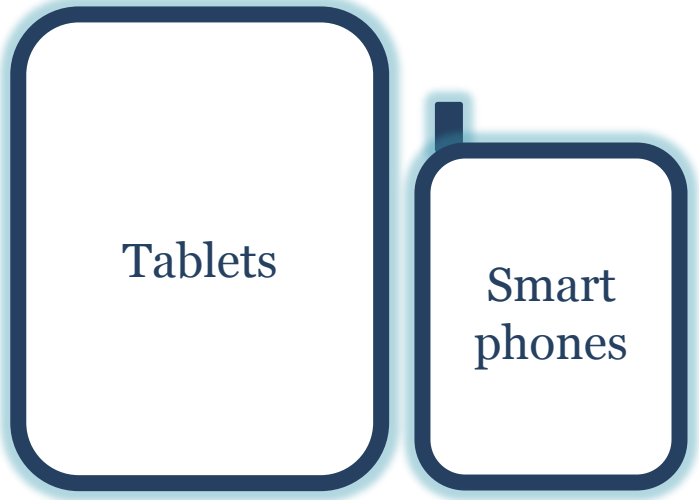
Personal Mobile Device Synchronization and Use Training

What are Personal Mobile Devices?

Primarily smart phones, but also include:

- Portable media devices.
- Tablet computers.
- e-Readers.
- Ultra-mobile/netbook computers.
- Portable gaming devices.



Any personally-owned device capable of storing corporate data and/or connecting to City of Lee's Summit's network is bound by the acceptable use policy.

Purpose

- Allowing you to bring your own devices to work is beneficial to you and the City of Lee's Summit by allowing you to be accessible and productive on a device you are already familiar with.

- However, outside technology brings potential risks to the integrity of private information and business data that is made available when connected with the City's technology.

- This acceptable use policy is necessary to mitigate the risk.

- By attaching a personal device to the City's network, you agree to comply with the policy explained here, and grant the City of Lee's Summit permission to erase the information on your device if necessary.

Case Study: James at World's of Fun

Incident

- James is at Worlds of Fun with his family when he receives a sensitive e-mail from a colleague on his personal iPhone, which is connected to the company network.
- Responding to the e-mail quickly, James continues with his day at the park.
- In the evening, James realizes he forgot his iPhone on a table in the food court at the park.

Action

- Upon realizing he has lost his phone, James immediately calls his manager and the ITS Help Desk.
- ITS is able to remotely wipe the Exchange data immediately, mitigating the risk of data leakage and the effect it may have on the company.

Effect on City and Employee

- James' quick action ensures that no sensitive data (personal or City) was retrieved from the phone by an unintended party.
- The net liability is $0 outside of the cost to set up the initial infrastructure.
- James buys a new iPhone and loads a backup image of his previous device onto it, minimizing the time required to return to productivity.

Quick action by employees that have lost devices is the most effective way to mitigate security threats from personal mobile devices. The faster we recover or wipe the data, the better.

Responsibilities

- You, as an employee of the City, are responsible for acting in accordance with the City's policies and procedures.
- Connections between mobile devices and the City's network *will* be managed by the City's ITS department.
- The ITS department *will not* directly manage the functionality or performance of devices except in their capacity to connect to the corporate network.
- Users are expected to adhere to the same security standards no matter where the device is used.

Policies: Access

Mobile devices must be used appropriately, responsibly, and ethically. In most circumstances, these goals can be reached by following the policies laid out here.

Mobile devices must be approved by ITS before being connected to the City's network.

If necessary, devices must be modified or set up to meet City's security standards.

Policies: Security
Do

Set up device to auto lock.
Use a strong password or unique pin.

Use reasonable physical security measures.
Do not leave your device unattended or unlocked.

Use anti-virus / anti-malware software.
Data corruption via a virus or malware can be passed to the City's network. If a mobile device connects to a computer, have anti-virus on the computer.

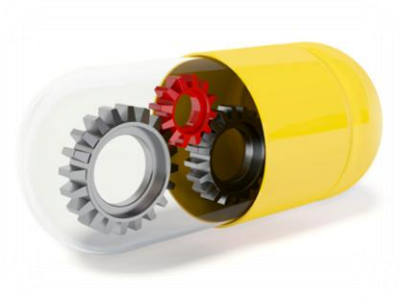
Backup your device.
Your are responsible for being able to restore your device if wiped, lost, damaged or stolen.

Policies: Security
Do Not

Do not store unencrypted confidential information.
For example, by e-mailing a password or storing it in a text file.

Do not try to bypass security measures from IT.
Leave additional software in place.

Do not leave company data on your device indefinitely.
If you stop using the device or end your employment, erase City data.



Incidents

Incidents involving devices that contain City data – such as a lost or stolen device, or suspicion of unauthorized access – must be reported within one business day to your manager and the ITS department.

Policies: Support

City will provide limited support for employee-owned devices.

Supported: verification that mobile access is available.
Not supported: phone won't turn on, screen is cracked, no service, personal applications, recovery from a backup, etc.

IT may limit access.

Your ability to transfer data to and from specific resources on the City's network may be reduced at any time.

Support Priority.

Personal Device support, within these parameters, is a non-critical, low priority issue and will be provided during normal business hours only.

Policies: Organizational Protocol

City will not reimburse the cost of devices or accessories.

City may reimburse the cost of services.

If authorized based upon your job duties, the City may provide a stipend to cover a portion of your personal device expense (see the City's Provision and Use of Portable Communication Devices Policy.)

Non-exempt employees.

Supervisors and their non-exempt employees should discuss the usage of remote data access during off-duty hours.

Devices with Blackberry OS

All devices with a Blackberry OS (City-owned or personally owned) will be synchronized with the City's network via the Blackberry Enterprise Server

The BES allows Blackberry OS users to have a secure and encrypted connection to the City's network. Additional encryption software for the device may not be necessary.

However, in the event of a loss or theft, users of a Blackberry OS device (including personally owned) will likely have all of their data wiped from the device as a security precaution.

Devices with an Alternate OS (incl. iOS, Android, Palm, etc.)

Users whose devices do not have a Blackberry OS will synchronize wirelessly with the City's network through Windows ActiveSync.

A separate account will be created on the device for the work information.

In the event of a loss of theft of the device, all of the city's data will be remotely wiped from the device. While every precaution will be taken, it is possible that all data on the device (including personal contacts, pictures, text messages, etc) will be lost when this remote wipe is performed.

Policies: Privacy

Information stored on a privately owned device that synchronizes with the City's email system is inherently less private.

Information sent/received using the City email & network is neither confidential nor private.

Any email sent and/or received using the City's email system are considered property of the City regardless of content.

Policies: Discoverability

Devices that are synchronized with the City's email system are subject to the discovery process for litigation purposes.

Any additional electronic item and/or service the device has been synchronized with is also subject to discovery.

Example:

James has purchased his new iPhone (after losing the old one at Worlds of Fun). Once he has loaded his backup image, he proceeds to use his phone as he always has: he checks email from his work account, checks email from his home account, updates his wall on Facebook, tweets about his weekend on Twitter, etc.

If the City ever enters into litigation that would involve James or his department, not only would his City email account be discoverable, but also his home email account, his Facebook, Twitter, and other social networking accounts, and his home PC if he docks his iPhone to it.

Alternative to Synchronization

The city does provide a free alternative to the synchronization process.

Any device with a web browser can access the City's webmail access portal at:
https://webmail.cityofls.net

Portal:

Users have access to most of the same functions as their desktop copy of Outlook:

•Email is accessible. Users can read, write, send, and/or receive email

• Calendar is available to view, create, modify, and cancel appointments and meetings

•Tasks are available, as well.

Policy Enforcement Technology

Device Wipe

By connecting to City's network and taking the necessary security measure, you agree to grant ITS the ability to erase all data on the device, if it is necessary* to preserve the City's data security and integrity.

** ITS will attempt to contact you before erasing the device to verify it is lost/stolen.*

Encryption

Confidential Data on the device should be encrypted. Contact your service provider to learn of encryption utilities that are available for your device.

Third Party Software

Certain devices may require obtaining and installing 3rd party software to ensure compliance with security policy.

Consequences of Non-Compliance

- The Chief Technology Office and Department Director will be advised of breaches in the policy and be responsible for remedial action.

- Failing to comply with these policies and procedures may result in one or more of the following:

Suspension of technology use at the City.

Loss of connection privileges.

Disciplinary action.

Termination of employment.

Questions?

- Review Personnel Policy #406 pertaining to the Provision and Use of a Portable Communication Device.

- A copy of the *Mobile Device Support Agreement* with all required signatures must be submitted to ITS before access to the City's network from a mobile device will be granted.

- All related Policies and documents are available for future reference at www.lsits.net.

- Questions or comments about the policy should be directed to the ITS Help Desk.