

Technology Policies & Guidelines

Data Storage Policy

Purpose:

To take full advantage of the benefits of the network to protect data

Policy:

Below is a list of guidelines and the reasons for their use.

1. All documents should be stored on a network drive to ensure that documents will be backed up on a regular basis. Users who need to store files on a local drive or on removable media do so at their own risk.
2. If a PC were to fail for any reason, the failed PC will be replaced with a PC from available inventory and any documents or files that may have resided on the former local hard drive may be lost.
3. Users may establish subdirectories within their portion of the network. For example, each individual is assigned a home directory, I:, as necessary. The user may establish additional subdirectories for documents related to specific subject, like "I:\budget". If you are sharing folders or files within your department, use the H: drive. If sharing between departments, please use the J: drive.
4. No user should alter data or e-mails of another user without authorization.
5. All documents and data created or stored on Village computers are the property of the Village and constitute Village records and must be retained or destroyed in accordance with the Local Records Act. See your Department Director for clarification.

In order to explain the directory system more clearly, the drives available to users are detailed below.

H:\	This is a general use/transfer storage area for your Department/Division, and only members of your Department/Division can access files stored here. Users may create sub-directories for their Department/Division
H:\Form	This area holds templates for letterhead, memos, Village logo, etc., eliminating the need for pre-printed letterhead.
I:	This is the user's private storage area for files that are not shared. Users may create sub-directories as needed to organize their files.
J:	This is a village-wide storage area. Items in here are shared among departments and include projects and Village teams.

Public Cloud Data Storage Policy

Purpose:

To establish a policy for staff storing Village data in public cloud storage

Scope:

The use of cloud-based applications is growing rapidly. There is a need to keep track of where Village data is stored, who administers any cloud-based applications, and who has access to use the applications.

Village staff has a responsibility to protect Village data. However, when data is saved to the public cloud, it is no longer protected by Village controls.

Definitions:

“Unstructured data” refers to services such as Dropbox, Google Docs, Google Drive, Microsoft OneDrive, Evernote, etc.

“Structured data” refers to cloud-based applications that the Village has subscribed to.

“Village-owned information” refers to day-to-day operational materials, employee work products, strategic or planning documents, invoices, receipts, etc.

Policy

Unstructured Data:

1. Staff should not use public cloud storage to store or transfer files containing sensitive information. This includes, but is not limited to:
 - a. Data protected by HIPAA (Health Insurance Portability and Accountability Act), PCI (Payment Card Industry), CJIS (Criminal Justice Information Services), or other regulations
 - b. Personally identifiable information (e.g. social security numbers, names)
 - c. Data that violates Village security policies (e.g. list of passwords)
2. Village documents that are considered “Public Records” in accordance with the Illinois Local Records Act should not solely be stored in the cloud. They should also be stored on a Village network drive or in Laserfiche.
3. Staff work product is owned by the Village. Staff should not use the public cloud to store critical documents that may be useful to other staff members and would become inaccessible. Any Village data stored in the cloud should be tied to Village email account or credentials, not personal credentials.

Structured Data:

1. Information Technology will maintain a record of all cloud-based applications and related information including URL, the administrators, the users, and any details on any special configurations, such as firewall rules.
2. Departments are required to keep Information Technology informed of any new cloud-based applications or changes regarding existing applications.

3. Every cloud-based application should have at least two administrators to ensure continued access to the account. The administrators may or may not be members of the Information Technology staff. Information Technology must be informed of who the administrators are and any passwords to the cloud system.
4. If an employee is separated from the Village, access for that employee will be terminated upon separation.

Security Policy

Purpose:

To preserve the integrity of data on the Village computer systems

Policy:

When using computer resources at the Village of Mount Prospect, employees are responsible for the following:

1. The employee's login account and password is equivalent to his/her LEGAL SIGNATURE and the employee should not disclose this to anyone or allow anyone to access the system using his/her login account.
2. The employee is responsible and accountable for all entries made and all retrievals accessed under their login and password, whether such action was made by the employee or by another, due to the employee's intentional or negligent act or omission. Any data available to the employee will be treated as confidential information. This means no sharing of passwords.
3. An employee will not attempt to learn or use another's login account.
4. An employee will not access any online system using a login account other than his/her own.
5. If an employee has reason to believe that the confidentiality of the login account has been compromised, he/she should immediately notify his/her supervisor and Information Technology staff.
6. If a user forgets his password, they should contact the IT division. A temporary password will then be issued, and then the user will be required to change his password when he logs in.
7. While signed on, an employee will not leave a secured computer application unattended.
8. A Department Director may make temporary exceptions to the prohibitions listed above if the organization would benefit (e.g. while another employee is on vacation).
9. An employee will not attempt to tamper with or circumvent Village security systems or interrupt programs that protect data or secure systems.
10. An employee will not attempt to gain unauthorized access to information that is confidential or protected, or to files or directories he/she is not entitled to access.
11. An employee will not run any programs in an attempt to identify passwords or codes.

12. An employee will not act in any manner that will knowingly disrupt normal operations of the computers or networks.
13. An employee will not install or run a program that will damage or place undue burden on the computers or networks.
14. Employees will not install or run any program that would interfere with the Village's ability to monitor or remotely utilize any Village-owned PC.
15. Village of Mount Prospect computer systems may be periodically monitored to ensure compliance to this policy.
16. Failure to adhere to these regulations may result in disciplinary action up to and including termination.

Multi-Factor Authentication (MFA) Policy

The Village of Mount Prospect uses a multi-factor authentication (MFA) service to help secure the Village's network from cyber security threats. This application is designed to safeguard users, devices and applications. After employees login to Village computers and applications, multi-factor authorization requires a second step to prove your identity. The MFA service used by the Village provides two options to accomplish this secure login.

1. A free app [Duo] on your Apple or Android smartphone (recommended); OR
2. A USB key

Once an employee is enrolled in MFA, their phone or USB key will be required in order to login to a Village computer or use the Village VPN*. The associated smartphone or USB key will need to be carried with the employee at all times, as this is needed to access Village computers or applications. Additional applications requiring an MFA may be added in the future as security needs dictate.

Village employees with a Village-issued smartphone are required to use the MFA app. Employees not provided a Village-issued smartphone shall choose whether to have the MFA app installed on their personal smartphone OR to use a USB key. Please let the IT division know your choice during enrollment.

If an employee chooses the USB key, this employee is responsible for the device. If the USB key is lost, stolen or damaged, the employee shall reimburse the Village for the cost of a replacement. At the time this policy is written, the cost is approximately \$45. This price is subject to change.

*Village VPN is the Village's Virtual Private Network – it is through VPN an employee is permitted to access work files stored on Village servers while working remotely.

Non-Disclosure Policy

Purpose:

To maintain the confidentiality of Village data. Village employees may have access to privileged information in the course of carrying out their official job duties. This information may include but is not limited to financial, patient identifiable, employee identifiable, resident identifiable, or contractual data. Information from any source or in any form may be considered confidential (i.e. paper, magnetic or optical, conversations, voice mail, or electronic). The value and sensitivity of this information is protected by law and by the policies of the Village of Mount Prospect. The intent of these laws and policies is to ensure that confidential information remain confidential through its use as a necessity to accomplish the organization's mission. Special consideration is expected for all information related to personally identifiable health information accessed in the course of business per the Health Insurance Portability and Accountability Act (HIPPA) privacy and security standards.

Policy:

1. An employee will comply with all policies and procedures regarding access and confidentiality of data.
2. An employee will not access any information for which he/she does not have responsibility or authority to access.
3. An employee will not disclose any confidential information unless required to do so in some official capacity of employment.
4. An employee has no rights or ownership interest in any confidential information or work product.
5. An employee will not use confidential information in any way detrimental to the Village of Mount Prospect.
6. The disclosure of information is prohibited indefinitely, even after termination of employment.
7. Any FOIA (Freedom of Information Act) information requests must be approved by the Village Manager or designee.
8. Failure to adhere to the Village's non-disclosure policy may result in disciplinary action up to and including termination.

Virus Prevention Policy

Purpose:

To reduce the threat of viruses and malware to the computer resources at the Village of Mount Prospect.

Policy:

1. If a virus is detected, the user shall immediately notify the IT division. In addition the following steps should be taken, if possible:
 - a. Write down the name of the virus as provided by the anti-virus software.
 - b. Record any noticeable affects from the virus (suspicious system behavior, screen displays, etc.).
 - c. Shutdown the computer and leave a note to prevent use until cleaned.
2. If a user receives a suspicious e-mail, he/she should notify the IT division before opening it.
3. Users should not attempt to browse CDs or other removable media (such as thumb drives) if they do not know the source of the media. Any disks from outside sources, including demo disks or CDs, must be scanned for viruses before use.
4. Computers that do not belong to the Village, such as laptops brought in for demos or technical support, will not be allowed to physically attach to the network until the IT division has checked to be sure the computer is being properly scanned for viruses and malware.
5. Security patches are periodically pushed out to networked computers. Computer restarts are scheduled to occur automatically.

E-Mail Use Policy

The e-mail system is provided at the expense of the Village to assist in carrying out the proper business of the Village. The e-mail system permits authorized users to communicate with each other internally and with selected outside individuals, business, and other service providers that the Village, at its sole discretion, decides should be connected to the system and for the intended purposes involved.

The Village considers the e-mail system to be for business use only. While it is possible that employees may decide to send personal messages, the Village assumes no responsibility for their content or for maintaining their privacy. Employees should have no expectation that such privacy will be maintained. In order to ensure that the system functions properly and that the Village and/or its employees are not liable for improper use of Internet and other connections, the Village considers all messages sent, received or stored as business messages, and thus, solely the property of the Village of Mount Prospect. This means that we reserve the right to access and inspect such messages at any time. Conducting business unrelated to the Village, other than incidental personal traffic (during authorized time when not expected to be working), is strictly prohibited and may result in disciplinary action against the offending employee.

The Village reserves the right to access, review, copy, or delete all e-mail messages for any purpose and to disclose them to any party (inside or outside of the Village) as it deems appropriate. We can and will periodically inspect such systems and messages to ensure compliance with this Policy and therefore no employee should expect privacy with respect to such communications. As of 2014, all e-mail communication with the Village e-mail system is being archived using the Village's archiving system. This aides the Village in responding to FOIA requests and retrieving e-mails that may have otherwise been deleted.

This includes the right to install software that monitors e-mail and Internet usage. The Village, however, bears no responsibility for the content of messages sent or received by its employees. The Village does not and will not preview, edit or approve material on a routine basis in the email system. All messages sent on the e-mail system are attributable solely to the individual users of the e-mail system, and not the Village. The Village shall not be liable for, assume any legal responsibility for, or bear any costs arising out of e-mail communications flowing in or out of the Village computer system.

Should employees make incidental use of the e-mail system (including Internet e-mail) for the purpose of transmitting or receiving personal messages, such messages will be treated no differently than other messages (i.e., the Village reserves the right to access, review, copy, delete, or disclose them for any purpose). Accordingly, authorized users should not use the e-mail system to send, receive, or store any messages that they wish to keep private. (Incidental use of the e-mail system is limited to occasional, casual, minor, or insignificant use that does not impact upon an employee's duties or impede business-use operations and which occurs when the employee is properly not performing his/her normal duties.) Please note that there is nothing in this paragraph which limits the Village's right to

inspect or search such systems to ensure compliance with this policy and/or for other business purposes.

No e-mail messages or information should be created, sent, or forwarded which may reasonably be deemed to be intimidating, hostile or offensive in nature, or which refer to or relate to race, color, religion, sex, national origin, sexual orientation, disability, or any other basis that is unlawful under applicable state and/or federal law. Nor should any obscene, profane, abusive, or offensive language be transmitted. Any violation of this Policy (which will be construed in accordance with our anti-discrimination and anti-harassment policies) is grounds for disciplinary action up to and including immediate discharge.

No e-mail or other electronic communication may be sent which hides, alters or misrepresents the identity of the sender or represents the sender as someone else. All messages communicated on the Village e-mail system should contain or reference the sending employee's name (with few exceptions in the event an anonymous communication is an appropriate exercise of an employee's free speech rights). The Village bears no responsibility for any consequences resulting from any employee who uses the e-mail system for any fraudulent, or other illicit purpose, or contrary to the provisions of this Policy. This Policy will be construed in accordance with the applicable laws including revisions thereto that are announced by the Illinois Labor Relations Board or other authorized administrative agency or court that governs employee communications.

Any employees who become aware of misuse of the Village e-mail system is urged to contact the IT Division immediately. Be assured that no retaliation will be taken against the person based on his/her report of a potential violation under this Policy.

Privileged Communications

Some of the messages sent, received, or stored in the e-mail or the Village computer system may be privileged communications between the Village and its attorneys, or other entities. Upon receipt of any such message, do not forward it or its contents to others inside the Village without the authorization of all authorized parties. Never forward such messages or contents to any outsiders. To the extent practicable, all efforts should be made to send such privileged communications in an encrypted form. Please contact the IT division who can provide options for encrypting e-mail attachments.

Viewing and Protecting E-Mail Messages

In order to guard further against dissemination and disclosure of confidential or Proprietary Information, employees should exercise caution when accessing their messages in the presence of others. E-mail windows should not be left open on the screen when the computer is unattended. Users shall not allow any other person to use their name and password to gain access to an email system. Passwords are required and should be changed regularly. If you believe someone has obtained access to your password, it is your obligation to immediately notify the IT division so that your password can be changed. The Village reserves the right to impose guidelines requiring mandatory password changes and encryption measures to provide additional measures of security to help protect its equipment and confidential information.

Storing and Deleting E-Mail Messages

The Village strongly discourages the storage of large numbers of e-mail messages. Retention of messages consumes space on the network server and/or individual hard disks and can reduce their performance. As stated above, the Village's archive system automatically stores e-mail messages from 2014 and beyond which can be retrieved by employees at any time during their employment. Accordingly, employees should promptly delete any e-mail messages they send or receive that no longer require action or are not necessary to an ongoing project. Employees should audit stored e-mail messages regularly and should delete any messages that are no longer needed by yourself or others.

The Village reserves the right to establish database management guidelines on memory storage size limits for users.

Copyrighted Information

Use of the e-mail system to copy and/or transmit any documents, software or other information protected by the copyright laws, without proper authorization by the copyright owner, is prohibited. Copyright protection applies to any document, photo, software, or information unless it is specifically marked as public, not copyrighted, or freeware. In the absence of any specific copyright markings, material or information should be considered copyright protected. The Village assumes no responsibility for reviewing, ascertaining or policing copyrighted material that may be transmitted to or from the e-mail system by employees.

E-Mail Etiquette

Please bear in mind that your e-mail messages likely will be read by someone other than the addressee, and may even have to be disclosed to outside authorized parties including courts in connection with litigation. For example, in accordance with the Illinois Freedom of Information Act, and its amendments, e-mail and Internet information (i.e. sites visited) are liable for disclosure with a Freedom of Information request. Accordingly, all e-mail messages must be courteous, professional, businesslike, and tasteful. Additionally, as noted, these systems are subject to inspection by the Village to ensure compliance with these use policies.

Hardware/Software Standardization Policy

1. All computer hardware and/or software to be purchased will first be reviewed by the IT division to ensure compatibility with other Village systems. Justification for the purchase must be provided as part of the review process.
2. All hardware or software purchases over \$5000 should utilize Computer CIP (Capital Improvements Plan) procedures as part of the budget process.
3. New hardware or software purchases are generally funded by the department. Replacements (upgrades) may be funded through Information Technology.
4. All hardware or software must be installed by Information Technology staff or their delegates. Users who violate this policy are subject to disciplinary action up to and including termination.
5. Employees are not permitted to modify PC settings without approval of their Network Administrator. This includes network and printer settings.
6. Employees are not permitted to allow non-authorized personnel to modify PC settings. Employees are responsible and accountable for all non-authorized changes made to a PC assigned to them. Department Directors are responsible for non-authorized changes made to shared PCs, such as a department laptop.
7. IT staff will remove from local PCs any software of which the Village is not a licensed user. Users are prohibited from installing unauthorized software onto local hard drives or the network. Any proposed software installation must be performed by or approved in writing by the Network Administrator. Users who violate this policy are subject to disciplinary action up to and including termination.

VILLAGE INTERNET AND INTRANET GUIDELINES

As with e-mail, the Village provides Internet access solely to facilitate the conduct of Village business as a public service provider. Access to the Internet may be limited at the sole discretion of the Village where necessary to protect Village property or information or as otherwise necessary for our business needs. This includes the use of filtering software to bar access to certain Internet addresses. Employees are expected to use the Internet and Intranet in the manner that benefits the Village. An automated web filter will keep a log of sites accessed by all employees on the Internet.

The following activities on the Internet and/or Intranet are specifically prohibited and may result in disciplinary action up to and including discharge (list is not all-inclusive):

- Using the Internet or Intranet for personal gain or for commercial activity unrelated to the Village.
- Sending, using or otherwise misappropriating Privileged Information, confidential information and/or Village Restricted Information.
- Sending, using or otherwise misappropriating material that is threatening, intimidating, hostile, offensive, or discriminatory on the basis of race, color, religion, sex, national origin, sexual orientation, disability, or any other basis prohibited by applicable law. In addition, the receipt of such material and/or showing such materials to co-workers is strictly prohibited.
- Copying or otherwise converting protected electronic information.
- Violating (actual or threatened) copyright or trademark laws.
- Making any unauthorized attempt to break into another person or organization's computer system.
- Using the Internet or Intranet for any activities not specified here that are in violation of federal, state, or local laws and/or contrary to the best interests of the Village.
- Village website modifications shall be in accordance with the Village's Communication Plan.

Telephone/Voice Mail Policy

Purpose:

To provide guidelines for the secure, effective, and proper use of the telephone and voice mail systems

Policy:

1. All calls will be answered in a pleasant and professional manner.
2. Initial access to the voice mail system will be authorized by the Department Director.
3. An employee will access his/her voice mail with a password or code. The confidentiality of the password will be the sole responsibility of the user. Any communications via the voice mail system will be attributed to the assigned name of the originating mailbox.
4. An employee shall not attempt any unauthorized access to the voice mail system.
5. The Village reserves the right to monitor voice mail messages and phone conversations.
6. The Village reserves the right to access and disclose the contents of any employee's voice mailbox. Such access may occur, but is not limited to, the Village's need to investigate a possible violation of policy or a breach of the computer or voice mail system security. Any contents obtained through these guidelines may be disclosed without consent of the employee, but only to those employees who have some reasonable need for access to the information. Such determination is at the sole discretion of the Village.
7. Voice mail is to be used as the last resort for recovering customer calls. It is not to be used as a substitute for answering the phone. All calls are to be answered first by an employee, and then by the voice mail system. Every attempt, whether departmentally or systematically, should be made to answer a call with a person. Voice mail is an option for the customer as a courtesy and as a backup to the employee's call path.
8. Telephones and voice mail are to be used to conduct Village business; however, incidental and occasional personal messages will be permitted as long as there is no disruption to Village operations of job duties.
9. No employee shall use the voice mail system for mass distribution of personal or non-business information including, but not limited to, personal advertisements, personal opinions, or personal requests.

Help! Who Do I Call?

Problem	First Choice	Second Choice
Forget your password? Logon/logout problems? Software/hardware problems? Internet/e-mail problems? Printing problems?	Send email to support@mountprospect.org with a detailed description of the issue. Include attachments and screenshots if necessary.	Call ext. 5440
Request to purchase software/hardware?	Your supervisor, who will pass along to CTIO/IT Supervisor	