City of New Hope, Minnesota

Non-City Owned Mobile Device Acceptable Use Policy

Policy

The purpose of this policy is to define standards, procedures and restrictions for employees who have a legitimate business reason for connecting a non-city owned mobile device to the City of New Hope network. This mobile device acceptable use policy applies, but is not limited, to all devices and accompanying media that fit the following classifications:

- Smartphones
- Other mobile/cellular phones
- Tablets
- Portable media devices
- Laptop/notebook computers
- Any mobile device capable of storing data and connecting to a network

This acceptable use policy applies to any hardware and related software that is not owned by the City of New Hope, but could be used to access City of New Hope resources.
The goal of the acceptable use policy is to protect the integrity of the confidential client and business data and private personal data that resides within the City of New Hope technology infrastructure. This acceptable use policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device. Therefore, all users employing a non-city owned mobile device connected to the City of New Hope's network, and or capable of backing up, storing, or otherwise accessing city data of any type, must adhere to City-defined processes for doing so.

Guidelines & Procedures

A. Access Control

The City of New Hope provides the capability to send and receive email from non-city owned mobile devices. Any non-city owned mobile device configured to access City of New Hope email must have a password to access/unlock the device. The unlock password must have a minimum of 6 nonrepeating alphanumeric characters. No pattern unlock programs are allowed. The unlock password must not be shared with any other person. The City of New Hope will electronically enforce security policies on devices connected to the email server.

B. Remote Wipe

Lost, stolen or replaced non-city owned mobile devices that have had access to the City of New Hope network must be reported immediately to IT. Lost stolen or replaced non-city owned mobile devices will be subject to remote wipes. When a remote wipe is initiated, **all** data will be removed from the device and the device will be reset back to the factory default settings. A remote wipe may remove personal data from the device and information not saved at another location may be permanently lost. The City of New Hope is not responsible for any lost personal data. The city of New Hope may also initiate a remote wipe if the employee leaves employment with the city or any other reason the city deems necessary to protect the integrity of the City's network and data.

C. Support

The City of New Hope will provide limited, best effort support for non-city owned mobile devices. IT support of non-city owned mobile devices will be limited to instructions for the employee on how to sync email. The City assumes no liability for any direct or indirect damages arising from the user's use of a non-city owned mobile device. The City of New Hope assumes no responsibility and/or liability for the exposure of the non-city owned mobile device personal data to public information data practice requests, and or legal searches.

D. Agreement

All employees who configure their non-city owned mobile device to connect to the City's network agree to the following terms:

1. Abide by the terms of the IT Policy as it relates to city business conducted on the non-city owned mobile device.
2. Give IT permission to make appropriate modification and changes to configuration settings on the non-city owned mobile device as required.
3. Contact IT immediately if:
   a. Non-city owned mobile device is lost or stolen or user suspects a security breach or
   b. User terminates the use of the non-city owned mobile device
4. Allow IT to completely wipe the non-city owned mobile device with remote wipe capability in the event of a suspected security breach, the device is lost or stolen or use of the mobile device is terminated. Wiping the non-city owned mobile device will result in the loss of all personal data including contacts, photos, music files and other data. User retains the responsibility to back up all personal data.
5. Surrender the non-city owned mobile device to IT in the event a security breach or privacy breach occurs or is suspected. If requested, user will grant IT access to user's usage records.
6. Sync user's mobile device to IT Systems only via approved wireless access software.
7. Remain personally responsible for the mobile number, contract and all carrier or service provider agreements associated with the non-city owned mobile device.
8. Direct support related inquiries, except for issues with installation and connection to IT systems, to user's service provider.

E. Routine Audits

IT staff will routinely audit sync connections (links) made between mobile devices and the City's network/Microsoft accounts. Links that are found to be excessively stale for security purposes will be removed and be the responsibility of the employee to reestablish. Assistance may be requested of IT if needed.

Policy Maintenance

Approved by *Director of HR/Administration* on 12/15/2023
Review cycle: *Every three (3) years* – Next due *12/15/2026*