

Kenosha



County

BOARD OF SUPERVISORS

RESOLUTION NO. _____

Subject: Resolution to Approve the Mobile Device Usage and Agreement Policy			
Original <input type="checkbox"/>	Corrected <input type="checkbox"/>	2nd Correction <input type="checkbox"/>	Resubmitted <input type="checkbox"/>
Date Submitted: February 21, 2018		Date Resubmitted:	
Submitted By: Finance/Administration Committee			
Fiscal Note Attached <input type="checkbox"/>		Legal Note Attached <input type="checkbox"/>	
Prepared By: Shawn Smith Assistant Director of Information Technology		Signature:	

WHEREAS, Kenosha County is committed to implementing policies which protect the County from forces which access and potentially compromise the security of all operations managed by Kenosha County Information Technology Department ("IT"), and

WHEREAS, personal and county issued mobiles devices may significantly threaten IT security and County systems when users access websites and use applications which infect IT operations, and

WHEREAS, control of access to Kenosha County IT systems by outside users is best protected by allowing IT to access any device that connects to County systems and download software to wipe the device and block access if necessary; and

WHEREAS, this software exists, and this policy is written to respond to this situation, and

WHEREAS, the Finance and Administration Committee has reviewed the Kenosha County Mobile Device Usage and Agreement Policy and found it to be a valuable policy worthy of inclusion with other County policies;

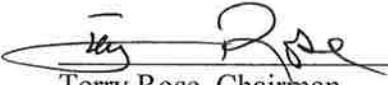

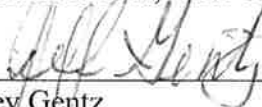
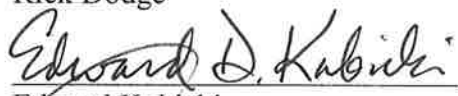
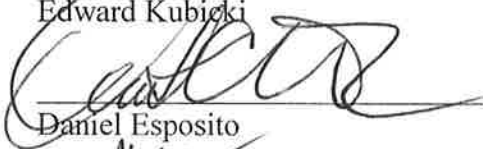

Resolution – To Approve the Mobile Device Usage and Agreement Policy
Page 2

NOW, THEREFORE BE IT RESOLVED, that the Kenosha County Board of Supervisors adopts the Mobile Device Usage and Agreement Policy.

NOW, THEREFORE BE IT FURTHER RESOLVED, that the Human Resources Department and/or Kenosha County Information Technology Department is authorized to make changes to this Policy as needed to comply with any applicable laws, regulations or existing policies in the future.

Approved by:

FINANCE/ADMINISTRATION
COMMITTEE

	<u>Aye</u>	<u>No</u>	<u>Abstain</u>	<u>Excused</u>
 Terry Rose, Chairman	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
 Ronald Frederick, Vice Chair	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
 Jeffrey Gentz	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____ Rick Dodge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
 Edward Kubicki	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
 Daniel Esposito	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
 Greg Retzlaff	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Mobile Device Usage and Agreement Policy Summary

Technology is constantly growing, evolving and becoming a more integral part of our daily lives. The use of mobile devices to enable business productivity has already become ubiquitous throughout businesses everywhere.

The County has taken the first step in connecting our users to resources in a variety of methods; mobile phones, tablets, and laptops to name a few. Protecting and securing County resources is critical, and this policy is the next step in that evolution.

This Mobile Device policy provides County IT the structure and framework to manage the information and resources safely and securely. This does not define the technology, only process and procedure.

The process will include:

- Adoption of the policy by the IT Steering Committee (Complete)
- Adoption of the policy by the Finance Committee and County Board (In progress)
- Publish the policy County-wide; provide information sharing sessions to answer questions
- Collect signed User Acknowledgement and Agreement forms
- Deploy the mobile device management software to everyone who has signed the agreement
- Disable access mobile device access for anyone who has not signed the agreement

MOBILE DEVICE USAGE AND AGREEMENT POLICY

Purpose

Kenosha County provides employees, contractors, and others working on behalf of Kenosha County electronic tools for those whose job performance requires them or would be enhanced by their use. The County supports connectivity to services, and it reserves the right to determine the nature of the connection and protect the information, regardless of whether the connection is to a County-owned or personal device.

The use and assignment of devices is defined in the Kenosha County Cellular Phone and Paging Device Policy, which outlines the assignment of devices or reimbursement of expenses. Appropriate use of devices is governed by the Kenosha County Electronic Communications Policy.

Scope

This policy is limited to the connection of devices to County services and applications from mobile devices. The policy covers both County-owned and employee-owned mobile devices and services.

Roles & Responsibilities

The County and the user both have specific roles and responsibilities. It is the responsibility of each to observe and abide by these responsibilities.

User

Users will acknowledge and accept all terms and conditions for the mobile device equipment/service as defined in this and all other related policies, referenced or not. Kenosha County business shall not be done on any personal cellular devices unless approved in accordance with the provisions of this policy.

When using a personally-owned device (BYOD), it is the sole responsibility of the user to support, replace, or configure the device. Kenosha County Information Technology ("IT") Department will provide best-efforts to connect the device to approved services.

Users must agree to allow the Kenosha County IT access to any device to download the software needed to wipe the device if necessary and to enforce Kenosha County password and encryption policies.

Kenosha County

The County will be responsible for:

- Review of policy and access requirements on an annual basis
- Making users aware of the requirements of this policy and others, as well as good practices related to the protection and security of devices
- Keeping the Acknowledgement form on record for the duration of the individuals' approved access to the services
- Authorizing usage and approving connectivity to services

- Maintaining an escalation process to ensure lost or stolen devices are addressed promptly
- Information Technology will provide guidance to County administration on best practices, conflicts, or questions pertaining to this policy
- Providing support and ensuring connectivity of County-owned devices to approved services

Technical Requirements

Government entities must prevent the unauthorized disclosure of non-public data on mobile devices. The County has implemented a mobile device management (MDM) platform that will govern access to County technology resources. These resources include any County-provided services such as, but not limited to email, SharePoint, Dayforce, or OneDrive.

The County supports the use of both County-issued and personally-owned mobile devices such as phones, tablets, and laptops. Any access request must be approved by a manager and submitted to IT for review and approval.

The manager is responsible for understanding the nature of the job and all associated work rules. IT is responsible for reviewing the request and ensuring the device meets or exceeds all technical requirements.

Public Records and Retention

Kenosha County abides by Wisconsin State Public Records law. All Kenosha County data and records are subject to Public Records Law and the applicable retention schedules. This includes any Kenosha County data and records maintained on personal devices. Users of these services are advised of their responsibilities in the Kenosha County Electronic Communications Policy.

To facilitate responding appropriately to any public record request, the County expressly prohibits automatically forwarding Kenosha County data to personally owned accounts. This includes but is not limited to disabling all auto-forwarding of Kenosha County email to a personal email account.

Encryption

All mobile device data must be protected and managed by IT. Data encryption is viewed in three different ways:

- In Transit: Data that is actively being transferred electronically; this includes but is not limited to email, File Transfer Protocol (FTP), copying from one device to another, or copying to external storage. An example of this is when email is sent; it travels across multiple networks to arrive at the destination.
- At Rest: When data is stored on electronic media such as network drives, USB drives, or phones, but not actively being accessed. This protects the data from unauthorized access. An example of this is a file that is stored on a phone.
- When Accessed: When a file or email is opened for viewing, it requires some level of additional security to gain access. An example of this is when an email is opened, and the viewer is asked to enter credentials or a code to view the data.

All devices granted access must meet the encryption and protection standards required by IT, local and state requirements, and any other compliance requirements such as HIPAA or CJIS. These requirements will vary depending on the device; please open a ticket with IT for additional information.

Password / Authentication Requirements

IT requires certain minimum levels of security in place on any mobile device granted access to IT resources. These will vary depending on the device, ownership, and type of data being accessed. All devices will require user authentication. In some instances, additional levels of authentication will be required; these may include, but are not limited to a PIN, multi-factor authentication, or custom settings. These requirements will vary depending on the device; please open a ticket with IT for additional information.

Access and Remote Data Wipe

Kenosha County has the right to access, monitor and delete Kenosha County information from any device being used to access Kenosha County services and applications. Anyone using a device to access Kenosha County's services and applications may be required to surrender the device for inspection and removal of Kenosha County information. Individuals shall have no expectation of privacy for any electronic communications made, received, transmitted or stored on Kenosha County owned technology resources.

Kenosha County IT also retains the rights and authority to remotely wipe Kenosha County data from any device granted access to County resources. When possible and except in situations involving termination or when Kenosha County determines in its sole discretion that notice would pose a threat to Kenosha County, individuals should be given reasonable notice that Kenosha County data and information will be "wiped" from any device.

Personal Device

If the device is personally owned, the County will restrict remote-wipe to County services. County resources, such as email or file servers, are not for personal use. The County will not preserve personal data stored on County resources, nor provide access to any data if employment is terminated.

County-Issued Device

If the device is County-issued, all data may be access and/or wiped from the device. The County will not provide access to any data if employment is terminated.

Technical Responsibility

It is the responsibility of the user of any device connected to County Services that they will not share their device or passwords and will report if the device is lost or stolen.

Termination from the Program and Services

At its own discretion, Kenosha County may terminate access to this program and any related County service for any reason, and without notice.

Scenarios for Termination

The following scenarios are examples of what may lead to termination from the program:

- The County may cancel the program at any time, for any reason.
- Users may withdraw.
- User violation of the policy.
- Termination of employment.

Process for Termination

Regardless of reason for termination from the program, the following will occur:

- The Service Desk is notified that user access has been terminated, and a service ticket will be created.
- The County will remotely wipe all devices with access. While the County will take steps to wipe only the County data and applications, it may be necessary to wipe the entire device. It is the responsibility of the user to back up personal application data prior to this event, and to restore only personal information after the device has been cleared of County data.
- If the user is using a County-owned device, it is the responsibility of the manager to collect the device immediately and return it to IT within 3 business days.
- The user is not authorized to restore any application or data that originated through the relationship with the County. Any attempt to restore such information will be subject to legal action.
- The user must sign-off on having no other copies of Kenosha County information stored on employee-owned devices (or backups of them), regardless of media.

Risk and Liability

The user is personally liable for all costs associated with his or her personal device. The user assumes full liability for risks including, but not limited to, the partial or complete loss of county and personal data due to an operating system crash, errors, bugs, viruses, malware and/or other software or hardware failures, or programming errors that render the device unusable. Lost or stolen devices must be reported to the Kenosha County IT Department within 24 hours. Users are responsible for notifying their mobile carrier immediately upon loss of a device. While Kenosha County IT will take every precaution to prevent the user's personal data from being lost, in the event it must remove wipe a device, it is the user's responsibility to take additional precautions including, but not limited to, backing up emails or contacts. Kenosha County will not be responsible for any lost devices or information lost from the device.

Definitions

BYOD: Bring Your Own Device, refers to personally owned devices granted access to Kenosha County Resources.

MDM: Mobile Device Management refers to the systems and technologies to manage devices, personal or County-issued, granted access to Kenosha County resources.

User Acknowledgement and Agreement

It is the County of Kenosha's right to restrict or rescind mobile device privileges, or take other administrative or legal action due to failure to comply with the above-referenced policy. Violation of these rules may be grounds for disciplinary action.

I acknowledge, understand, and will comply with the above-referenced security policy and rules, as application to my mobile device usage of Kenosha County services. I understand that the addition of any required County-provided third-party software may decrease the available memory or storage on my personal device and that Kenosha County is not responsible for any loss or theft of, damage to, or failure in the device that may result from use of third-party software and/or use of the device in this program.

I understand that contacting vendors for troubleshooting and support of third-party software is my responsibility, with limited configuration support and advice provided by Kenosha County IT. I understand that business use may result in increases to my personal monthly service plan costs and that Kenosha County is not liable for any increased costs.

Should I later decide to discontinue my participation in the mobile device program, I will allow the County to remove and disable any County-provided third-party software and services from my personal device.

User Name (Printed)	
Manager / Supervisor Name (Printed)	
Requested Effective Date	
Device Ownership (County or Personal)	
Business Justification	
Notes	
Employee Signature / Date	
Manager Signature / Date	

(This page should be signed, scanned, and attached to the ticket request for access.)