ASHEVILLE POLICE DEPARTMENT POLICY MANUAL

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

Original Issue: 5/10/2002
Last Revision: 5/6/2020

CONTENTS

INTRODUCTION
POLICY STATEMENT
DEFINITIONS
RULES AND PROCEDURES
206.1 GENERAL PROVISIONS
206.2 SECURITY
206.3 DATA BACKUP AND STORAGE
206.4 E-MAIL 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 to include 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 that are issued or maintained by the City.

DEFINITIONS

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 (ISP) 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.

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.

D. Remote access to workstations from external computer systems is governed by the City of Asheville Remote Access Policy.

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

206.2 SECURITY

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 to access department resources, including computer systems and information networks, must not be shared or made known to any other individual.

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

F. Access to programs or data for which users do not have authorization is prohibited.

G. An annual audit of passwords and access codes will be performed with the assistance of IT Services to maintain the integrity of computerized systems and security of records contained in the systems. [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 approval by IT Services; however, applications directly related to work activities may be downloaded on department-issued mobile phones if in conformance with this policy.

    1. Employees must use caution when installing mobile applications requesting access to device data, such as location, e-mail information, or contacts; if there is any concern IT Services or a supervisor will be consulted prior to installation. [41.3.7 c,d]

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 E-MAIL 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.

B. Accessing or transmitting materials (other than that required for law enforcement purposes) that involves 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. MDT users will be trained on operation and proper care of MDT equipment and associated standard operating procedures.

B. 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.

C. Employees utilizing the North Carolina Division of Criminal Information (DCI) network through an MDT must be DCI certified and operate mobile computing devices in accordance with DCI standards and protocols.

D. Information received through law enforcement databases and computer systems (e.g., 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. MDT screens will be blacked out or closed from view when information can be viewed by unauthorized persons.

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

J. MDTs may not be moved between vehicles without approval from a supervisor and notification to the Logistics Unit.

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

BY ORDER OF:

David Zack
Chief of Police