



COUNTY OF CARROLL OFFICE OF THE COMMISSIONERS

Administration Building
95 Water Village Road Box 1
Ossipee, New Hampshire 03864



Policy Title:	County-Issued Cell Policy
Effective Date:	June 16 2025
Revision Date:	
Reference (s):	

Purpose

The purpose of this policy is to establish clear guidelines for the issuance of and the appropriate and responsible use of cell phones and other mobile communication devices for Carroll County employees and officials. This policy aims to:

- Ensure efficient and effective communication for legitimate county business.
- Protect confidential and sensitive county information.
- Maintain employee productivity and professionalism.
- Mitigate risks associated with mobile device use, including safety hazards and data breaches.
- Define responsibilities and consequences for non-compliance.

Scope

This policy applies to all employees, officials, contractors, and volunteers of the County who are assigned or authorized to use a County-issued cell phone or other mobile communication device for county business.

Definitions

- **County-Issued Cell Phone (or Device):** Any mobile communication device (e.g., smartphone, tablet, laptop with cellular capabilities) provided by the County to an employee for official County business.
- **Employee:** Any individual employed by the County, including full-time, part-time, temporary, and contractual employees, as well as elected officials and authorized volunteers, who are subject to this policy.
- **County Business:** Any activity performed by an employee within the scope of their employment or official duties for Carroll County.
- **Confidential Information:** Any non-public information related to County operations, residents, employees, finances, or legal matters, regardless of its form (e.g., electronic, written, verbal).

General Principles

- **County Property:** All County-issued cell phones and the data stored on them are the property of Carroll County.
- **Primary Use:** County-issued cell phones are primarily intended for official County business.
- **Responsible Use:** Employees are expected to use County-issued devices responsibly, ethically, and in a manner that reflects positively on the County.
- **Compliance:** Employees must comply with all applicable federal, state, and local laws, as well as all other County policies and procedures, when using County-issued devices.
- **Security:** Employees are responsible for safeguarding County-issued devices and the data they contain from unauthorized access, loss, or damage.

Usage Guidelines

Authorized Business Use

County-issued cell phones are provided to facilitate official County business. Authorized uses include, but are not limited to:

- Making and receiving business-related calls.
- Sending and receiving business-related emails and text messages.
- Accessing County-approved applications and resources necessary for job duties.
- Communicating with supervisors, colleagues, clients, and the public for County business.

Limited Personal Use

Incidental and infrequent personal use of County-issued cell phones is permitted, provided it:

- Does not interfere with the employee's job duties or productivity.
- Does not incur significant additional costs to the County (e.g., excessive data usage outside of standard plan, international calls without prior approval). Employees may be held responsible for excessive personal charges.
- Does not violate any other County policies or laws.
- Is conducted during non-work hours, breaks, or in a manner that does not disrupt the work environment or other employees. Employees are encouraged to use personal cell phones for personal calls and communications whenever possible.

Prohibited Use

The following uses of County-issued cell phones are strictly prohibited:

- **Driving:** Using a County-issued cell phone (hand-held, hands-free, or voice-activated) while operating a County vehicle, personal vehicle, or equipment during work hours, unless parked safely and legally. This includes talking, texting, emailing, or interacting with applications. Emergency personnel may have exceptions defined by their department's specific protocols.
- **Fueling Vehicles:** Using a cell phone while fueling any vehicle or equipment.
- **Illegal Activities:** Engaging in any illegal activities.
- **Inappropriate Content:** Accessing, transmitting, or displaying sexually explicit, obscene, discriminatory, harassing, threatening, or otherwise inappropriate content.
- **Confidential Information Disclosure:** Storing, transmitting, or discussing confidential or sensitive County information on non-secure networks or in a manner that compromises its confidentiality, integrity, or availability.

- **Unauthorized Software/Hardware:** Installing unauthorized software, applications, or making unauthorized modifications to the device's hardware or operating system
- **Commercial Use:** Using the device for personal commercial purposes, soliciting, or engaging in outside business activities.
- **Gaming/Entertainment**
- **Impersonation:** Impersonating another person or misrepresenting one's identity.

Data Security and Confidentiality

- **Password/PIN Protection:** All County-issued cell phones must be protected by a strong password, PIN, or biometric authentication (e.g., fingerprint, facial recognition) that is enabled at all times. Passwords must be changed regularly, as per County IT policy.
- **Encryption:** County IT will ensure appropriate encryption is enabled on devices where County data is stored or accessed. Employees must not disable these security features.
- **Public Wi-Fi:** Employees should avoid accessing or transmitting sensitive County data over unsecured public Wi-Fi networks. A County-approved Virtual Private Network (VPN) should be used when available for remote access to County systems.
- **No Sharing:** Employees must not share their County-issued device or access credentials with unauthorized individuals.
- **Data Minimization:** Only necessary County data should be stored on the device. Employees are responsible for regularly backing up critical data to County-approved storage locations.
- **Cloud Services:** Use of third-party cloud storage or collaboration services for County data on a County-issued device is prohibited unless explicitly approved by County IT and covered by a formal agreement.

Software and Applications

- Only County-approved applications relevant to an employee's job duties may be installed on County-issued cell phones. Employees should not download or install personal applications without explicit permission from County IT, as these may pose security risks.
- Operating system and application updates should be installed promptly as directed by County IT.

Device Management

Assignment and Return

- County-issued cell phones are assigned to specific positions or employees based on demonstrated business need, as determined by the employee's Department Head and County Administration.
- Upon termination of employment, transfer to a position that does not require a County-issued device, or at the request of the County, employees must immediately return the County-issued cell phone and all associated accessories (e.g., charger, case) to their Department Head or County IT.
- Employees and elected officials are responsible for ensuring all County data is maintained on the device prior to return, only County IT is authorized to remove data.

Care and Maintenance

- Employees are responsible for exercising reasonable care to keep County-issued cell phones in good working order and to protect them from damage, loss, or theft.
- Any damage to a County-issued device, beyond normal wear and tear, due to negligence or misuse by the employee may result in the employee being responsible for repair or replacement costs.
- Employees must notify their Department Head or County IT immediately of any malfunction or damage to the device.

Lost or Stolen Devices

- Employees must immediately report the loss or theft of a County-issued cell phone to their Department Head or County IT.
- Upon notification, County IT will take immediate steps to remotely wipe or disable the device to protect County data.
- Employees must cooperate fully with any investigation into the loss or theft.

Inspection and Monitoring

- Employees should have no expectation of privacy regarding any communications, data, or files on County-issued cell phones.
- The County reserves the right to inspect, monitor, access, retrieve, and disclose any information transmitted, received, or stored on County-issued cell phones at any time, with or without notice, for legitimate County business purposes (e.g., security, compliance, legal investigations, operational needs).
- This includes, but is not limited to, call logs, text messages, email, internet browsing history, and application usage.

Privacy

While the County may permit limited personal use of County-issued cell phones, employees should be aware that all data on the device, including personal data, is subject to County inspection and may be discoverable in legal proceedings. Employees should avoid storing highly sensitive personal information on County-issued devices.

Costs and Reimbursement

- The County will cover the monthly service charges and reasonable usage costs for County-issued cell phones, as determined by the approved service plan.
- Employees will be responsible for any excessive charges incurred due to unauthorized use or personal use that exceeds the incidental allowance.
- The initial purchase of the device and standard accessories is the responsibility of the County.

Criteria for County Phone Issuance

An employee should be considered for a county-issued cell phone if their role consistently meets one or more of the following criteria:

- **Required Off-Site Communication:** The employee regularly needs to communicate for county business while working outside of a county office
- **Critical On-Call/Emergency Response:** The position involves being on-call or responding to emergencies, requiring immediate and reliable communication for critical county operations.
- **Handling Sensitive Information:** The employee frequently discusses or transmits confidential or sensitive county data that requires secure, county-controlled communication channels.

Violations and Disciplinary Action

Any violation of this policy may result in disciplinary action, up to and including termination of employment, loss of County-issued cell phone privileges, and/or legal action, depending on the severity and nature of the violation. Disciplinary action will be in accordance with the County's human resources policies and collective bargaining agreements, where applicable.

Employee Acknowledgment

All employees assigned a County-issued cell phone or using a personal device for County business must read, understand, and sign an acknowledgment form confirming their agreement to abide by this policy. The signed acknowledgment form will be kept in the employee's personnel file.

Policy Review

This policy will be reviewed periodically by the HR and IT departments and revised as necessary to ensure its continued effectiveness and compliance with evolving technology and legal requirements.

Chuck McGee
Chairman

Harold B. Parker
Vice-Chairman

Gene Chandler
Clerk