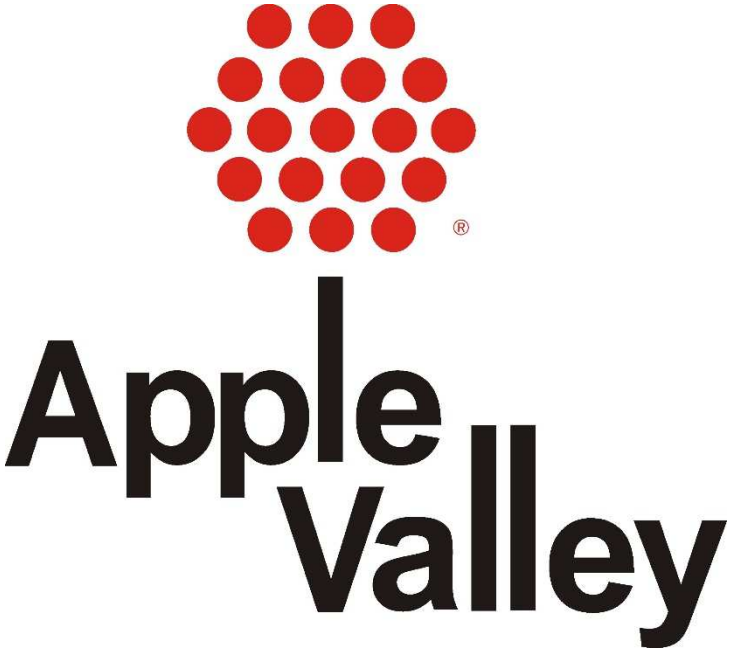
City of Apple Valley
Information Technology Policy



City of Apple Valley
7100 West 147th Street, Apple Valley, MN 55124

City of Apple Valley Information Technology Policy

Table of Contents

Information Technology Policy.

I. *Policy:*

1.1 It is the City of Apple Valley's policy to establish standards for appropriate Information Technology usage and protect the City's IT systems from business interruption, unauthorized or inappropriate access, and maintain security.

1.2 IT systems include, but are not limited to, City-owned computers, email, Internet, printers, software, telephone, voicemail, mobile communications devices, and others.

II. *Discipline*:

2.1 Employees engaging in such activity that violates the terms of this policy may be subject to disciplinary action, up to and including termination of employment.

III. *Auditing:*

3.1 The City of Apple Valley reserves the right to monitor and audit use of its IT systems at any time without user's consent.

IV. *Reporting:*

4.1 Users should notify their immediate supervisor, Department Head, the IT Manager, the Human Resources Manager, or the City Administrator upon learning of violations of this policy.

V. *Expectation of Privacy:*

5.1 As a government agency, the City is subject to public disclosure laws. All files and documents, including e-mail messages and Internet logs, are owned by the City and may be subject to requests under public records law. Users should have no expectation of privacy.

VI. Application:

6.1 The policy shall apply to all employees, including those represented by a bargaining unit, full-time, part-time, seasonal, contractors, volunteers, elected officials, and firefighters who have access to or use the City of Apple Valley IT systems both on and off City property.

VII. Access:

7.1 All users must be authorized to use City IT systems through the user's department head and IT.

VIII. Hardware and Software Acquisition for City owned IT Systems:

8.1 The IT Manager must approve all hardware and software prior to acquisition to ensure consistency with the design and architecture of the City's IT network. Users are prohibited from downloading, installing, or acquiring hardware and software, including product demonstrations, without prior approval from the IT Manager. Software applications not required for official City business are strictly prohibited. The IT Manager may allow exceptions for users to install apps on mobile communications devices.

IX. Installation, Downloads, and Configuration:

9.1 No user will be allowed to manipulate hardware and software standard configurations. The IT department, or designee, must always be contacted for hardware and software support.

9.2 Users are not allowed to change the computer setup or configuration files. Customization of City-owned software such as wallpaper, screen savers, icons, toolbars and colors, may be allowed for personal preference inasmuch as it doesn't interfere with normal computer operations or with other users' settings. Users are prohibited from downloading or installing any software through the Internet, e-mail, and/or vendor demonstrations without prior approval from the IT department.

X. Licensing:

10.1 To ensure license compliancy, all software must be purchased by and licensed to the City.

10.2 Development: Any software programs, e.g., custom designed Microsoft Access databases, developed for use by the City becomes the property of the City. Software programs may not be sold or distributed without prior approval.

10.3 Home: City-owned software may not be installed on non-City owned equipment unless there is prior approval of department head and IT Manager.

10.4 Copyright Laws: City users are required to abide by software and documentation copyright laws and licensing agreements. If there is any question about the legality of the software and documentation, it should be directed to the IT Manager. At no time should any user make copies of City-owned software and documentation. To prove legal ownership of software, the City must have the original media and manuals stored on City property. The IT Manager may periodically check for software that may be in violation of the above policy.

XI. Data Management and Protection:

11.1 Under the provisions of the Minnesota Data Practices Act, all data classified as City data, regardless of where it is stored, is considered to be owned by the City. This data is subject to the Minnesota Data Practices Act and its use and dissemination is consistent with the data classification under the Minnesota Data Practices Act. This data is also subject to review and investigation at the discretion of the City Administrator, Human Resources,

department heads, IT Manager, and/or law enforcement. The City Clerk should be contacted with questions regarding the classification of public and private data.

11.2 Data Ownership: All information developed or introduced to a City technology system by a user in conjunction with employment with the City is the property of the City.

11.3 Data Storage: All City data must be saved to a network drive on a City server. Users are responsible for deleting outdated files that are no longer needed for the compliancy of the City Records Retention Schedule; this includes data files and e-mail messages. The City Clerk should be contacted with questions regarding the City Records Retention Schedule. Users should not store City data on privately-owned mobile communications devices. Any City data created or modified on a mobile communications device should be transferred onto a City server.

11.4 Data Back-up: The IT department backs up all data stored on the file servers. Workstation hard drives or any other devices are not backed up.

11.5 Portable files: To facilitate off-site work, users may copy appropriate files, including word processing, spreadsheets, and presentation graphic files to and from removable media, such as flash drives, CDs, or to mobile communication devices. No other files or information may be copied to or from the City computers. A current copy of the portable file(s) must be maintained on the City server.

11.6 File and File Folder Password Protection: Because the City is responsible for ensuring access to its data, the City requires the ability to access City files or data that may be only accessible through a password created a by an employee. If any software product that the City has purchased has the option to allow users to have individual files password protected, the password must always be shared with the appropriate management personnel. If the City has purchased access to a service on-line that includes granting of user rights, appropriate administrator login credentials must be shared with appropriate management personnel.

XII. Portable Information Systems:

12.1 Portable laptop computers, tablets, digital cameras, projectors, and other City-owned portable equipment may be used for City business within or outside of City facilities. When users check out portable equipment they are expected to provide appropriate protection against theft, accidental breakage, environmental damage and other risks. Desktop computers and attached devices are not to be removed from City buildings. The user is responsible for the backup of or loss of any data stored on the standalone or portable computer. IT staff is available to assist in the development of procedures for disaster recovery of portable units. Documents stored or accessed from portable information systems containing sensitive or private data must be password protected or otherwise secured on the equipment in accordance with IT approved practices.

Further policies for City-owned or privately-owned mobile communications devices are found in Appendix 2: Wireless Communications Device and Phone Policy.

XIII. Non-City Owned Equipment:

13.1 Use of non-city owned mobile communications devices may be utilized only to the extent that these devices are not connected to the City's internal network, systems, or computers, except for special purposes pre-approved and arranged by the IT department on a temporary basis. For further details, see Appendix 2: Wireless Communications Device and Phone Policy.

XIV. Electronic Mail (e-mail):

14.1 The City e-mail system is a tool to be used for matters directly related to the business activities of the City and as a means to provide services that are efficient, accurate, timely, complete, legal and appropriate, subject to Section XVIII Personal Use. E-mail messages are subject to regulation under the Minnesota Data Practices Act. The content of the message determines whether a message is public or non-public/private. E-mail is intended as a medium of communication, not for information storage; therefore, e-mail should not be used for the permanent storage or maintenance of official City records or other City information.

14.2 Inappropriate use of the City e-mail system includes, but is not limited to the transmission, access or receipt of:

- Non-business audio, video or image files (including streaming audio and video, MP3, Jpg, Tif, Gif, Mpg, AVI, etc.);
- Software programs or executables;
- Chain letters;
- Offensive, sexually explicit or pornographic material;
- Intolerance, hate, violence, or tasteless material;
- Copyrighted material or large data files not directly related to City of Apple Valley business.

14.3 The use of e-mail for these purposes is strictly prohibited. If a user receives an unsolicited e-mail that falls within these prohibited categories, the user must immediately delete it. If the activity continues, the user must notify the IT Manager and their supervisor.

14.4 The City retains the right to monitor, track and restrict all e-mail activity. Software may be employed to reduce the delivery of junk e-mail, including e-mails that contain profanity, sexually explicit or adult content material, or which otherwise may be deemed inappropriate or non-business oriented.

XV. Internet:

15.1 The Internet is available to users for research, education, and communications directly related to the mission, goals/objectives, or work tasks of the City, subject to Section XVIII Personal Use. Access to the Internet will be determined by department management. Use of the Internet through City computers is a privilege, not a right, which may be revoked at any time for inappropriate and/or abusive conduct. Users of the Internet should minimize

unnecessary network traffic that might interfere with the ability of others to make effective use of this shared network resource. Users are responsible for adhering to City standards when browsing the Internet. Failure to adhere puts the City and the individual at risk for legal or financial liabilities, potential embarrassment and other consequences.

15.2 Inappropriate use of the City's internet services includes, but is not limited to the transmission, access or receipt of:

- Offensive, sexually explicit or pornographic material;
- Intolerance, hate, violence, or tasteless content;
- Games or gambling;
- Non-business related chat or instant messaging;
- Unauthorized downloads, proxies, or peer-to-peer networking.

The use of the internet for these purposes is strictly prohibited. The City retains the right to monitor, track and restrict all internet activity.

XVI. Intranet:

16.1 The City of Apple Valley's Intranet is an internal website for use exclusively by employees. The site is accessible by employees within City premises for business-related purposes to foster communication, enhance customer service and information-flow. Access to and within the intranet shall be determined by department management. Intranet usage is governed by the same guidelines as internet use.

XVII. Prohibited Use:

17.1 Use of City IT systems, including internet, intranet, and e-mail, is strictly prohibited at all times for the following:

- Illegal, criminal, or unethical activities;
- Profit or commercial activities;
- Gambling, wagering, or selling chances;
- Transmitting, accessing or receiving threatening, pornographic, obscene or harassing material;
- Transmitting, accessing or receiving chain letters;
- Fund-raising or charitable solicitations, except for City approved activities;
- Transmitting, accessing or receiving software programs or executables, non-business audio, video or image files, copyrighted material, or large data files not directly related to City business;
- Political or religious promotion;
- Access resulting in unauthorized expense to the City;
- Activities that interfere with or disrupt network users, services or equipment, including mass distribution of messages, intentional distribution of viruses, or seeking unauthorized access to other computers or systems;
- Any other public office or employment which is incompatible with City employment responsibilities, as determined by the City Administrator.

XVIII. Personal Use:

18.1 The City of Apple Valley offers users the privilege of limited personal use of its technology. Recognizing that users will benefit from practice using technology, personal use is allowed using the following guidelines listed below:

- IT systems may be used for occasional, incidental personal use as long as it does not interfere with the normal duties of the employee.
- Only City employees are to use the computers and computer related peripherals.
- No personal files or data are to be stored on the City file servers.
- Users must not use IT systems for items listed above in Prohibited Use.

18.2 E-mail: E-mail may be used for incidental personal correspondence, as long as it does not interfere with the normal duties of the employee and the above guidelines are followed. Using e-mail to participate in any kind of non-business related list-serve or broadcast mailing is prohibited. Users shall have no expectation of delivery or receipt of non-business related e-mail.

18.3 Internet: Internet access may be used for occasional, incidental personal use as long as it does not interfere with the normal duties of the employee and the above guidelines are followed.

18.4 Desk Telephones: Desk telephones may be used for personal use as long as it does not interfere with the normal duties of the employee and the above guidelines are followed. Personal long distance toll calls are prohibited on City-owned phones.

18.5 Cellular Telephones: Policies for City-owned or personal mobile communications devices are found in Appendix 2: Wireless Communications Device and Phone Policy.

18.6 Copiers, Printers, Fax Machines: Users are granted limited, incidental use of photocopiers, printers, and fax machines as long as it does not interfere with the normal duties of the employee and the above guidelines are followed.

XIX. Computer and Network Logins and Passwords:

19.1 All users must use and maintain unique IT-issued login IDs for computer and network-related access. Login IDs are not to be shared with others, and corresponding passwords must remain confidential. Multi-user or generic login IDs are permissible only in special circumstances approved and maintained by IT. Users are prohibited from saving their password credentials with the computer or device such that the City's network accounts are accessed through an automated login unless the device itself is password protected or otherwise secured by an IT-approved security method. The City must conform to adopted security practices, including password requirements, as governed by LOGIS and/or state and federal government guidelines. All users are required to follow password requirements as defined in Appendix 1, Network Password Requirements.

19.2 Appropriate network access shall be assigned by the IT department to each user login ID, and users may only log into computers and equipment with their assigned login ID. User login ID passwords are not to be shared with anyone, and will be forced to change periodically. New passwords should not be easily guessed. Anyone forgetting their password, or suspecting that their password's security has been compromised, must contact the IT department to be issued a new one, which will then be changed immediately.

XX. Physical Security:

20.1 City users are expected to provide reasonable security to their computer workstations and related IT equipment. This includes ensuring that passwords are not written down in accessible places, removable media must be kept in a secured area, and that confidential data is not displayed in such a manner that unauthorized personnel can access it.

20.2 Users may not move IT equipment outside of its assigned area without prior approval from the IT department. Portable equipment must be reserved and checked out only to City users. Users are expected to provide appropriate protection against theft, breakage, environmental damage, and other risks.

20.3 Users are required to log off computer workstations when absent for an extended time, such as end of day. Users may, however, "lock" their workstation instead when absent for a short period of time, such as during a meeting or over lunch.

20.4 Security policies for City-owned or personal mobile communications devices are found in Appendix 2: Wireless Communications Device and Phone Policy.

XXI. Virus Protection:

21.1 All computer workstations, laptops, and servers must be protected from viruses using up-to-date antivirus software. Users may not alter their system's configuration or take other steps to defeat virus protection devices or systems. All files on removable media must be scanned for viruses prior to installation onto or access from City computer equipment. Any files suspected or known to contain viruses must be immediately reported to the IT department for proper handling.

XXII. Remote Network Access:

22.1 Remote access is defined as the ability to connect to a computer or network from a distance, such as from home, hotel, conference, Internet kiosk, etc. Remote access into the City's network may be granted upon meeting the following conditions:

- Business-related purpose approved by requesting department head and IT Manager.
- Use of industry standard encryption and/or City supported VPN (Virtual Private Network) technology.
- Authentication and access control will be maintained by the IT department. Valid network login and passwords are required.
- While remotely connected, nobody but the authorized user may have access to the computer making the connection.
- Remote computer must comply with current anti-virus and security parameters as specified by the IT department.
- Additional policies for remote network access by City-owned or personal mobile communications devices are found in Appendix 2: Wireless Communications Device and Phone Policy.

22.2 All remote users are subject to the rules and regulations set forth in this entire policy for all network users. Users should follow proper data practices protocols as directed by the Minnesota State Statutes. Storing of business related information on a home computer creates an extension of the City's network; thus anything stored on that computer, might be subject to public data requests.

XXIII. Wireless Access:

23.1 Unauthorized wireless access into the City's computer network is strictly prohibited. Users may not attempt to scan, connect to, or install any wireless computing device on City equipment or property.

23.2 Wireless access must be authorized and configured by the City's IT department. Any authorized wireless access must utilize standards-based encryption, and conform to adopted security practices as governed by LOGIS and/or state and federal government guidelines. The City offers limited authorized use of wireless access for both employees, as necessary, and non-employees (guests) as a convenience. Access to this wireless network by guests is governed by a separate use policy presented upon connection or upon request for login credentials. All users of the City's wireless network must comply with this usage policy, however access is not guaranteed.

Glossary of Terms

Configuration: The way a system is set up or the assortment of components that make up the system. Configuration can refer to either hardware or software or the combination of both.

Downloads: To copy data, usually an entire file, from a main source to a computer device, such as from the internet or online service to a computer.

Electronic Mail (e-mail): A network application that allows users to exchange messages over communications networks with someone else.

File Server: An enhanced computer with network operating software that is used for file storage, application functionality, and managing network resources.

Information Technology Systems: Includes, but not limited to, computers, printers, software, e-mail, Internet, telephone, voice mail, and others.

Internet: A global network connecting millions of computers.

Intranet: Network base access accessible only within an organization. An intranet ‘s Web sites look and act just like any other Web site, but firewall security restricts unauthorized access.

Installation: The process of connecting and configuring hardware or software.

Local Area Network (LAN): A computer network.

Licensing: Legal compliancy of assets.

Mobile Communications Devices: Mobile devices that have the ability to communicate with the Internet, City networks, or other communications systems including laptop computers, tablets, cell phones, and smart phones.

Peripherals: A computer device, internal or external, such as a CD-ROM drive, printer, mouse, that is not part of the essential computer.

Software: System software includes the operating system and all utilities that enable the computer to function. Application software includes programs that do real work for users (e.g. word processors, spreadsheets, and database management systems).

Portable Equipment: Hardware that is small, lightweight, and non-stationary (e.g. laptop computers, hand-held computers, tablets, projectors, digital cameras).

Users: regular, part-time, and temporary employees, vendors, consultants, volunteers, elected officials, interns, and other.

VoIP: Voice over Internet Protocol, a category of hardware and software that enables people to use the Internet as the transmission medium for telephone calls by sending voice data in packets.

Appendix 1: Network Password Requirements

All passwords are to be treated as sensitive and confidential information. Employees must keep their passwords confidential and not share them with anyone that is not authorized.

All network passwords must follow these specifications:

- Must be a minimum of eight characters in length.
- Must be changed every 180-days.
- Have a digit and/or symbol character as well as letters, for example: kep1tSaf
- Have not been previously used in the last ten password rotations.

Supervisors must notify IT staff upon termination/separation of employees so their network accounts can be disabled.

Appendix 2: Wireless Communications Device and Phone Policy

Purpose
Customer expectations for prompt resolution of questions or service concerns often require the use of wireless communications devices including cellular or smartphones by City officials. Efficient participation in meetings or work from multiple locations may require the use of wireless network access devices by employees or elected officials (hereafter referred to as mobile communications device users).

The purpose of this policy is to outline the reasons for (i) providing a City-issued phone; (ii) allowing access to a City network through a privately-owned mobile communications device; and (iii) providing a stipend for use of personal cellular phone/ smartphone or mobile device. Mobile communications device users who: (i) must remain accessible due to the nature of their job duties; (ii) must be available for emergency response or consultation; (iii) have job duties that require receiving work communications remotely; or (iv) require wireless network access for City duties may be eligible for a City-issued device or participation in one of the City's offered stipends defined in this policy.

This policy does not apply to wireless devices physically connected to buildings, vehicles, or other infrastructure that serve as part of the City's network infrastructure, including the Supervisory Control and Data Acquisition (SCADA) System, that are not assigned to individuals.

Scope
This policy applies to all City mobile communication device users.

Policy
This policy covers City-issued communication devices and use of privately-owned personal mobile communication devices for City business.

Section 1: General Provisions for City-Issued and Personal Devices Used for City Business
The City retains the right to monitor and enforce network security through a mobile device management system. The mobile device management system may require installation of an app or other software on the mobile communications device. In the event that a communications device is damaged, lost, or stolen, the mobile communications device user is responsible for notifying their immediate supervisor and the IT Division as soon as possible. If a stipend is involved, the mobile communications device user is responsible for notifying the HR Division as soon as possible. In the event of a reported damaged, lost, or theft of a device or upon replacement of a device or when an employee is no longer employed by the City, the IT Division reserves the right to remotely remove all City data and/or City information such as contacts, tasks, or applications. The City is not responsible for any lost personal data.

Mobile communications device users shall maintain a password, PIN code protected, photo-password, biometric, or other IT-approved security access protocol on any City-owned or personally-owned smartphone or mobile device. Mobile communications device users are responsible for ensuring the proper elimination of City data, including City network passwords and photos from personal devices before disposal.

A mobile communications device user's use of the device is subject to data practices and data retention requirements under Minnesota law. The mobile communications device user is responsible to upload or transfer any data obtained in the conduct of City business from the device to the appropriate storage medium for the data within the City's network.

Section XVII of the City's Information Technology Policy on Prohibited Use applies to use of City-owned wireless devices. Section XVII also applies to use of personal devices for City business or when a mobile communications device user would be reasonably expected to be conducting City business.

The City of Apple Valley has no expectation for non-exempt employees to check or respond to emails or messages during non-work hours. A non-exempt employee shall not be authorized to incur hours worked or overtime for using email or logging into the City's network outside their normally scheduled work hours, unless explicitly requested by the employee's supervisor. The City discourages use of cell phones (City-issued or personal) while operating a motor vehicle. Mobile communications device users are encouraged to place and answer calls prior to engaging a motor vehicle, or during a break from operation of the motor vehicle. In some jurisdictions, laws may prohibit the use of cell phones while operating a motor vehicle. It is the City's expectation that mobile communications device users will abide by all applicable laws.

Mobile communications device users using City-owned devices or connecting personal devices to the City's non-public networks shall sign the relevant waiver forms prior to obtaining network access credentials for the device. In order to receive an access key for a non-public network, the City may require the mobile communications device user to provide an e-mail address associated with the device.

Section 2: City-Provided Smartphone/ Cellular Phones and Mobile Data Devices

The City may provide and maintain mobile data devices for mobile communications device users requiring mobile access to data. The City may provide and maintain smartphones / cellular phones and/ or mobile data devices for certain eligible employees, if approved by their Department Director and approved by the City Administrator. In general, the following criteria will be used to determine eligbility.

- The position requires the ability to respond to business requests on a regular basis.
- The position requires the employee to frequently work off-site during business hours or on an on-call basis.
- Position job duties require immediate or emergency response during regular business hours and after business hours.
- Position job duties require frequent access of wireless networks outside of the office environment

City-issued communication devices are for dedicated business use. Incidental personal calls or texts on City-issued devices will be acceptable. Frequent personal use that interferes with an employee's job functions is prohibited. Personal use may be considered excessive if it causes the City to increase its alloted minutes or payment plan for that department. Frequent personal use,

regardless of time of use, may result in reimbursement to the City of any cost associated with personal use.

The service and City-owned equipment should be procured through appropriate available government procurement practices.

Work-related applications may be purchased for a City-owned device with prior approval by the department director. Applications that negatively interact with the City-owned device or with the City's network are prohibited on City-owned devices.

All devices remain City property and shall be returned to the City upon termination of employment, upon end of term of office, or if the device is no longer necessary for work-related purposes.

The purchase of City-owned devices must be done either through the IT Division or in consultation with the IT Division to ensure the device is currently supported by the IT Division.

Cellphone, smartphone and other mobile data devices are purchased, installed, maintained and owned by the City of Apple Valley to facilitate business communications. The contents of communications either made or stored are accessible at all times by City management. These systems shall be treated like other shared filing systems.

All electronic communications on City-owned devices are City records. The contents may be obtained and disclosed without your permission. **Therefore, the user should not assume that messages are either private or confidential.**

Section 3: Personal Mobile Data and Smartphone Devices Allowance
If approved by their Department Director and approved by the City Administrator, a stipend may be provided for privately-owned personal mobile data devices (including smartphones) that are purchased by the mobile communications device user and used for City business. Business necessity includes meeting customer or client service expectations in a timely fashion; need for immediate communication with department staff or others where employee job requirements take the employee outside of primary work area; need for access to data or phone communications on properties where wired access is not available; or job duties support 24x7 business infrastructures and require immediate response(s) to urgent communication needs.

Availability
An employee receiving a stipend for a smartphone device must make the phone number available to his or her supervisor, the IT Division, and emergency contacts and Emergency Operations Plan (EOP) call list if the employee is a designated EOP contact.

Licensing
Each data device syncing with City communications systems requires a Client Access License to be procured by the City.

Repair and Maintenance
Mobile communications device users receiving a stipend for a communications device are personally responsible for ensuring the device is in good working order. The IT Division is not responsible for upkeep, support or replacement of personal devices that are used for City business. IT support will be limited to instructions for the mobile communications device user on how to sync email, schedules, and tasks (if available), and use of City-supplied security products (if available). The City assumes no liability for any direct or indirect damages arising from the user's use of personal data device.

Connecting a personal device to the City's network opens the City's network to security vulnerabilities. Mobile communications device users connecting a personal device to the City's network are responsible for taking appropriate steps to keep their device operating systems current and updated and to protect their connected devices from virus, malware, and security threats. The City reserves the right to deny connection to the network for any personal devices the IT Manager deems to be a significant security risk to the City's network or resources. If an application on a personal device is found to negatively interact with the City's network, the City may prohibit connection of that device to the City's network until the application is removed.

Compliance with IRS Regulations
Payments by the City are considered a taxable benefit and will be included as taxable income to the employee or elected official.

Stipends
Stipends will be on a tiered basis based on each department's determination of appropriate need for the employee with the device:

Tier	Description	Monthly Amount
Tier #1	Limited Use Need (Voice and Text Only)	$20
Tier #2	Wi-Fi Data Need Only	$30
Tier #3	Voice, Text, and Data Need	$50

An employee must submit a Request for Stipend form to his or her supervisor to approve the payment of a stipend. Department directors will determine if a City-owned device or stipend will be provided for an employee. All payments are subject to the approval of the City Administrator and may be eliminated if job duties change such that the above criteria are no longer met. Departments should review employee needs for communications devices annually.

Work-Related Applications
Work-related applications may be purchased by the City and used on a personally-owned device with prior approval by the department director or City Administrator.

Interference with Job Duties
Department directors may prohibit employees from carrying their own personal devices during working hours if it interferes with the performance of their job duties.

Section 4: Responsibility

An employee who is found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

City of Apple Valley
Information Technology Policy
Employee Acknowledgement and Receipt

I acknowledge receipt of a copy of the Information Technology Policy. I agree to familiarize myself with the contents of the policy and to observe and comply with them.

Employee Name:_____
(please print)

Employee Signature:_____

Date:_____

City of Apple Valley
Information Technology Policy
Training Attendance Acknowledgement

I hereby acknowledge that I attended a training session on _____ at the City of Apple Valley. The training covered the City's Information Technology Policy.

Employee Name:_____
(please print)

Employee Signature:_____

Date:_____

Please sign this form and return it to your facilitator

Thank you.

City of Apple Valley

Wireless Communications
Device and Phone Policy
Employee Acknowledgement and Receipt

I acknowledge receipt of a copy of the Wireless Communications Device and Phone Policy. I agree to familiarize myself with the contents of the policy and to observe and comply with them. I understand that these policies may be added to, or changed by the City at any time. It is my responsibility to bring any questions I have about the Wireless Communications Device and Phone Policy to my supervisor or to a representative of the IT Division.

I understand that I am requesting that the City provide me with access credentials for my mobile device or phone to access the City's Microsoft Exchange or other network assets. I understand that in managing access to its network assets, the City may require that I install a mobile device management system application on my device as a condition of access.

Employee Name:_____
(please print)

Employee Signature:_____

Date:_____

City of Apple Valley

Employee Wi-Fi Wireless
Network Access Policy
Employee Acknowledgement and Receipt

The City of Apple Valley (the "City") provides free wireless internet access to the public, employees, and elected officials at certain City facilities ("Hotspots"). My use of the Hotspots is subject to the terms and conditions of this policy.

Employees and elected officials may request an automatic connection of City-owned devices or personal devices used for work purposes to the City's employee Wi-Fi network. I understand that in order to receive an access key for the non-public network, the City requires me to provide an e-mail address associated with the connected device.

The City does not provide printing, computer or technical support, or security protection for Hotspot users. Hotspots shall not be used by any person located outside of City facilities.

Hotspots shall not be used to view or access pornographic or obscene material, or for any illegal or unauthorized purpose. The City retains the right to monitor or filter my use of the Internet through Hotspots at the City's discretion. The City may restrict, suspend, or terminate my use of Hotspots for any reason, including violation of City policies or guidelines.

My use of hotspots is solely at my own risk. All representations and warranties related to the hotspots and the Internet are hereby excluded and disclaimed. Hotspots are provided on an "as is" and "as available" basis. The City makes no warranty that Hotspots or any information, software, or material accessible on the Internet is free of viruses, worms, Trojans, malware or other harmful components. Hotspots are not secure and may provide third parties with an opportunity to access my computer, software and data and to monitor my use of the Internet.

By using Hotspots, I agree to release the City from any claim you may have or acquire and agree to indemnify and hold the City and its officers, employees, agents and contractors harmless from any claim, liability, loss, damage, cost, or expense (including without limitation reasonable attorney's fees) arising from or related to my use of the Hotspots or the Internet.

Employee Name:_____
(please print)

Employee Signature:_____

Date:_____

Associated E-mail Address:_____

City of Apple Valley

Wireless Communications Device and Phone Stipend Request and Authorization Form

Employee Name: _____ **Department:** _____

Employee Plan Information

Cell Phone Number:_____
Service Provider: _____
Must attach copy of provider billing as proof of phone or data service plan.

Stipend Request (check one)

Voice and Text Only ($20 per month) _____
Wi-Fi Data Need Only ($30 per month) _____
Voice/Text/Data/E-mail ($50 per month) _____

Employee Affidavit:

By accepting a voice stipend, I understand that I must have a mobile device available for use during business hours and department-established on-call times up to and including 24/7. I understand that as a device used for work purposes, the phone number may be made available as public information. For all stipends, I am responsible for all costs associated with purchase, maintenance, replacement and upgrade of the mobile device to ensure service availability. I will pay all taxes, including personal income tax, on any Mobile/cellular phones/Smartphone allowance paid pursuant to the policy. I understand that the allowance will no longer be paid if the City determines there is no need or if I am no longer employed by Apple Valley.

Employee Signature: _____ **Date:** _____

Approvals

Department: _____ Date: _____

City Administrator: _____ Date: _____

Finance Director: _____ Date: _____

This form must be kept on file with the Finance Department and renewed annually.