and other pertinent employment information. As part of our internal investigation and work with a specialized company, we determined that, on , all of the personal information contained on the computer system was accessed by unauthorized personnel.

We are taking this matter very seriously and have conducted a thorough investigation. Please be assured that we are taking all reasonable steps to mitigate the circumstances resulting from this incident and to ensure an incident like this does not happen again. We have filed a police report with the NYS Police Troop K. If you would like a copy of the report, you can obtain it by calling the NYS Police Troop K at 845.677.7300 and asking for a copy of police report number .

Importantly, there is no evidence to date that your personal information has been misused in any way. Nevertheless, we care about the protection of your personal information and understand the concern that this situation may cause you so we want to make you aware of the incident and present steps you can take as precautionary measures.

First, if you receive a call from someone asking for your credit card information, or any other personal information, in order to pay for products or services, we suggest that you end the call and call the applicable person directly to find out if they were the ones who made the call. Do not give out your credit card information, social security number, health insurance information, or other confidential information to someone who calls you unless you are certain of that individual's identity.

We suggest that you place a fraud alert on your credit files as a precautionary measure. There is no cost to you to place this fraud alert. A fraud alert requires potential creditors to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days and can be placed by calling the three credit reporting agencies listed below. You will then receive letters from all three agencies confirming the fraud alert has been placed and letting you know how to get a free copy of your credit report. The contact information for each reporting agency is:

Experian	**Equifax**	**TransUnion**
1-888-397-3742	1-888-766-0008	1-800-680-7289
www.experian.com	www.equifax.com	www.transunion.com

When you receive your credit reports, you should review them carefully. Look for accounts you did not open as well as inquiries from creditors that you did not initiate. Also, you should look for personal information that is not accurate, such as home address or Social Security Number. If you see anything on the report that you do not understand, call the credit reporting agency at the telephone number on the report. If you find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. You should ask for a copy of the police report, as you may need to give copies of the police report to creditors to clear your records. Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports periodically. Under U.S. law you are entitled to one free credit report a year from each of the three credit agencies. You can also keep your fraud alert in place by calling again after the first 90 days has ended.

If you see any service or product that you believe you did not receive, you should contact the vendor immediately. Please keep a copy of this notice for your records in case of future problems with your personnel records or credit information. Further information about steps you can take to avoid identity theft can be obtained from the following sources:

Federal Trade Commission 1-877-438-4338 **www.ftc.gov/idtheft**

We value all our residents and sincerely regret that this incident occurred. If you have any further questions on this matter, please call 1-845-677-3939, Monday through Friday, 9:00 a.m. to 7:00 p.m. Eastern Time. (Closed on U.S. observed holidays.) Please be prepared to provide the following reference number when calling:

Very truly yours,

Sarah J. Witt

Clerk/Treasurer

Village of Millbrook