Asheville Police Department Policy Manual

Chapter: 2 - Administration
Policy: 206 - Technology Use & Security
Previously: 1800 - Computer Technology

Original Issue: 5/10/2002
Last Revision: 9/5/2025

Contents

Introduction
Policy Statement
Definitions
Rules and Procedures
206.1 General Provisions
206.2 Security
206.3 Data Backup and Storage
206.4 Email and Electronic Messaging
206.5 Mobile Data Terminals

Associated Directives

City of Asheville Remote Access Policy
City of Asheville Password Policy
City of Asheville Internet Policy
City of Asheville Email Policy

Introduction

The following policy provides guidance on the proper use of department computer systems, including the use of email, the internet, and related electronic message transmissions.

Policy Statement

It is the policy of the Asheville Police Department (APD) that all department members abide by the department and City of Asheville directives when using information technology resources, including computers, software, and systems issued or maintained by the City.

Defintions

Automatic Vehicle Locator (AVL): a safety feature of the mobile communications system that allows for the automatic location of field units via a GPS signal.

Computer System: all computers, electronic devices, hardware, software, and resources owned, leased, rented, or licensed by the City of Asheville that are provided for official

use. This includes access to and use of Internet Service Providers (ISPs) or other service providers provided by or through the City.

Hardware: includes, but is not limited to, computers, computer terminals, network equipment, electronic devices, telephones, or any other tangible computer device generally understood to comprise hardware.

Software: includes, but is not limited to, all computer programs, systems, and applications. This does not include files created by an individual user.

Mobile Data Terminal (MDT): a system for providing real-time data communications and field reporting, typically consisting of specialized, secured mobile computers within vehicles.

Rules and Procedures

206.1 General Provisions

A. Department employees must use all department computer systems in accordance with all applicable federal, state, and local regulations, City of Asheville policies, and department directives. [41.3.7 b]

B. Computer repairs will only be made by city-approved sources.

C. Department computer systems are to be used for business purposes; however, personal use may be permissible if *limited in scope and frequency* and in conformance with department and city policy. [41.3.7 b]

D. The City of Asheville Remote Access Policy governs remote access to workstations from external computer systems.

E. Employees do not maintain any right to privacy in department computer systems or their contents, including any personally owned software authorized for installation. The department may monitor or inspect information contained in department computer systems.

206.2 Security [82.1.6]

A. All system access requires supervisor authorization and is activated via the City of Asheville Information Technology Services (IT Services). [41.3.7 a]

B. Access to the department's electronic records management systems and criminal justice information systems (CJIS) is granted only with approval from the chief of police or designee. [82.1.1 a]

C. All department members will comply with the City of Asheville Password Policy.

D. User passwords for accessing department resources, including computer systems and information networks, must not be shared or disclosed to any other individual.

E. To protect centrally located data from unauthorized viewing, all users will log off or otherwise secure their computers when leaving a device unattended.

F. Access to programs or data for which users are not authorized is prohibited.

G. An annual audit of passwords and access codes will be conducted with the assistance of IT Services to maintain the integrity of computerized systems and ensure the security of records stored within them. [82.1.1 a][82.1.6 c,d]

H. For security reasons, application programs/software will not be installed, uninstalled, or altered on city hardware without prior approval from IT Services. However, applications directly related to work activities may be downloaded on department-issued mobile phones, provided they are in conformance with this policy. [41.3.7 c]

    1. Employees must exercise caution when installing mobile applications that request access to sensitive device data, such as location, email information, or contacts. If concerns arise, IT Services or a supervisor will be consulted before installation. [41.3.7 c,d]

I. Employees must carefully evaluate and exercise caution when introducing any unverified or unknown external data storage devices (e.g., thumb drives or external hard drives) to city computers. Devices of unknown origin should not be plugged into city computers without proper precautions. If there is a concern of a security risk related to accessing data from a data storage device, a supervisor or IT services must be consulted. [11.4.4]

206.3 Data Backup and Storage

A. Data storage systems will be backed up and stored by IT Services according to a regular schedule and in compliance with record retention laws or regulations. [82.1.6 a,b]

B. If media is not recycled, methods of destruction should be determined to ensure compliance with CJIS security regulations by confirming data is not retrievable from the discarded media.

206.4 Email and Electronic Messaging

A. Transmission of electronic messages and information on communications media provided to department members will be treated with the same degree of

propriety, professionalism, and confidentiality as official written correspondence or verbal communication. [41.3.7 b]

B. Accessing or transmitting materials (other than those required for law enforcement purposes) that involve the use of obscene language, images, jokes, sexually explicit materials, or messages that disparage any person, group, or classification of individuals is prohibited, whether or not a recipient has consented to or requested such material.

C. All department members must comply with the City of Asheville Internet Policy and Email Policy.

D. The Professional Standards Section may conduct reviews of department electronic messaging traffic to ensure compliance with this policy. [41.3.7 e]

206.5 Mobile Data Terminals

A. Access to Mobile Data Terminal (MDT) systems will be arranged by the Logistics Section in conjunction with the City of Asheville ITS. Only trained department members with proper certifications will be authorized to utilize department MDTs. [41.3.7 a]

1. MDT users will be trained on the operation and proper care of MDT equipment and associated standard operating procedures.

2. Employees utilizing the North Carolina Division of Criminal Information (DCI) network through an MDT must be DCI certified and adhere to all DCI standards and protocols, including but not limited to rules and regulations regarding access and disclosure of information. [4.01]

B. MDTs will only be used for APD-related operations and investigations. [41.3.7 b]

C. Wherever equipped, AVLs will remain on at all times while the vehicle is in operation. The AVL device will not be tampered with or turned off.

D. Information received through law enforcement databases and computer systems (including but not limited to NCIC, DCI, NLETS, DMV, and CJLEADS) is confidential. The use of this information is for law enforcement purposes only.

E. Department members will power on and log into the terminal, and ensure it remains on at all times while operating a marked department vehicle equipped with an MDT. This includes, but is not limited to, all working hours, traveling to and from work in take-home vehicles, traveling to and from training, callouts, and secondary or extra-duty assignments.

F. Department command staff members must have MDTs powered on and operational while operating a department vehicle when performing patrol support functions, such as, but not limited to, watch command, District Commander responsibilities, call-outs, and secondary or extra-duty assignments.

G. Employees will only utilize the MDT when it is safe to do so. Employees must focus their attention on the safe operation of their vehicles.

H. Department members are responsible for the physical security, care, and safekeeping of assigned MDTs, related documentation, and accessories, whether assigned on a permanent or temporary basis.

    1. MDT screens will be blacked out or closed from view when information can be viewed by unauthorized persons.

    2. MDTs may not be moved between vehicles without approval from a supervisor and notification to the department's logistics function.

I. No unauthorized software will be installed on MDTs. Hardware and software configuration settings will only be changed by personnel authorized by the City of Asheville IT Services or APD Logistics. [41.3.7 c,d]

J. Shift supervisors will inspect all MDTs in their district during regular vehicle inspections and note any damage, function problems, or unauthorized programs. Maintenance issues will be forwarded to the department's logistics function for follow-up.

By order of:

Michael Lamb
Chief of Police