

		Bring Your Own Device Policy			
Owner:	IT Director	Approving Position:	Common Council	Pages:	3
Issue Date:		Revision Date:		Review Date:	
Special Instructions:					

I. PURPOSE

This policy establishes that the City of Whitewater recognizes guidelines for employee use of personally owned electronic devices for work-related purposes.

II. GUIDELINES

Employees of the City of Whitewater may have the opportunity to use their personal electronic devices for work purposes when authorized in writing, in advance, by the employee and management. Personal electronic devices include personally owned cellphones, smartphones, tablets, laptops, and computers. The use of personal devices is limited to certain employees and may be limited based on compatibility of technology. Contact the Human Resources or IT departments for more details.

III. PROCEDURE

A. To ensure the security of the City of Whitewater’s information, authorized employees may be required to have antivirus and mobile device management (MDM) software installed on their personal mobile devices. Prior to the installation of MDM software or any security applications, employees must provide explicit, written consent regarding the monitoring of their personal devices, the use of MDM software, and the potential for data removal or wiping functions. This MDM software will store all City-related information, including calendars, emails, and other applications, in a password-protected and secure area.

B. Employees may store City-related information only in this area. Employees may not use cloud-based apps or backup that allows City-related data to be transferred to unsecure parties. Due to security issues, personal devices may not be synchronized with other devices in employees’ homes. Making any modifications to the device hardware or software beyond authorized and routine installation updates is prohibited unless approved by IT. Employees may not use unsecure Internet sites except for City-sponsored. Personal devices should be turned off or set to silent or vibrate mode during

Bring Your Own Device Policy

meetings and conferences and in other locations where incoming calls may disrupt normal workflow.

- C. The City of Whitewater's IT department is not responsible for personal items. The IT department may not be used as personal IT technician on personal items. If you are working for the City of Whitewater remotely and use personal devices for working, it is your own responsibility to make sure that device's operating system and drivers are up-to-date, you have an antivirus solution, and is able to function properly while working for the City of Whitewater. The City of Whitewater's IT department is only responsible for only the City owned devices. It is at the discretion of an IT staff member whether they choose to assist with a personal device during their own personal time. Employees using home WiFi must ensure that their router is password-protected.
- D. Employees whose personal devices have camera, video, or recording capability are restricted from using those functions anywhere in the building or on City property at any time unless authorized in advance by management.

While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of City devices. The City of Whitewater's policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information, and ethics apply to employee use of personal devices for work-related activities.

Excessive personal calls, e-mails, instant messages, or text messaging during the workday, regardless of the device used, can interfere with employee productivity and be distracting to others. Employees must handle personal matters on nonwork time and ensure that friends and family members are aware of the policy. Exceptions may be made for emergency situations and as approved in advance by management. Managers reserve the right to request employees' work cellphone bills and use reports for calls and messaging made during working hours to determine if use is excessive.

Employees may not use their personal devices for work purposes during periods of unpaid leave without authorization from management. The City of Whitewater reserves the right to deactivate the City's application and access on the employee's personal device during periods of unpaid leave.

An employee may not store information from or related to former employment on the City's network or devices. Family (including children) and friends should not use personal devices that are used for City purposes. Employees cannot use personal USB drives for City business. Only IT approved USB drives can be used in City business.

- E. No employee using his or her personal device during work hours should expect any privacy except that which is governed by law. The City of Whitewater has the right, at any time, to monitor and preserve any communications that use its networks, including data, voicemail, telephone logs, internet usage, and network traffic, to determine proper use. Management reserves the right to review or retain personal and City-related data on personal devices or to release the data to government agencies or third parties during an investigation or litigation. Management may review the activity and

Bring Your Own Device Policy

analyze use patterns and may choose to publicize these data to ensure that the City of Whitewater's resources in these areas are being used according to this policy. No employee may knowingly disable any network software or systems identified as monitoring tools.

- F. Employees are expected to follow applicable local, state and federal laws and regulations regarding the use of electronic devices at all times.

Employees whose job responsibilities include regular or occasional driving are expected to refrain from using their personal devices while driving. Regardless of the circumstances, including slow or stopped traffic, employees are required to pull off to the side of the road and safely stop the vehicle before placing or accepting a call or texting. Special care should be taken in situations involving traffic, inclement weather or unfamiliar areas.

Employees charged with traffic violations resulting from the use of their personal devices while driving will be solely responsible for any resulting liabilities. Employees who work in hazardous areas must refrain from using personal devices while at work in those areas, as such use can potentially be a major safety hazard.

- G. Employees are expected to protect personal devices used for work-related purposes from loss, damage, or theft.

In an effort to secure sensitive data, employees may be required to have 'remote-wipe' software installed on their personal devices by the IT department before using the devices for work purposes. This software allows the City-related data to be erased remotely in the event the device is lost or stolen. Wiping City data may affect other applications and data.

The City of Whitewater will not be responsible for loss or damage of personal applications or data resulting from the use of City applications or the wiping of City information. Employees must immediately notify management in the event their personal device is lost, stolen or damaged. If IT is unable to repair the device, the employee will be responsible for the cost of replacement.

- H. Upon resignation, termination of employment, or at any time upon request, the employee may be required to produce the personal device for inspection
- I. Employees who have not received authorization in writing from the City of Whitewater's management and who have not provided written consent will not be permitted to use personal devices for work purposes. Failure to follow the City of Whitewater's policies and procedures may result in disciplinary action, up to and including termination of employment.