ORDINANCE NO. 2017- 003

AN ORDINANCE OF THE CITY OF FLORESVILLE, TEXAS ESTABLISHING CHAPTER 36 OF THE CITY'S CODE OF ORDINANCES RELATING TO CITY PROVIDED TECHNOLOGICAL DEVICE USAGE; ESTABLISHING POLICY AND RULES RELATING TO APPROPRIATE USAGE OF SUCH DEVICES; ESTABLISHING POLICY AND RULES RELATING TO SECURITY OF SUCH DEVICES; ESTABLISHING POLICY AND RULES RELATING TO RECORDS RETENTION OF SUCH DEVICES; ESTABLISHING DISCIPLINE FOR A VIOLATION OF THIS POLICY; AND ESTABLISHING AN EFFECTIVE DATE.

WHEREAS, the City of Floresville ("City") provides certain employees and officials with mobile devices, laptops, desktops, and/or other technological devices; and

WHEREAS, such devices are necessary for the efficient function of a municipality in the modern age; and

WHEREAS, there are inherent risks associated with the use of such devices that the City must seek to mitigate where able because inappropriate use of information technology exposes the City to additional internal and/or external vulnerabilities that may reduce the reliability, confidentiality, integrity and/or availability of those systems.; and

WHEREAS, to accomplish the goal of having a safe, effective, and reliable technological environment the City must adopt a comprehensive technological device usage policy.

NOW, THEREFORE BE IT ORDAINED AND ENACTED BY THE CITY COUNCIL OF THE CITY OF FLORESVILLE:

That the following amendments are made to the City Code of Ordinances regulating technological device usage for employees and officials of the City of Floresville:

Chapter 36

INFORMATION TECHNOLOGY DEVICE USAGE POLICY

SUBCHAPTER I. APPLICATION OF POLICY

Sec. 36.01. Scope and Purpose of Policy.

This Technological Device Usage Policy provides guidance for the acceptable use of information technology systems including electronic devices, electronic mail, Internet access, and/or software among other City systems. This includes acceptable use of City-owned computers, mobile devices and/or personal devices reimbursed through City stipends. This policy establishes and identifies responsibility for the acceptable use of technology to help ensure the confidentiality, integrity and availability of City systems.

Sec. 36.02. Definitions.
The following words, terms and phrases, when used in this subchapter, shall have the meanings ascribed to them in this section, except where the context clearly indicates a different meaning:

City-administered information technology systems means any technology or equipment that is used and/or managed by the City even if the City does not own the technology or equipment. City-managed information technology systems include technology or equipment owned by the City, on loan to the City, funded by grants, leased by the City, etc. Information Technology systems ("IT") includes but, are not limited to computers, mobile communication devices, telecommunication devices, servers, networks, software, databases and email messages, among other physical and virtual infrastructure.

Digital Signature means an electronic identifier intended by the person using it to have the same force and effect as the use of a manual signature.

Electronic mail record means an electronic government record sent and received in the form of a message on an electronic mail system of a government, including any attachments, transmitted with the message.

Electronic Record means a record created, generated, sent, communicated, received, or stored by electronic means.

Electronic Signature means an electronic sound, symbol, or process attached to, or logically associated with a record and executed or adopted by a person with the intent to sign the record.

Incidental Use means personal use of technology that does not interfere with the performance of assigned duties, does not have a detrimental effect on City information technology systems, and is not prohibited by this policy.

ITSD means the Information Technology Systems Department and is the designated individual or department responsible for maintaining the operation and security of the City's technological environment.

Local Government Record Retention Schedules means publications issued by the Texas State Library and Archives Commission under the authority of Subchapter J, Chapter

441 of the Government Code which establish the mandatory minimum retention period for a local government record except and as where superseded by a records retention schedule adopted by the City as authorized by the Government Code.

Malware means malicious software designed to impact the confidentiality, integrity and/or availability of an information technology system. Malware can include viruses, worms, Trojan horse, or adware among other malicious programs.

Network means a group of two or more computers linked together to facilitate communication, data sharing and processing among other computer activities.

Policy means this Technological Device Usage Policy

Records Management Officer means the person who administers the records management program established in each local government under section 203.026, chapter 203 of Local Government Code.

Retention Period means the minimum time that must pass after the creation, recording or receipt of a record or the fulfillment of certain actions associated with a record before it is eligible for destruction.

Sponsor means the departmental representative responsible for authorizing non-employee access to City assets and/or systems.

User means any employee or non-employee who uses City-administered information assets and/or systems, exclusive of the City's web and/or social media pages

SUBCHAPTER II. ACCEPTABLE USE OF TECHNOLGY SYSTEM

Sec. 36.10. Acceptable Use.

Personal use of technology must not interfere with the performance of assigned duties, must not have a detrimental effect on any City information technology system, and not be prohibited by this policy. This includes the personal use of City-owned or managed technology that:

(a) does not cause any additional expense to the City;
(b) is infrequent and brief;
(c) does not have a negative impact on overall user productivity;
(d) does not interfere with the normal operations of the a user's department or work unit;
(e) does not compromise the City in anyway;
(f) does not embarrass either the City or the user;
(g) does not contravene other elements of this policy; and

(h) serves the interest of the City in allowing employees to address personal matters which cannot be addressed outside of work hours without leaving the workplace.

Examples of personal communications that can be in the interest of the City include:

(a) communications to alert household members about working late or other schedule changes;
(b) communications to make alternative child care arrangements, communications with doctors, hospital staff or day care providers;
(c) communications to determine the safety of family or household members, particularly in an emergency;
(d) communications to reach businesses or governmental agencies that only can be contacted during work hours; and
(e) communications to arrange emergency repairs to vehicles or residences. City departments may consult with the Human Resources Department to determine whether a use is personal or business and if the usage is personal, whether it is incidental.

Sec. 36.11 Unacceptable Use.
The following activities are prohibited unless performed in the course of legitimate job responsibilities. The list below is by no means exhaustive, but provides a framework for activities which fall into the category of unacceptable uses of City IT systems:

(a) Engaging in any activity that is illegal under local, state and/or federal statutes as well as any activity that violates City policies and Administrative Directives;
(b) Accessing, displaying, storing or transmitting material that is offensive in nature, including sexually explicit materials, or any text or image that can be considered threatening, racially offensive, or hate speech. This includes any images, text, files, etc. sent via email to co-workers or outside parties. Accessing, storing, displaying, or transmitting pornographic materials using City-owned and managed technology is strictly forbidden;
(c) Engaging in any form of harassment, whether sexual or otherwise, or sending any unwelcome personal communication. It is the perception of the recipient that prevails in most instances, not the intent of the sender;
(d) Any personal use that interrupts City business and that keeps an employee from performing his/her work. Users should not use their City e-mail account as a personal email address or to register with a non-work related social network. City systems shall also not be used to chat online, "blog", or shop online;
(e) Extensive personal use of the Internet for any non work-related purpose during working hours which decreases the employees productivity or results in decreased performance of the City's Internet facilities;
(f) Violating any copyright, trade secret, patent and/or other intellectual property or similar laws or regulations, including, but not limited to, the installation or

distribution of "pirated" or other software products that are not appropriately licensed for use by the City;

(g) Revealing a City account password to others or allowing use of a City account by others. This includes household members and visitors when work is being done at home. Revealing a City account password to an authorized technician during a troubleshooting procedure is not a violation of this policy. In such a situation, a new password should be established as soon as possible, after the problem is resolved;

(h) Requesting a password to another users network or application account;

(i) Unauthorized reading, deleting, copying, modifying, printing and/or forwarding of electronic communications of another, or accessing electronic files of another without authorization;

(j) Unauthorized downloading or duplication of copyrighted material including, but not limited to, text and photographs from magazines, books or other copyrighted sources, copyrighted music and/or copyrighted movies. Downloading, copying, or installing copyrighted software for which the City or the end user does not have an active license is not permitted;

(k) Sending SPAM, chain letters, memes, and other non-City business related mass communications to either internal or external parties. Individual email accounts will be limited by technical controls as a preventive measure to detect SPAM originating from a City email account. Large volume emails to recipients will not be allowed from individual email accounts. Request for approved email accounts designated for such business purposes will be submitted to the City Manager;

(l) Approved email accounts must not regularly send bulk emails unless distribution lists are maintained. All undeliverable or invalid addresses from distribution lists must be regularly removed to prevent the City from not being able to send email through Internet Service Providers and/or mail hosts;

(m) Downloading and/or copying music, photographs or video material, including such material that has been obtained legally, onto City computers or servers unless such are for authorized City purposes;

(n) Downloading and/or installing executable program files from external media or the Internet without the approval of the City Manager or his/her designated official;

(o) Exporting software, technical information, encryption software and/or technology, in violation of international or regional export control laws;

(p) Using the City's electronic mail or Internet systems for private gain or profit;

(q) Using unauthorized personal software which allows peer-to-peer communications between two workstations (Yahoo Messenger, AIM, Google Talk, Torrent Networks, etc.);

(r) Maliciously introducing malware or similar programs into the network or server;

(s) All soliciting for political and/or religious causes as such are in violation of state and federal law, and/or other non-business uses not authorized by the City. Using City technology, electronic mail and/or Internet facilities for political activity including voting, private gain, gambling, shipping, games, entertainment or other non-business function unless permitted by this directive;

(t) Making fraudulent offers of products or services originating from any City account;

(u) Accessing any non-business related application which maintains a persistent application connection to the Internet, such as streaming videos or media, such as Pandora, YouTube, Netflix, and/or Google Video, among others;

(v) Including email "tag lines" or personal quotations other than ones that state the mission of the City or the user's Department;

(w) Using the City's email system to automatically forward City email to a personal email account;

(x) Causing security breaches or disruptions of City communications. Security breaches or disruptions can include, but are not limited to:

- Accessing data which the user is not authorized to access or logging into a server or user account that the user is not expressly authorized to access.
- Causing network disruptions for malicious purposes including, but not limited to, network sniffing, ping floods, packet spoofing, denial of service of any kind, and forged routing information for malicious purposes.
- Port scanning or vulnerability scanning for malicious purposes is prohibited. Non-malicious scanning that is part of a City-sanctioned security process is allowed. The City Manager or ITSD should be notified prior to any such scanning.
- Circumventing user authentication or security of any device, network or account.
- Maliciously interfering with or denying service through a denial of service attack, or by other means.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, and/or disable, another user's device or session, via any means, locally or via the City's network.
- Adding/removing hardware components, attaching external devices, and/or making configuration changes to information technology devices without the explicit approval by City Manager or ITSD.
- Storing confidential data on personally owned devices.

Sec. 36.12. Fees Associated With Use of IT Systems.

The user of any device owned by the City or operated on the City's network that incurs an unauthorized fee or expenditure in excess of that approved by the City Manager shall be responsible for reimbursement to the City for the actual charge incurred as well as any associated taxes, penalties, and fees associated therewith. This shall include overage fees for excessive minutes, text messages, and internet usage as applicable.

Sec. 36.13. Monitoring to Ensure Compliance With Usage Policy.

City systems may be monitored by the City to support operational, maintenance, auditing, security and/or investigative activities including enforcement of this Policy, legal requests, and public records requests or for other business purpose. Only Department Directors or higher may request monitoring of City administered IT systems for employees under their supervision for administrative purposes. Unauthorized monitoring

or reading of electronic communications systems or their contents violates this Policy. Any request to monitor must be approved by the City Manager or his/her designees or the City Council. To obtain the necessary authorization, a written request from the requestor's Department Director to the City Manager or City Council must include subject employee information (i.e. name, employee number), a specific description of request (e.g. Email, share drives, web usage etc.) and name and phone number of the employee in the requesting department who is responsible for coordination of the request.

Sec. 36.14. Electronic Signatures and Electronic Records.

Electronic signatures, an automated function that replaces a handwritten signature with a system generated signature statement, and electronic records can be utilized as a means for authentication of City documents, computer generated City documents and/or electronic City entries among other uses. System generated electronic signatures are considered legally binding as a means to identify the author of record for entries and confirm that the contents of what the author intended. City departments and staff will be allowed to utilize electronic signature in accordance with this directive, City, State, and/or Federal regulations regarding such. As such, acceptable Use of Electronic Records and Electronic Signatures are allowed:

(a) Where policies, laws, regulations, and rules require a signature and that requirement is met if the document contains an electronic signature;
(b) Where policies, laws, regulations, and/or rules require a written document, and that requirement is met if the document is an electronic record;
(c) Each party to a transaction must agree to conduct the transaction electronically in order for the electronic transaction to be valid and binding. Consent may be implied from the circumstances, except with respect to any electronic records used to deliver information for which consumers are otherwise entitled by law to receive in paper or hardcopy form;
(d) If a law prohibits a transaction from occurring electronically, the transaction must occur in the manner specified by law;
(e) If a law requires an electronic signature to contain specific elements, the electronic signature must contain the elements specified by law;
(f) If a law requires that a record be retained, that requirement is satisfied by retaining an electronic record of the information in a record that accurately reflects the information set forth in the original record and shall remain accessible for later reference. When the requirements for retention require an original form, retention by an "electronic form" shall provide and satisfy the retention requirement.

Procedures, Forms, Guidelines and Resources for electronic signatures:

(a) Procedures for electronic signatures can be found under the Texas Uniform Electronic Transactions Act;
(b) United States governance can be found in 18 USC 2510, Electronic Communications Privacy Act;

(c) Record management for the City is established by Local Government Code: 201 through 205. The Texas State legislature requires local governments to establish a records program by Ordinance;
(d) The charter of the City of Floresville mandates that the City Secretary shall keep the records of the Council and of the City

SUBCHAPTER III. SECURITY REQUIREMENTS OF TECHNOLOGY SYSTEM

Sec. 36.20. Confidentiality of Information on Technological Devices.
Information stored on any City-administered information technology system should be classified in accordance with federal, state and local statues, ordinances, regulations, and/or policies among other directives regarding the confidentiality of the information. Users shall take the necessary steps or follow the prescribed processes to prevent unauthorized access to confidential information. Unclassified information should not be released to non-City entities without authorization and approval by the City Manager's Office. Users must comply with all City Directives regarding use of information technology, including:

(a) Electronic Communications (e-mail, voice and Internet);
(b) Password Management;
(c) Security;
(d) Data Management and Classification;
(e) Monitoring;
(f) Remote Access

Sec. 36.21. Protection from Unauthorized Access.
(a) All personal computers, laptops, and workstations should be protected from unauthorized access when the system is unattended. The recommended method of security for City devices is with a password-protected screensaver (with the automatic activation feature set to 15 minutes or less) or by manually locking the device (Ctrl-Alt-Delete for most Microsoft Operating Systems). Devices that cannot be locked as described above should be secured by logging off the devices or turning them off.

(b) For all other technological devices, users must take reasonable and necessary precautions to secure and protect such devices; this includes requiring a password for access to mobile phones and tablets.

(c) ITSD regularly maintains operating systems, updates security software, and applies security patches by sending those updates during non-business hours to computers attached to the network. When a user leaves for the day, he/she should log off from his/her computer, but should leave the computer turned on and attached to the network. If laptops are secured during non-business hours and are not connected to the network, it is possible that updates were sent; as such users should work with their business owner to ensure updates to portable devices are installed in a timely manner.

(d) All technology devices used by a technology user to connect to the City's networks shall continually execute approved security software with a current virus definition file. This includes user-owned equipment attached to the City's networks through remote access technologies. The City is not responsible for providing the required security software for user-owned computers.

(e) E-mail attachments that may constitute a risk to the City's technology environment will be removed from e-mail messages passing through the City's mail servers if possible. Removed attachments are replaced by a message indicating that they have been removed and the header and text of the original message delivered normally.

(f) A spam message filter is used to reduce the transmission of chain letters, broadcast announcements, general advertisement postings, or any other message via e-mail to a group of persons not requesting the message.

Sec. 36.22. Passwords.

Passwords are an important element of the acceptable use of technology and associated information security. A poorly chosen password may result in the compromise of the City's network. All technology users are responsible for taking appropriate steps to select and secure passwords. Users shall take reasonable and necessary care to prevent unauthorized access to workstations, laptops, applications, mobile and/or other devices. No departmental personnel, including administrative staff, shall request access to or maintain lists of other user passwords.

Password Guidelines:

(a) Use of "strong" passwords. Strong passwords that are at least eight characters in length, are not based on words in any language, slang, dialect or jargon, are not based on personal information such as family names, use at least one (1) each English uppercase (A through Z), lowercase (a through z), digit (0 to 9) and non-alphanumeric character (!,$,#,%), are not common usage words like family, pets, friends, "Floresville", birthdays, phone numbers, addresses, computer terms, fantasy characters and/or common patterns like aaabbb, qwerty, zyxwvuts, 123321 or any derivation followed by a digit.

(b) If ITSD deems required, all users' passwords will expire at intervals of ninety (90) days. In the event that this occurs, ITSD will institute a policy where users will be prompted to change passwords beginning 10 days before the next expiration date. Passwords may not be re-used;

(c) Passwords will be changed immediately after a security breach has been detected to the affected City systems;

(d) As the City system software permits, an initial or reset password issued to a user will be valid only for the user's next log in. After that, the user must be prompted to change their password;

Password Protection Guidelines:

(a) Do not write passwords down, store them on-line, or reveal them in any electronic format;
(b) Do not use the same password for City accounts as for other accounts (i.e. social media, personal email account, banking sites, etc);
(c) Passwords must be treated as sensitive and confidential information thus do not share City passwords with anyone;
(d) ITSD support personnel may require a user's password to resolve a problem however, the user be present to enter the required password;
(e) Do not talk about a password in the presence of others;
(f) Do not hint at the format of a password ("my family name");
(g) Do not click on links in emails from unknown sources and provide account information that includes personal information and/or password;
(h) Do not reveal a password on questionnaires or security forms;
(i) Do not use the "remember password" feature;
(j) Do not store passwords in a file on ANY computer system without encryption.

Sec. 36.23. Reporting Security Breaches.
Technology users shall report any suspected security violations or threat to the City Manager and/or ITSD immediately. Any activity performed under a user-id/password combination is presumed to have been performed by that user and is the responsibility of that technology user.

SUBCHAPTER IV. RECORDS RETENTION OF TECHNOLOGY SYSTEM

Sec. 36.30. Records Retention of Electronic Records.
The City's approved Declaration of Compliance with the Local Government Records Retention Schedules establishes record series and the retention period for each series. It is the content and function of an e-mail, text message, or any other electronic communication that determines the retention period for that message. All e-mail, text messages, or other electronic communication sent or received by a government is considered a government record. Therefore, all e-mails, text messages, and other electronic communications must be retained and disposed of according to the City's retention requirements. E-mail systems must meet the retention requirement found in chapter 7, section 7.77 of the Texas Administrative Code.

Users and their supervisors or sponsor should seek guidance from the City Manager if there is a question concerning whether an electronic message should be deleted.

SUBCHAPTER V. PENALTIES

Sec. **36.40. Penalties.**
Compliance with City administrative directives, security policies, and/or procedures is the responsibility of all City employees, contractors and/or other third parties. The City

can temporarily or permanently suspend, block, and/or restrict access to information or physical assets, independent of such procedures, when it is reasonable and associated probable cause exists to do so in order to protect the confidentiality, integrity or availability of City resources as well as protect the City from liability, and/or to comply with applicable federal, state, and municipal laws, regulations, statutes, court orders, or other contractual obligations. Violations of any of portions of this Policy shall result in disciplinary actions in a manner as determined by the City Manager. Disciplinary action may range from reprimand and loss of access privileges to suspension to separation of employment. Violations may also result in civil and/or criminal prosecution.

This Ordinance shall have an Effective Date of February 9, 2017 and have an enforcement date of all criminal and civil penalties upon publication in the Wilson County News.

Upon motion of _____, seconded by _____, with the following ____ voting in the affirmative, _____ voting in the negative, _____ absent, and _____ abstaining, the above Ordinance is duly **PASSED and APPROVED** this ____ day of _____, 2017.

_____
CECELIA GONZALEZ-DIPPEL
Mayor

Attest:

_____
MONICA CORDOVA
City Secretary