
	POLICY AND PROCEDURAL ORDER		013-007
	Computer Use		Page 1 of 5
	Issued By: Interim Chief Aimee Metzger	CALEA Standards 82.1.6 	
Effective: 02/01/2002	Updated: 03/15/2021		
Last Reviewed: 09/16/2023			

I. Purpose

The purpose of this policy is to ensure the proper use of the city's and the department's computing systems, including the Internet and electronic mail (e-mail) by Ann Arbor Police Department employees, while supporting the needs of city residents, other customers of city services and city employees.



II. Definitions

- A. Non-employee User: Any user authorized access to the City's computer system who is not an employee of the city, including contractors and volunteers.
- B. Unlicensed Software: Software that the user has no legal right to use or install.
- C: Virus: A computer program not controlled by normal computing system utilities. A virus' impact on the operations of the computing systems may range from a minor annoyance to complete failure of the computing systems.



III. Policy

It is the policy of this department that all electronic systems, hardware, software, temporary or permanent files and any related systems or devices purchased or acquired by the City are the property of the City of Ann Arbor.

- A. All hardware additions or modifications must be authorized by the City's Information Technology Services Unit.
- B. The Chief of Police or their designee can authorize Information Technology Service Unit (ITSU) employees, to inspect the contents of any equipment, files, calendars, or electronic mail in the normal course of their supervisory responsibilities. Reasons for review include, but are not limited to, system, hardware or software problems including software license compliance, general system failure, litigation or potential litigation, suspicion of a crime or violation of a policy, or a need to perform work or provide a service when the employee is not available. As a normal, daily business procedure, automated monitoring software may be used to monitor system performance, application usage, and e-mail content. Notice will be given to the organization prior to these applications being activated. These inspections or reviews will be under the direction of the Chief of Police or their designee.
 - 1. If files deemed confidential by the City are involved, either the user, his/her immediate supervisor, or the Chief of Police shall authorize access in writing, except in the case of an emergency.

	POLICY AND PROCEDURAL ORDER		013-007
	Computer Use		Page 2 of 5
	Issued By: Interim Chief Aimee Metzger	CALEA Standards 82.1.6 	
Effective: 02/01/2002	Updated: 03/15/2021		
Last Reviewed: 09/16/2023			

2. It is a violation of this policy for any user, including ITSU employees, department heads and supervisors, to use the e-mail and computer systems for purposes of satisfying idle curiosity about the affairs of others, with no substantial business purpose.
- C. Requests for computer access must be approved by the Chief of Police or their designee before access shall be granted by ITSU.
1. The Chief's management assistant will notify ITSU of users' changes in access authorization, i.e. termination, transfer, or end of contract. Changes as a result of termination and suspension will be conveyed to the above parties prior to the termination or suspension.
 2. Non-employee user (e.g., authorized contractors or volunteers) access must have a set termination date.
- D. Only licensed software may be installed on the City's computing system. Users may not install unlicensed software. Users will be held personally liable for any penalties associated with unlicensed or unauthorized software that the user has placed on the computing system.
1. Any software ITSU will be expected to support must receive prior written approval from the Information Technology Services Unit.
 2. All software installations not approved in writing by the section commander may be subject to deletion.
- E. Users are expected to exercise good judgment while using the City's computing systems. ITSU monitors and reports on each individual's use of the computing system, including Internet activity.
- F. The City's computing systems shall be used for the purpose of conducting City business. Occasional personal use of the City's computing systems for activities allowed under this policy is permitted outside of the employee's working hours. The city permits this with the purpose of encouraging employees to improve their computing skills.
- G. Users are prohibited from utilizing the City's computing systems to compromise the integrity of the city and its business in any way. Prohibited uses outside of the scope of your assigned duties include, but are not limited to:


	POLICY AND PROCEDURAL ORDER		013-007
	Computer Use		Page 3 of 5
	Issued By: Interim Chief Aimee Metzger	<div>CALEA Standards</div> <div></div> <div>82.1.6</div>	
Effective: 02/01/2002	Updated: 03/15/2021		
Last Reviewed: 09/16/2023			


1. Accessing, distributing, or publishing pornographic materials, unless necessary for investigative purposes.
2. Activities that will incur a cost to the City without prior authorization from the Chief Police or their designee.
3. Activities that compromise the security of the computing systems.
4. Activities that degrade the performance or impair the reliable operation of the City's computing systems.
5. Business uses unrelated to the city.
6. Chain letters through e-mail.
7. Defamation (slander/libel).
8. Deliberate misinformation.
9. Endorsements.
10. Harassments.
11. Activities that violate any law or regulation including copyright laws.
12. Offensive messages or material.
13. Political activities unrelated to job function.
14. Religious activities.
15. Threats.

- H. Members of the Ann Arbor Police Department, as City employees, are required to adhere to City Human Resources [Policy 2.13 "Personal Use of Social Media"](#). This City policy is hereby incorporated as an AAPD Policy and Procedure.

The city may block access to various web sites which do not meet city needs. Sites to which access may be blocked shall be approved by the Chief of Police or their designee, the Administrative Services director and/or the City Administrator.

- I. Communication with elected officials is governed by Council Administrative Rule 1: Administrative Responsibility, located on page 16 in [Rules of the Council and](#)

	POLICY AND PROCEDURAL ORDER		013-007
	Computer Use		Page 4 of 5
	Issued By: Interim Chief Aimee Metzger	CALEA Standards 82.1.6	
Effective: 02/01/2002	Updated: 03/15/2021		
Last Reviewed: 09/16/2023			



[Pertinent Charter Provisions.](#) If an Ann Arbor Police employee has any concerns about communications received from an elected official, it should be directed to the Office of the Chief of Police.



- J. All electronic messages will be retained on the city system for **35 days** after the message has been discarded to “Trash” and emptied or otherwise deleted by the employee.

IV. Responsibilities

- A. It is the responsibility of users to adhere to all City and department computing systems policies and procedures. All employees using the City’s computing systems shall have electronic access to this policy and certify that they have read and fully understand the contents.
- B. It is the responsibility of ITSU to maintain and safeguard the information technology infrastructure for the city.
- C. It is the responsibility of ITSU to plan for and provide City staff with training to use the City’s computing systems.
- D. It is the responsibility of division commanders to ensure that computing systems policies and procedures are followed by users within their departments.
- E. It is the responsibility of ITSU to review Internet usage and recommend policy and procedure changes to the Internet Policy Committee, which shall make recommendations for changes to the City Administrator.
- F. It is the responsibility of users to backup any data files saved to their local drives.
- G. It is the responsibility of the Information Technology Services Unit to ensure that all police department servers and databases are routinely backed-up. The back-ups will be stored off site in a secure location for data retrieval in the event of data loss to the active production servers. Police department servers will be included in the City ITSU back-up schedule when possible.

V. Passwords

It shall be the responsibility of ITSU to develop and enforce password security measures. Members of the Ann Arbor Police Department, as City employees, are required to adhere to Information Technology [Policy 706 Password Policy](#). This City policy is hereby incorporated as an AAPD Policy and Procedure.

	POLICY AND PROCEDURAL ORDER		013-007
	Computer Use		Page 5 of 5
	Issued By: Interim Chief Aimee Metzger	<div>CALEA Standards</div> <div></div> <div>82.1.6</div>	
Effective: 02/01/2002	Updated: 03/15/2021		
Last Reviewed: 09/16/2023			

VI. Viruses

ITSU is responsible for providing an automatic virus detection program. Users should not circumvent the program's installed configuration.

- A. When a virus is detected, a user shall immediately notify the **ITSU Help Desk (x45502) or at 734-794-6550**. In addition, the following steps should be taken:
 1. Write down the name of the virus as provided by the anti-virus software.
 2. Record any noticeable effects from the virus.
 3. Post a note on the infected machine to prevent further spread of the virus.
 4. If the computer is on the network, as a precaution, physically disconnect the computer from the network.
- B. ITSU will oversee the effort to eradicate the virus from the City's computing systems. In addition to "cleaning" the infected computers, ITSU will ensure that the virus is removed from all exposed machines and diskettes.

VII. Violations

Violation of this policy may result in disciplinary action up to and including termination as provided in the Personnel Rules and Regulations and appropriate union contracts.