City of Marietta Technology Usage Policy

Purpose

The intent of the Technology Usage Policy is to define the acceptable use of technology at the City of Marietta and to ensure that the City complies with all legally mandated requirements. It outlines the responsibilities of those who work for and on behalf of the City in contributing to the maintenance and protection of its information resources in a secure, stable and cost-effective manner. This policy is consistent with the intent and requirements of the City's work policies and rules.

Policy Scope

The City of Marietta's Technology Usage Policy defines the oversight, use and protection of the City of Marietta's computing equipment, network, voice, electronic communications and data repositories. This includes the acquisition, access and use of all software, hardware and shared resources, whether connected to the network, configured off the network, or while in transit (mobile).

It applies to all those who work on behalf of the City of Marietta including, but not limited to, employees, contractors, consultants, temporaries, supplementals, interns, volunteers and other workers including all personnel affiliated with third parties. This policy also applies to all equipment that is owned or leased by the City regardless of project and program funding sources.*

Acquisition of Technology Resources – The Information Technology Department must evaluate and approve all software, hardware, removable devices, and related maintenance and support contracts, whether the selected products or solution will be on the network or off; used by one or many people; and for all program and project funding sources.* In addition, acquisition of technology resources should conform to existing purchasing policies and procedures as defined by your Information technology Department. Most City-owned technology has a pre-determined lifecycle replacement period and must be surrendered for replacement on a 1:1 basis or retired, according to that schedule. Such technology may not be redeployed or otherwise put back into use without approval from the Information Technology Department.

Access to the City's Technology Resources

- The IT Department must approve the setup of new user* accounts.
- Users are responsible to establish and maintain passwords consistent with the City's standards.
- User accounts and ALL passwords may not be shared with anyone other than the named owner and City IT employees. Examples include co-workers, subordinates, business associates, household members, etc.
- The individual logged onto the City network must be present while the logon credentials are being used to access Network resources, or must ensure that the account is locked or logged off and not being used by others when not present.
- Information Technology must approve connection of ALL devices using the City's infrastructure (i.e. Internet, network, wireless channels, switches, hard drives, and telephone lines).
- Information Technology must approve installation of all software, freeware* and software that is obtained for evaluation purposes.
- Any software or files downloaded via the Internet into the City's network become the property of the City. Any such files or software may be used only in ways that are consistent with their licenses and/or copyrights.
- Direct secure (peer-to-peer)* connections are provided only in unique circumstances, requiring prior approval from the IT Department.

- Information Technology must be consulted during the ***infancy*** stages of major projects pertaining to or including IT equipment and/or software.
- Connection or installation of personally-owned hardware or software within the City-provided infrastructure (i.e. network, Internet, cell phones, fax lines, telephone lines, and other computers) is not allowed.
- All activity resulting from device*, network or software application access is the responsibility of the person assigned the user account.

Remote access to City Systems

Remote access to certain City systems, applications, and data is maintained for selected employees. City remote access systems require a high level of application and user maintenance as well as monitoring. In addition, they significantly increase the security risks associated with outside access to applications and data. Remote access systems are therefore restricted only to those City Officials and employees who show a demonstrated necessity to access data or applications while away from City facilities and ONLY for City business. Remote access will not be granted for convenience. Users who do not regularly utilize remote access systems may be removed as Remote Access Users. Use of remote access for other than official business will result in immediate removal as a remote user and, if appropriate, disciplinary action.

1. Authorization Required

Prior to use by any City Official or employee, the appropriate City Official must submit a written request to the IT Department identifying the user and stating what business necessity exists requiring the potential user to utilize remote access. Permission will be based on demonstrated need and subject to the criteria listed below.

2. Web Based Email (WebMail)

The City maintains a WebMail system (https://officemail.mariettaoh.net/owa) that allows access to the City email system.

Internet and Intranet Usage

- Use of the Internet should be consistent with City policies and work rules. Incidental personal use of City resources is allowed as defined in the paragraph Incidental Personal Use. See examples of incidental use in Appendix B. Visiting, referencing, downloading and/or storing materials that are inappropriate in a work environment is prohibited unless such activity is specifically related to your job. Examples include but are not limited to data from sexually explicit sites, and those associated with violence, hate crimes or illegal activities.
- Content and images posted on the City's website, FTP, Cloud, or Social Media sites should be consistent with the City's policies and practices, and should conform to professional standards in tone and format.
- The City wants its officials and employees to be aware that its security systems are capable of recording (for each and every user) each World Wide Web site visit. The City keeps a log (public record) of employees accessing the Internet which will be periodically audited. No user should have the expectation of privacy as to his/her Internet usage.
- Monitoring and Reporting of Internet Use - It is the responsibility of Department Heads to monitor and audit Internet web use within their department. Because there is the potential for employee abuse of the system, the City may monitor and record user access to Internet sites and provide the Department Heads with information that can be used to track access to all Internet sites as required or requested to enforce City or department policy
  *defined in Appendix A
- All information that is posted, copied or shared, either on the City's servers and desktops or on

the City's website or Social Media sites, must be done so in accordance with the laws that govern copyrighted materials including, but not limited to, photographs, magazines, books, copyrighted music, the installation of any copyrighted software for which the City or end user does not have an active license, or the installation of "pirated" software.

- Web usage that significantly impacts network bandwidth may be restricted. Individuals should utilize only the City's tools and recommended best practices to manage their connections when viewing, downloading, sharing and printing information to ensure that these shared resources are not negatively impacted.
- Any attempt to misrepresent one's identity on the Internet (via newsgroups, social media, chat rooms, blogs, etc.) is prohibited except when performed by an officer during a police investigation.

E-mail Communications

- The City provides access to and support of its own e-mail system and web-related components. Use of any other e-mail system to conduct City-related correspondence is prohibited, due to public record laws.
- The electronic mail system is intended for business purposes. Electronic mail communications constitute public records and the City has the right to access or monitor messages for work-related purposes, security, or to respond to public record requests. All messages should be composed with the expectation that they are public. Refrain from using your City email address for anything other than official business.
- Users shall have no expectation of privacy in email messages, whether they are business related or an allowed personal use as provided herein. Use of electronic mail shall be considered consent to City Officials, managers, and other employees to inspect, use, or disclose any electronic mail or other electronic communications and/or data.
- Use of Non-City Email Accounts - Non-City email accounts (like MSN, Yahoo!, Gmail, Hotmail, etc.) may not be used to conduct City business. Likewise, a non-City email account may not be forwarded to a City email account.
- Transmission of Confidential Information - Confidential material must not be sent via electronic mail. Electronic mail messages may be intercepted, viewed, and used for non-approved purposes, especially when corresponding via the Internet, a medium over which the City has no control.
- E-mail communications will conform to the same professional standards as with written and verbal business correspondence. A professional tone should prevail and content will be consistent with and representative of the City's policies and practices.
- Any attempt to misrepresent one's identity via e-mail is prohibited.
- E-mail is considered part of the public record and is subject to disclosure under Ohio State law. Managing individual e-mail storage and retention is the responsibility of each department, consistent with document and records-retention guidelines. Effort should be made to restrict unnecessary e-mail traffic, including minimizing the size of attachment files; and using network drives instead of large distribution lists to share file attachments with large groups.

Intellectual Property, Privacy and Monitoring

There is no right to privacy in the course of using the City's technology resources, whether conducting City business or for incidental personal use. The City owns all data stored on its network and peripheral devices and reserves the right to inspect and monitor any and all such use at any time (examples include e-mail, voice-mail, Internet logs, computers, laptops, cell phones, etc.). The City may conduct requested audits in order to ensure compliance with its policies and requirements, to respond to public disclosure* requests, investigate suspicious activities or security threats, or to fulfill legally mandated requirements (i.e. software

license rules, Payment Card Industry (PCI*) regulations, and the Health Insurance Portability and Accountability Act (HIPAA*) requirements).

Incidental Personal Use

The City's technology resources including e-mail and Internet web browser are City property and intended for use to conduct City business by its authorized employees, contractors, consultants, temporaries, supplementals, interns, volunteers and other workers including all personnel affiliated with third parties; hereafter referred to as the user. Limited personal use is permitted as long as it does not result in a cost to the City, does not interfere with the responsibilities and fulfillment of job duties, is brief in duration and frequency, does not distract from the conduct of City business and does not compromise the security or integrity of City information or software. As noted previously, there is no right to privacy in the course of using the City's technology resources, whether for City business or incidental personal use.

Permissible Use - This policy allows minimal personal e-mail under specific circumstances. Personal e-mail must conform to permissible use standards and may not be related to activities listed as prohibited uses. Apart from this, the rule does not sanction the use of City computers for unofficial purposes, e.g., writing letters, playing computer games, surfing the Internet, etc.. Downloading personal email to the City's system or attaching a personal email box is prohibited. See Appendix B for specific examples of permissible personal use.

*defined in Appendix A

Prohibited Uses - A prohibited use is any use related to the conduct of an outside business; a use for the purposes of supporting, promoting, or soliciting for any non-City sponsored outside organization or group; or religious activity, campaign or political use; commercial use; posting to or buying from online auction or sales sites; use to conduct illegal activities; any entertainment uses; and/or uses which result in the City being placed on electronic mailing lists related to prohibited uses. See Appendix B for specific examples of prohibited use. Soliciting funds for any purpose, except as may be used for the expression of condolences and sympathy for City employees. The IT Director has the authority to make an exception on a case by case basis.

Security, Storage and Protection

Effective security requires the participation and support of every user in the organization. The City employs enterprise tools to manage, monitor and protect the organization from internal and external security threats and data loss. In addition to these measures, it is the responsibility of individuals to remain vigilant in their awareness and protection of the City's resources, including equipment and data they have access to and while in their possession. Specific due diligence requirements are outlined below:

• City devices and computer equipment must be logged out or "locked" when unattended. **This also includes a screen lock on City smart phones.

• All users must log off of their pc and leave it powered on at the end of their shift to enable off- shift maintenance and security updates

• Intruding or attempting to intrude into any gap in the system or network security is prohibited. Sharing of information with others that facilitates their unauthorized access to the City's data, network or devices, or their exploitation of a security gap is also prohibited.

• It is the responsibility of each individual to prevent unauthorized and indiscriminate access to "personal information" (see Definitions) that could pose the threat of identity theft, thus risking a person's privacy, financial security and other interests.

• As noted above, user accounts and passwords may not be shared. The individual logged onto the City

network must be present while logon credentials are being used to access Network resources

• In general it is not permissible to download “personal information” to any removable/portable device, including laptop computers, unless access to that information is within the scope of your job, your manager has approved the copy of information to a portable device and the data or device is encrypted*. Please see the City’s Personal Information Security policy for further information.

• Transmitting confidential* data in part or full via e-mail or other unencrypted medium is prohibited.

• Leaving personal, sensitive* or confidential* information exposed to view while unattended, either on paper or on screen, is prohibited.

• Whenever possible, laptop and desktop hard drives and removable devices should only contain copies of source files, not the original file.

• Individuals must report to the City any equipment, software or data that is lost, damaged or stolen at their first available opportunity. Reports will be made to a supervisor, manager, or director. Unrecoverable equipment may incur additional replacement costs.

• Lost equipment, especially that containing sensitive or confidential information as defined here, including building access cards, must be reported immediately to the I.T. Staff.

• Stolen computers, laptops, thumb drives, smart phones, etc. must be reported immediately to the Police Department at 740-376-2007 **AND** to the IT Staff.

• Individuals must utilize City provided anti-virus software and scanning tools regularly to scan material from removable devices* prior to use.

• Storage of any copyrighted material on a network server or local hard drive including, but not limited to, photographs from magazines, books or other copyrighted sources, copyrighted music, the installation of any copyrighted software for which the City or end user does not have an active license, or the installation of “pirated” software is strictly prohibited.

Reporting and Administration

Anyone who observes or suspects a violation of these policies and requirements, or a potential gap in security or protection of the City’s assets or data, should immediately report these to their Department Head, or the Safety Service Director. Violations may result in disciplinary actions up to and including termination of employment. Requests for exceptions to any of the Technology Usage Policy definitions must be submitted in writing from department heads to Information Technology. Exceptions require the approval of both the requesting department’s director and the IT Director. Approvals must be documented in writing and limited in duration to provide for periodic re-evaluation.

*defined in Appendix A

Social Media

Legal stuff: The goal of the City's social media channels is to serve as an online information source focused on city issues, projects, news and events, and is not intended as a public forum. The social media sites are administered by the City of Marietta, but the content on the sites is not entirely controlled by the City. The City does not endorse any link or advertisements on its social media sites placed by the site owners or their vendors or partners. The City reserves the right to remove any content from its social media sites at any time.

Comment Policy: All comments posted to the City's social media page will be monitored. The City reserves the right to remove inappropriate comments including those that: contain obscene language, or sexual content; threaten or defame any person or organization; violate the legal ownership interest of another party; support or oppose political candidates or causes; promotes illegal activity; promote commercial services or products, or are not related to the particular topic."

The City of Marietta reserves the right to restrict or remove any content that is deemed to be in violation of its Social Media Policy or any applicable law.

Policy Purpose - This Social Media Policy ("Policy") establishes guidelines for the establishment and use by the City of Marietta ("City") of social media sites as a means of conveying information to members of the public.

The intended purpose of City social media sites is to disseminate information from the City about the City's mission, meetings, activities, and current issues to members of the public.

The City has an overriding interest and expectation in protecting the information posted on its social media sites and the content that is attributed to the City and its officials.

Definitions - "Social media sites" means content created by individuals, using accessible, expandable, and upgradable publishing technologies, through and on the internet. Examples of social media include, but are not limited to, Facebook, Twitter, Blogs, RSS, YouTube, LinkedIn, and Flicker.

"City social media sites" means social media sites which the City establishes and maintains, and over which it has control over all postings , except for advertisements or hyperlinks by the social media site's owners, vendors, or partners. City social media sites shall supplement, and not replace, the City's required notices and standard methods of communication.

"Posts" or "a posting" means information, articles, pictures, videos or any other form of communication posted on a City social media site.

General Policy -

1. The City's official website at www.mariettaoh.net (or any domain owned by the City) will remain the City's primary means of internet communication.

2. The establishment of City social media sites is subject to approval by the IT Director.

3. All content on City social media sites shall be reviewed, approved, and administered by the City's Public Information Officer or a designated City employee.

4. City social media sites shall clearly state that such sites are maintained by the City and that the sites comply with the City's Social Media Policy.

5. City social media sites shall link back to the City's official website for forms, documents, online services and other information necessary to conduct business with the City.

6. The City's Public Information Officer shall monitor content on City social media sites to ensure adherence to both the City's Social Media Policy and the interest and goals of the City.

7. The City shall use social media sites as consistently as possible and in conjunction with other established City communication tools.

8. Members of the City Council and City Administration shall not respond to any published postings, or use the site or any form of electronic communication to respond to, blog or engage in serial meetings, or otherwise discuss, deliberate, or express opinions on any issue within the subject matter jurisdiction of the body.

9. The City reserves the right to terminate any City social media site at any time without notice.

10. City social media sites shall comply with usage rules and regulations required by the site provider, including privacy policies.

11. The City's Social Media Policy shall be displayed to users or made available by hyperlink.

12. All City social media sites shall adhere to applicable federal, state and local laws, regulations and policies.

13. City social media sites are subject to the Ohio Public Records Act. Any content maintained on a City social media site that is related to City business, including a list of subscribers, posted communication, and communication submitted for posting, may be considered a public record and subject to public disclosure.

14. Employees representing the City on City social media sites shall conduct themselves at all times as a professional representative of the City and in accordance with all City policies.

15. All City social media sites shall utilize authorized City contact information for account set-up. The use of personal email accounts or phone numbers by any City employee is not allowed for the purpose of setting-up a City social media site.

16. City social media sites may contain content, including but not limited to, advertisements or hyperlinks over which the City has no control. The City does not endorse any hyperlink or advertisement placed on City social media sites by the social media site's owners, vendors, or partners.

17. The City reserves the right to change, modify, or amend all or part of this policy at any time.

Content Guidelines

1. The content of City social media sites shall only pertain to City-sponsored or City-endorsed programs, services, and events. Content includes, but is not limited to, information, photographs, videos, and hyperlinks about events that affect the majority of Marietta residents.

2. The City shall have full permission or rights to any content posted by the City, including photographs and videos.

3. Postings shall be made during normal business hours. After-hours or weekend postings shall only be made with approval of the City Public Information Officer.

4. Any employee authorized to post items on any of the City's social media sites shall review, be familiar with, and comply with the social media site's use policies and terms and conditions.

5. Any employee authorized to post items on any of the City's social media sites shall not express his or her own personal views or concerns through such postings. Instead, postings on any of the City's social media sites by an authorized City employee shall only reflect the views of the City.

6. Postings must contain information that is freely available to the public and not be confidential as defined by any City policy or state or federal law;

7. Postings may NOT contain any personal information, except for the names of employees whose job duties include being available for contact by the public;

8. Postings to City social media sites shall NOT contain any of the following:

8.1. Comments that are not topically related to the particular posting being commented upon;

8.2. Comments in support of, or opposition to, political campaigns, candidates or ballot measures;

8.3. Profane language or content;

8.4. Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, or status with regard to public assistance, national origin, physical or mental disability or sexual orientation, as well as any other category protected by federal, state, or local laws;

8.5. Sexual content or links to sexual content;

8.6. Solicitations of commerce;

8.7. Conduct or encouragement of illegal activity;

8.8. Information that may tend to compromise the safety or security of the public or public systems; or

9. These guidelines shall be displayed to users or made available by hyperlink on all City social media sites. Any content removed based on these guidelines must be retained, including the time, date and identity of the poster, when available.

10. The City reserves the right to implement or remove any functionality of its social media site, when deemed appropriate by the Public Information Officer. This includes, but is not limited to, information, articles, comments, pictures, videos or any other form of communication that is posted on a City social media site.

11. Except as expressly provided in this Policy, employees accessing any social media site shall comply with all applicable City policies pertaining to communications and the use of the internet including e-mail content.

12. All of the content on City social media sites must be provided to the City's Public Information Officer or designated City employee for review, approval and subsequent posting to the social media site.

Current City employees who are able to post on behalf of the City on Social Media:

Public Information Officer/Network Administrator – Amy Tucker

Hardware/Software Administrator – Scott Steinel

Mayor's Secretary – Cheyenne Oaks

Chief, Marietta Fire Department – CW Durham

Nursing Secretary, Health Department – Diane Drost

911 Dispatcher, Marietta Police Department – Steve Baumgard

911 Dispatcher, Marietta Police Department – Kevin Burns

911 Dispatcher, Marietta Police Department – Toni Roach

911 Dispatcher, Marietta Police Department – Tamela Miller

Social Media (Personal Account Advisements)

- Employees should conduct themselves in an appropriate manner at all times.
- Remember that this is a small area and people know where you work whether you have labeled it or not.
- Do not engage in negative discussion regarding the City.
- Avoid shenanigans in work hours and within the workplace.
- Don't say anything about your colleagues or boss or workplace on social media.
- Express only your personal opinions. Never represent yourself as a spokesperson for the City of Marietta.
- If the City is a subject of the content you are creating, be clear and open about the fact that you are an employee and make it clear that your views do not represent those of the City, fellow employees, customers, suppliers or people working on behalf of the City.

- If you do publish a blog or post online related to the work you do or subjects associated with the City, make it clear that you are not speaking on behalf of the City.
- It is best to include a disclaimer such as “The postings on this site are my own and do not reflect the views of the City of Marietta.”

City Cellular Phone Usage

- Refer to Codified Ordinance 333.11 USE OF ELECTRONIC WIRELESS COMMUNICATION DEVICES WHILE DRIVING PROHIBITED
- Understand that City cell phone devices should be used with the same expectation as City computer equipment/email and are subject to public record.
- Be prepared to explain high usage of data or minutes used. Any use greater than 4 GB/monthly or 500 minutes shall be investigated by a supervisor/administration.
- Standard City phones (non-smart phones) are limited to 100 text messages per month.
- Revocation of privileges, followed by additional disciplinary actions are possible if abuse occurs.

APPENDIX A DEFINITION OF TERMS

CONFIDENTIAL (DATA) – for purposes of this policy, examples include but are not limited to social security numbers, health and insurance information, and any combination of information that would allow a person's identity or information to be further compromised (credit card number and name).

DEVICE – any piece of equipment attached to a computer in order to expand its functionality. Some of the more common peripheral devices are printers, scanners, disk drives, speakers, cameras, etc. For purposes of this policy, the word device also includes removable devices such as USB devices, cell phones, etc.

ENCRYPTION – a process by which data is converted into a form that cannot be easily understood by unauthorized access. It is generally thought that encryption is the final layer of data protection, since it assumes the device on which the data is stored has already been compromised. Unless the perpetrator has the encryption key, they cannot decode any of the data stored there. In the most secure environments, entire hard drives can be maintained in an encrypted state. This is typically only recommended on mobile devices, not those that are already secured inside an organization's network.

FTP (File Transfer Protocol) – a communications protocol that is used to connect two computers over the Internet so that the user of one computer can transfer files and perform file commands on the other computer. Companies will often create FTP sites to allow sharing of large files. Cloud.

FREEWARE / SHAREWARE – Freeware is copyrighted computer software which is made available for use free of charge, for an unlimited time. Google and Yahoo tools for personal use are an example of Freeware. Shareware generally requires the user to pay for software use after a designated trial period. The biggest issue with such programs is that there aren't any standards applied to its development; and thus there is little in the way of validation between legitimate and non-legitimate products. Recent industry studies have shown that even with legitimate programs, up to 76% of them are abandoned and never updated. Oftentimes the terms shareware and freeware are used loosely on non-legitimate Internet sites to entice unsuspecting end users to download files and programs that contain viruses or other malware. Items that are designated as Free for personal use may have licensing implication for Business use. Government use is considered business use.

FUNDING SOURCE - examples include but are not limited to: operational funds, the general fund, capital equipment project funding, grant-funded projects and programs, research and development funds and donations.

HIPAA - To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, included "Administrative Simplification" provisions including national standards for electronic health care transactions. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information, so also incorporated provisions that mandated the adoption of Federal privacy protections for individually identifiable health information. Any agency or entity that stores health-related data must conform to the provisions as outlined in HIPAA.

PCI / DSS - stands for Payment Card Industry Data Security Standard. This set of policies and processes was developed by the major credit card companies as a requirement to help organizations that process credit card payments to prevent fraud, hacking and various other security issues. A company processing credit card payments must be PCI compliant or they risk losing the ability to process credit card payments.

PEER-TO-PEER - A peer-to-peer (or P2P) computer network relies primarily on the computing power and bandwidth of the participants in the network rather than concentrating it in a relatively low number of servers. A pure peer-to-peer network does not have the notion of clients or servers, but only equal peer nodes that simultaneously function as both "clients" and "servers" to the other nodes on the network.

PUBLIC DISCLOSURE - As a local government agency in the state of Ohio, the City of Marietta is required

by law to follow specific guidelines in the management of its public records. These guidelines include adhering to retention schedules and the specific handling of public disclosure requests. They also include definitions of what is disclosable and what is not.

REMOVABLE DEVICE – Any storage device that can be removed from a computer, laptop or network with or without administrative privileges to the device. Examples include but are not limited to: removable hard drives; cameras; memory cards; thumb drives (aka "flash" drives); hot-swappable CD/DVD drives, etc.

SENSITIVE (DATA) – for purposes of this policy, "sensitive" refers to examples of information that relates to a person's state of employment, including personnel matters, disciplinary actions, and employee appraisal documentation. A good rule of thumb is that sensitive information is intended only for the parties who are directly involved or impacted by it. It would not be freely shared with others unless specifically warranted by permission or legal mandates.

SOCIAL MEDIA - media designed to be disseminated through social interaction, created using highly accessible and scalable publishing techniques. Social media supports the human need for social interaction, using Internet- and web-based technologies to transform broadcast media monologues (one to many) into social media dialogues (many to many). It supports the democratization of knowledge and information, transforming people from content consumers into content producers. Social media can take many different forms, including Internet forums, weblogs, social blogs, wikis, podcasts, pictures, video, rating and bookmarking.

TECHNOLOGY RESOURCES – the physical and communication components that are necessary for hardware and software applications to perform in a diverse corporate environment. These include but are not limited to the servers, complex network of cabling, telecommunication and Internet devices, etc. The ability to leverage existing infrastructure or extend its use is often a primary consideration in any new project proposal involving a technology component.

USERS – examples include but are not limited to full and part-time employees; council members; contractors or consultants with network accounts and those granted access to the secure City network or extranets; supplemental, temporary or limited-term employees; interns and volunteers.

Reference www.wikipedia.com for some definitions

City of Marietta Technology Usage Policy
APPENDIX B

Examples of permissible personal e-mail use

The following are examples of allowable computer uses, so long as the permissible use requirements are met:

1. User sends an e-mail communication home to make sure his or her children have arrived safely from school.
2. User receives a brief e-mail from his or her son or daughter, who is away at college, solely for the purpose of telling the parent he or she is coming home for the weekend.
3. User is flying to visit relatives but flight plans have changed, and user is sending e-mail solely for the purpose of informing the relatives of the new arrival time.

Examples of permissible computer use

The following are examples of allowable computer use, so long as the permissible use requirements are met:

1. Uses the Internet to view City job announcements.
2. Uses the Internet to check weather or commute information.
3. Uses City computer to take on-line job-related training courses pre-approved by supervisor or manager in lieu of attending a similar class off-site.
4. Uses City computer to read the newspaper during breaks.

Examples of non-allowable computer use

The following are examples of computer uses that are not allowed. This list is not intended to be all-inclusive. Additionally, any use that is not expressly allowed is considered to be not allowable:

1. Uses the Internet to track his personal investment portfolio.
2. Uses City e-mail to solicit for non-City sponsored charity or fundraiser.
3. Uses Internet to do personal research such as comparison-shopping for automobiles.
4. Uses City e-mail to sell or give away personal items; e.g. baseball or theater tickets.
5. Download software to City computer from the Internet.
6. Uses Internet to access nude or sexually explicit materials (text, photographs, graphics, etc.) that are not related to their duties.

When using your City computer it is a good idea to ask yourself this question: Can I directly support a work purpose for this use? If the answer is yes, there should be no problem. Apart from Incidental Personnel Use, if the answer is no, don't do it.

If you have questions as to what constitutes City business, please ask your department head. If you have questions about this policy, please contact the Safety Service Director or IT Department.

PAGE
INTENTIONALLY
LEFT
BLANK

City of Marietta Technology Usage Policy

APPENDIX C

My signature below indicates that I have received a copy of the Technology Usage Policy and have read and understand my responsibilities as a user of the City's technology resources. I understand this policy is subject to change without notice and agree to abide by it and all subsequent changes. I also understand that violation of the policy may result in disciplinary action including termination.

Employee Signature _____ Date _____

Employee Name (print) _____ Dept._____

Employee's Supervisor Name (print)_____