

## MEDINA POLICE DEPARTMENT

Subject: <b>Technology Usage</b>	Policy Number: <b>4100</b>	<b>Technology Usage 4100</b>
Reference: <b>Chief's Directive</b>	Pages: <b>2</b>	
Personnel: <b>Sworn and Non-Sworn Personnel</b>		
Issue Date: <b>01-01-2004</b>	Revised Date: <b>11-17-2020</b>	

### **4100.1 – INTRODUCTION**

It shall be the policy of this agency to comply with applicable federal laws regarding electronic communications, cell phone use and software copyright regulations, to safeguard the department from computer virus infections, and to limit Internet use for business purposes, it is understood that Internet use will be used on a limited basis for personal use. In compliance with these issues, the following guidelines will be adhered to:

### **4100.2 – SCOPE**

This policy serves to state the position of this agency relative to computer software, usage of agency computers by unauthorized personnel, proper Internet/e-mail usage, cell phone usage, and safeguarding of laptop computers.

### **4100.3 – POLICY**

In compliance with software piracy laws, no software from this agency may be removed from the premises or copied for personal use. No software may be brought into this department and installed into agency computers without the express written permission of the Chief of Police or designee. When such permission is obtained, the software will be installed by a qualified individual in accordance with licensing agreements only.

Personally owned devices will not be allowed to access or store any criminal justice information for any reason.

Requests for new software beneficial to the mission of this agency may be made through the Chief of Police or designee. If approved, the software will be purchased and registered to the police department.

Software loaded on individual computers is subject to review at any time, and unauthorized software will be removed.

No unauthorized personnel are to be allowed to access or use police department computers either in the agency office space or in the homes of employees.

The email system is the property of the police department and is intended for the furtherance of official business for this agency. Messages transmitted or received by the email system are messages and property of this agency.

Telecommuting – Police employees desiring to work from a remote site, such as a home office, must obtain permission from the Chief of Police. The Chief of Police will contact the City Administrator and the City’s IT consultant to set up remote access for the user. A reliable current-model compatible computer and anti-virus software acceptable by the IT consultant will be required at the employee’s expense.

Right to Inspect – The City has the right to inspect the contents of any City-owned equipment, files, email, or voice mail for any reason. The City also has the right to inspect any employee owned equipment that is being used to conduct City business if there is cause to do so. By using the City’s technology, all users consent that the City may, at its discretion, inspect, use or disclose any electronic communications and/or data without further notice for any legitimate business, legal or disciplinary purpose and may disclose or disseminate such data to appropriate third parties. All messages sent on the email system are viewed as police department messages and **not** personal, confidential messages of the employee.

The supervisory staff of the police department has the right to enter the agency e-mail system and review, copy, delete, or disclose any message.

Passwords will be used to gain access to the e-mail system for the purpose of protecting the integrity of the police department.

Email messages are the intellectual property of the police department, not of the employees, and must pertain only to agency business.

Email messages should not be left on the computer screen when the employee is away from his/her desk or workstation, in order to protect agency proprietary information.

Passwords will be changed as directed.

Documents, files, or programs will not be password protected without prior approval of the Chief of Police.

No information protected by copyright laws, including software, will be sent or copied via e-mail.

All messages on the e-mail system are to be businesslike. There will be no tolerance for messages which contain profanity, vulgarity, and/or harassing or defamatory language.

Employees may use technology for personal use provided it does not interfere with or pre-empt City business and is used at appropriate times. (breaks, before or after work).

Personal Use of City Phones – Limited personal phone calls on city-owned phones are allowed without reimbursing the City. Employees must reimburse the City for all strictly personal phone calls made on the City’s phone when number of minutes on the rate plan are exceeded.

## Supervisor On-Call Phone Usage

Supervisors that are expected to be available for after hour calls will be assigned a cell phone. This cell phone can be used for personal use. The phone is considered City property and will be held to the same standards as listed above. The supervisor will not be compensated for calls received after hours.