City of Kings Mountain

Administrative Policy:
Information Technology Policies

Section:	Administrative	
Prepared By:	Information Technology Department	
Approved By:	Kings Mountain City Council	
Effective Date:	1-25-2011	Page: 1 of 9
Revision:	#5 (Revised 8-1-2017)	

TABLE OF CONTENTS

1.0 Purpose

The City's computers and internet are powerful business tools. Unfortunately, it can also be both a distraction from productive work as well as a threat to the security of our network. In an effort to clarify our position on the use of these items, we have developed the following policy. This policy will be amended and re-distributed in the future as appropriate.

2.0 Scope

This policy applies to all employees, temporaries, and other users conducting business on City of Kings Mountain grounds, and to all equipment that is owned or leased by the City of Kings Mountain. This policy targets network related equipment and may not apply to special projects where computer equipment is specific to other systems that are not part of the city network.

Departments may add additional restrictions to this policy, but may not remove or delete any provisions. This policy serves to protect the users and network of the City of Kings Mountain; removing any part of this policy may place users or the network at risk of compromise.

3.0 General Technology Policy

3.1 Use and Ownership

While the City of Kings Mountain does not desire to be intrusive in its monitoring of networks, users should be aware that the data they create on the City's systems remains the property of the City of Kings Mountain. Because of the need to protect the City's network, management does not guarantee confidentiality of user data stored on any network device belonging to the City of Kings Mountain.

Internet/Intranet related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP, are the property of the City. These systems are to be used for business purposes in serving the interest of the city.

No one may relocate any computer equipment without prior approval from the IT Department.

For security and network maintenance purposes, authorized City personnel may monitor equipment, systems, and network traffic at any time. The City reserves the right, and intends to audit networks and systems on periodic basis to ensure compliance with this policy. Individuals authorized to audit systems include the City Manager, HR Manager, and IT staff.

All software request, hardware request, and purchases of computers and network equipment will be processed through the IT Department. All hardware and software will be shipped to the IT Department where it will be inventoried. The hardware will be configured by the IT Department prior to delivery to the department for final setup.

3.2 Security

Effective security is a team effort involving the participation and support of every City employee and affiliate. It is the responsibility of technology users to know these guidelines and to conduct their activities accordingly.

You are responsible for both your computer and your login. Your network password is private information and is not to be shared with other employees. You are ultimately responsible for what happens at your computer or with your login. Employees using City accounts are acting as representatives of The City of Kings Mountain. Employees should act accordingly to avoid damaging the reputation of the city. Anyone other than the IT Department staff must obtain permission from the computer owner before using that person's computer or login. Department directors are allowed to access others computers, but only those within their department. If a situation is unavoidable where you have to share your login or computer you must change

your password afterward in order to remove future access by that person. Contact the IT Department if you need assistance in doing so.

No unauthorized external access. Access to The City of Kings Mountain's programs, software, and information from outside the company premises is only allowed with permission and strict pre-requisites. Tools such as "PCAnywhere", "GoToMyPC", and "LogMeIn" are strictly prohibited from being used to connect remotely unless authorized by the IT Department. Approval to connect must first be approved by both your supervisor and the IT Department. The computer used to gain access must be either provided by The City of Kings Mountain and/or meet security standards before attempting to connect. Security standards include, but are not limited to, installation of critical Windows Updates and a current antivirus program installed with the most up-to-date definitions.

Connecting equipment to the City network is restricted. Personal equipment such as computers, laptops, mp3 players, and cameras are strictly prohibited from being connected to the network as these items can bypass security measures and easily introduce viruses to the City network.

No user may download or in any way install software or hardware that has not first been authorized by the IT Department. Software includes, but is not limited to desktop themes, music downloads, screensavers, messenger services, or anything else that was not originally shipped with your operating system. Personal photographs may be used as wallpaper on your desktop; however, they must be acceptable for viewing by the general public.

At the end of the day, you are responsible for closing all applications on your computer, and turning off the monitor. This is for both security and power conservation. You do not have to shutdown your computer every day, but it is recommended that you shut it down if you will be out of the office for several days or as a preventative step if lightning storms are likely.

3.3 Unacceptable Use

Under no circumstance may an employee engage in any activity that is illegal under local, state, federal or international law while using City of Kings Mountain owned or leased resources.

The installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City of Kings Mountain is not allowed.

Any activities with the intention to create and/or distribute malicious programs into the City's network (e.g., viruses, worms, trojans, etc.) are prohibited.

4.0 System Resource Policy

The system resources policy addresses access to system resources such as email, internet, and servers.

4.1 Email and Communications

Business communications can occur in many formats. Email, among other formats, can be a public record based on content and may be subject to public disclosure in accordance with the Public Records law, as cited in North Carolina General Statues 132. Every employee is individually responsible for the public records they generate or receive and for retaining those records in accordance to this law, regardless of the technology used to create the records.

Emails that are considered inappropriate, sensitive, offensive, vulgar, or illegal are prohibited and may not be sent from your email account. Individuals shall not use the City's internet or email for personal use or to forward email chain letters; view, download, save, receive or send material related to or including: offensive content of any kind, including pornographic material; promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, political affiliation, or disability; threatening or violent behavior; or illegal activities such as gambling.

Employees must use extreme caution when opening attachments. If an attachment is in question, contact the IT Department to have them evaluate it before opening.

Sending of "Junk Mail" (email spam) is not allowed.

All messages distributed via the City email system are property of the City of Kings Mountain. You have no expectation of privacy in anything that you create, store, send or receive on the City's email system. Your emails can be monitored without prior notification whenever the City deems this appropriate. Individuals authorized to monitor email include the City Manager, HR Manager, and IT staff.

Accessing personal web mail such as AOL, Hotmail, Google, and Yahoo is prohibited. These email systems are not filtered or scanned by the City and are more vulnerable to viruses which would bypass City security measures that are in place.

Although the City's email system is meant for business use, the City will allow minor personal usage if it is reasonable and does not interfere with work. "Reasonable" will be defined by each department head.

You should not use your city email address to register for anything unless it pertains to city business. This includes but is not limited to social networking sites, store emails and coupons, etc.

4.2 Passwords

Passwords are an important aspect of computer security. A poorly chosen password may result in the compromise of the City's entire corporate network. As such, employees are asked to memorize your password(s) and never write it down or store it online.

The IT Department will dictate how often passwords will change and what level of security passwords must meet.

4.3 Internet Access

Internet access is primarily for official business. Employees are authorized to access the Internet for a reasonable amount of personal use during non-business time, in strict compliance with the other terms of this policy. Non-business time and "Reasonable" will be defined by each department head.

Websites that are considered inappropriate, sensitive, offensive, vulgar, or illegal such as sites containing pornography, gambling, or racism are prohibited.

The City of Kings Mountain expects its employees to present a favorable and professional image of the City to the entire Internet community and to adhere to customary Internet ethics.

Employees may not use City resources for accessing or attempting to access information, programs, services or sites to which you do not have specific authorization.

Streaming of internet video and/or audio (such as internet radio) is not allowed. Streaming places a huge strain on internet bandwidth and can negatively affect other network systems.

Using the Internet to make personal phone or video calls via services such as Skype is prohibited.

4.4 Cell Phones/Mobile Devices Usage Policy

This policy applies to City issued and personal cell phone/mobile device usage. The mobile device is primarily a business tool and its use must comply with all requirements of the policy as outlined below as well as any additional policies and procedures.

Under NO circumstances should a cell phone/mobile device be used while operating equipment, or in hazardous environments.

Use of any devices while on the job is prohibited except for emergency situations and with the approval of Supervisor/Manager.

As a rule, employees should not use mobile devices while driving. For those employees needing to use cellular/mobile devices while driving, the use of a hands-free device is recommended.

Taking and storing inappropriate photographs/images is prohibited pursuant to the City's use of Internet and E-mail policy. Usages of these devices are subject to and must comply with all sections of the City's Information Technology Policies. The city is not responsible for the retention of personal photos taken on city cell phones.

It is the department director's decision on when devices are to be upgraded.

Employees are expected to abide by all applicable laws covering the use of mobile devices while driving. **The City will not be held liable in part or portion for any fees, fines or judgments imposed by law enforcement or the courts for violations of this nature or accidents deemed to be caused by the use of a cellular/mobile device.**

4.4.1 City Issued Cell Phones/Mobile Devices

Mobile devices will be provided for eligible employees based on business needs as a productivity tool.

Texting from or to a City issued device is also public record and may be subject to public disclosure in accordance with the Public Records law. For that reason, text messaging on city provided phones will be archived. All text messages distributed via a City issued cell phone are property of the City of Kings Mountain. You have no expectation of privacy and your text messages can be monitored without prior notification whenever the City deems this appropriate. Individuals authorized to monitor text messaging include the City Manager, HR Manager, and IT staff.

Smartphone devices will only be approved for those eligible employees who have the need to frequently be away from their offices in remote working locations and require prompt or immediate availability/access and have a business need for data services. These devices will provide you with the capability of utilizing standard email, contacts, and calendar services. In addition, Smartphone devices can be monitored remotely to provide additional security and to ensure that the proper Security Policies are in place. Since these devices are City owned, they are subject to inspection by the IT Director, the Human Resources Director or the City Manager.

- Positions qualifying for Smartphones are (but may not be limited to):
  Directors/Management/IT – Other positions must have approval of Department Director and City Manager

Standard cell phones will be provided for eligible employees who have the need to frequently be away from their offices in remote working locations and require prompt or immediate availability/access but do not require data services in the normal function of their job responsibilities.

- Positions qualifying for Standard cell phones are (but may not be limited to):
  Supervisors/Crew Leaders - Other positions must have approval of Department Director

Discretion should be used when choosing or adding apps to City provided cell phones as these can track and remotely access information that may be detrimental to the employee or the City and/or may be prone to viruses negatively affecting the device. When in doubt as to the integrity of these apps contact our IT Director.

It is required that all City Smartphone devices be password, PIN, or Pattern protected. This password should be kept private for your own use and safety and not distributed to others.

It is the City's policy that the wireless numbers associated to all City issued smartphone and cell phone devices are City owned. There will be no approval granted to an employee to seize their wireless number upon separation from the City. If an employee that transferred his/her personal number to the City separates from the City and wishes to transfer their number back to a personal device, approval will not be granted.

Each mobile device will be issued with a wall charger and a case. Should an employee wish to purchase any additional accessories (vehicle chargers, other cases, etc.), they can do so at the employee's own expense.

If a City issued device is damaged, lost or stolen, the employee is responsible for contacting both their Department Director and the IT Department immediately.

Loss, accidental damage, or neglect to cell phones and/or accessories must be reported to the department director and can result in the employee being written up by the director. The employee may also be held financially responsible for replacement cost due to damage. The director will then notify IT staff on how to proceed with the replacement.

Although these devices are provided as tools for the job and the expenses are borne by the City, employees are allowed to use City provided cell phone/mobile devices for reasonable personal use. Should this usage be perceived as being excessive, the employee may be held responsible for some portions of their monthly mobile expense. General rate plans are selected by and absorbed by the City.

4.4.2 Personal Cell Phone/Mobile Devices

Certain security measures are in place on City issued devices which cannot be enforced on personal devices. **Access to City email accounts is only to be setup on city issued phones, and not on personal devices without the approval of the Director and the City Manager.**

Use of personal cell phones for employees not qualifying for City provided cell/mobile devices should be limited to break and personal times. Use of personal devices while on the job is prohibited except for emergency situations and with the approval of Supervisor/Manager.

5.0 Data Policy

No removal or sharing of company information or files. Employees shall not remove data or files from the premises without approval from the department director, City Manager or IT Department. This includes, but is not limited to, print outs, reports, emails, floppy disks, CD-ROM, USB flash drive, or uploading to cloud storage. Employees shall not place company material (copyrighted software, internal correspondence, etc.) on any publicly accessible Internet computer without proper permission.

5.1 Data Storage

All laptops should have the hard drives encrypted to prevent theft of data in the event the laptop is lost or stolen.

When a device has reached its "End of Life" and is replaced or pulled from service, that device must have the hard drive removed and destroyed or "scrubbed" to remove any data from it. Devices include, but are not limited to, desktop computers, laptops, mobile devices, fax machines, and copiers.

6.0 Directors Responsibilities

Technology has become an integral part of every department in some way. Each department director is asked to assist with the monitoring and enforcement of this policy.

6.1 Personnel Changes

Department directors are responsible for notifying the IT Department in a timely manner of changes in personnel.

If a new person is hired, the director should notify the IT Department well before that persons start date to allow time for the account creation and configuration. This also applies to when personnel transfer to a different position or department.

If an employee quits or is terminated, the department director should notify the IT Department immediately so that the account may be disabled. Failing to disable an account immediately for someone no longer employed by the City is a huge security issue.

7.0 Social Networking

As social networking sites like but not limited to Facebook, and Twitter become intertwined with government uses, The City has developed this Social Networking Policy.

The absence of, or lack of explicit reference to a specific site does not limit the extent of the application of this policy. Where no policy or guidelines exist, employees should use their professional judgment and take the most sensible action possible.

7.1 City or Department Social Networking Sites

If the City, or a Department of the City, has a Social Networking Site it must be consistent with applicable state, federal, and local laws, regulations, and policies. This includes any applicable Records Retention and Disposition Schedules or policies, procedures, standards, or guidelines provided by the Department of Cultural Resources.

Like e-mail, communication via agency-related social networking web sites is a public record. This means that both the posts of the site administrator and any feedback by other employees or non-employees, including citizens, will become part of the public record. Because others might not be aware of the public records law, agencies should include the following statement (or some version of it) somewhere on the social networking Web site: "Representatives of The City of Kings Mountain government communicate via this Web site. Consequently any communication via this site (whether by a City employee or the general public) may be subject to monitoring and disclosure to third parties."

The IT Department is to keep a record of all Social Network accounts and have a list of approved users and the passwords for each account upon creation. If you create a City or Department account, it is your responsibility to provide this information to the IT Department. These records are only to be used by the IT Department for emergency issues such as a hijacked or corrupt site, not for regular maintenance.

7.2 Personal Social Networking Sites

Employees should be mindful of blurring their personal and professional lives when administering social media sites. Employees are allowed to have personal social networking sites. These sites must remain personal in nature and be used to share personal opinions or non-work related information. This helps ensure a distinction between sharing personal and agency views. In addition, employees should never use their City e-mail account or password in conjunction with a personal social networking site. Employees may use personal social networking for personal communications so long as those communications do not interfere with their work and are kept to a reasonable amount of use. "Reasonable" will be defined by each department head.

8.0 Public Records and Retention

8.1 Definition

A public record is defined by the North Carolina General Statues in chapter 132

§ 132-1. "Public records" defined.

(a) "Public record" or "public records" shall mean all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions. Agency of North Carolina government or its subdivisions shall mean and include every public office, public officer or official (State or local, elected or appointed), institution, board, commission, bureau, council, department, authority or other unit of government of the State or of any county, unit, special district or other political subdivision of government.

(b) The public records and public information compiled by the agencies of North Carolina government or its subdivisions are the property of the people. Therefore, it is the policy of this State that the people may obtain copies of their public records and public information free or at minimal cost unless otherwise specifically provided by law. As used herein, "minimal cost" shall mean the actual cost of reproducing the public record or public information.

8.2 Retention/Archiving

Public Records are archived to meet retention laws stated in North Carolina General Statues in Chapter 121-5. Below is a section from 121-5 that discusses specifically the destruction of records.

§ 121-5 (b). Public records and archives.

(b) Destruction of Records Regulated. – No person may destroy, sell, loan, or otherwise dispose of any public record without the consent of the Department of Natural and Cultural Resources, except as provided in G.S. 130A-99. Whoever unlawfully removes a public record from the office where it is usually kept, or alters, mutilates, or destroys it shall be guilty of a Class 3 misdemeanor and upon conviction only fined at the discretion of the court.

8.3 Conducting City Business

To be compliant with Public Records and Retention laws, the City has measures in place to archive primary City communication methods (which currently include email, social media, and text messaging). It is near impossible for The City to archive all possible means of communications and therefore states that employees are not to conduct City business using personal devices. This includes, but is not limited to, personal computers, personal email accounts, personal cell phones, personal text messaging, personal social media accounts, or other personal applications.

9.0 Policy Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

When a violation is found, please report it to the appropriate department director first, then to the Human Resources Department, or the IT Department.

In order to keep current with technology, this policy may be revised as the City feels necessary, and every attempt to post changes will be taken. If something is not specifically stated in the policy, it does not necessarily mean that it is allowed. If something is ever in question, please speak with your department director, the Human Resources Department, or the IT Department.

Appendix A – Definitions

Cloud Storage – storing digital information on hosted equipment by a third party, outside of the city network.

Flash drive - is a mass storage device. Flash drives are often used for the same purposes as floppy disks were.

FTP - short for File Transfer Protocol is a standard network protocol used to copy a file from one host to another over a network, such as the Internet.

Internet - is a global system of interconnected computer networks that use the standard Internet Protocol to serve billions of users worldwide

Intranet - is a private computer network that securely shares any part of an organization's information or operational systems within that organization.

IT Department - short for Information Technology Department and can mean either direct employees of the city or contracted staff assuming this role.

Junk mail - also known as SPAM, unsolicited bulk Email (UBE), or unsolicited commercial email (UCE), is the practice of sending unwanted e-mail messages to an indiscriminate set of recipients.

Retention and disposition schedule – a document that identifies and describes an organization's records, usually at the series level, provides instructions for the disposition of records throughout their life cycle. (SAA Glossary)

Skype - is a software application that allows users to make video voice calls over the Internet.

Social networking - the use of a variety of Web sites that allow users to share content, interact, and develop communities around similar interests. (Examples are: Facebook, MySpace, and Twitter)

Smartphone – A mobile phone offering advanced capabilities beyond a standard cell phone, often PC-like functionality. These phones require a data package.

Standard cell phone – A cell phone with the standard features to allow voice calling.

Streaming - multimedia that are constantly received by an end-user while being delivered by a streaming provider. (Examples: Listening to Online Radio Stations or watching a movie over the internet)

Post - comment made to a user's social networking page or site.

Appendix B

City of Kings Mountain

Information Technology Policies User Agreement

Highlighted Points of the Information Technology Policy

- E-mail, Internet, and City issued Mobile Devices, and Computer systems are city property.
- All systems may be reviewed by the City Manager, HR Manager, or IT Department at any time.
- There is no expectation of privacy. Emails, Text Messages and any public record will be archived.
- Do not relocate computer equipment without IT Department approval.
- Employees are responsible for their computer and login.
- No unauthorized external access.
- Personal equipment is strictly prohibited from connecting to the city network.
- No downloading or installing software without IT Department authorization
- No Illegal use, pirated software, or malicious programs.
- Accessing personal web mail such as AOL, Hotmail, Google mail, and Yahoo mail is prohibited.
- Sending junk email is not allowed.
- Do not use your city email address to register for anything unless it pertains to city business.
- Viewing inappropriate websites is prohibited.
- Streaming of internet audio and/or video is not allowed.
- Employees shall not remove data or files from the premises without approval from the department director, City Manager or IT Department.

Notify your department director first, then the Human Resources Department or the IT Department of any violations of this policy.

In order to keep current with technology, this policy may be revised as management feels necessary, and every attempt to post changes will be taken. If something is not specifically stated in the policy, it does not necessarily mean that it is allowed. If something is ever in question, please speak with your director first, then with the Human Resources Department, or the IT Department.

I have read and received the City of Kings Mountain Information Technology Policies and agree to abide by it and to be subject to its provisions. I understand that violation of any of these policies may result in disciplinary action and potential termination of employment. Please sign below and return to the Human Resources Department.

Printed Name of Employee: _____

Department: _____

Signature of Employee: _____

Date Signed: _____