

CITY OF ALPENA  
COUNCIL POLICY STATEMENT

General Subject:	Computer, Email, and Internet Usage	Policy No.	<u>56</u>
		Date Issued	<u>May 12, 2016</u>
		Effective Date	<u>Feb 1, 2017</u>

---

Copies to: City Council, City Manager, City Attorney, Department Heads, File.

---

**PURPOSE:**

The purpose of this Council Policy Statement (CPS) is to provide guidelines for the usage and operation of City-owned computer systems, email, internet access, and other equipment by City Employees and their assigns.

The use of City computer equipment is a privilege that may be suspended or revoked at any time. Any violations of this policy are subject to appropriate and applicable disciplinary action by the Department Head and/or the City Manager, up to and including termination of employment.

**DEFINITIONS:**

“IT Staff” refers to the appointed City Employee (IT Coordinator) and the entire contracted IT services staff. It will also refer to any additional City employee appointed by the City Manager.

Various terms shall be universally used, independently or in some combination, to describe City-Owned and issued electronic equipment. These terms include, but are not limited to: Computer, system, desktop, laptop, tablet, network, server(s), printer(s), scanner(s), digital camera(s), copier(s), peripherals, email, and internet. The terms computer, computers, and computer system may be used to refer to any and all parts, or the entirety of City-Owned and issued electronic equipment.

The term “user(s)” shall collectively refer to City Employees, City Council, Contractors, Authorized Guests and their Assigns who may, in their course of work, use City-owned and operated computer equipment.

**APPLICATION:**

The computer system, including, but not limited to, computers, monitors, printers, all peripherals, all electronic communication, and all data and information transmitted by, received from, or stored in these systems, are the property of the City of Alpena.

The City of Alpena reserves the right to monitor all computer/network/internet traffic.

**USERS:**

Only City of Alpena employees, and their assigns, that have computer user accounts and passwords, are permitted to use the computer systems. Computer accounts are established immediately prior to the first day of employment and users may not login until they have read the Computer, Email, and Internet Usage Policy and acknowledged via signature page or email to Human Resources indicating that they

have read and understand the policy. Upon separation from the City, the user's computer account and all associated privileges will be revoked.

**DEVICES:**

Users shall not connect personal or non-City-owned devices to the network. In certain circumstances, a Department Head may request, in writing, for a particular device to be connected to the network and may only do so after permission is granted by City and/or County IT Staff.

Unauthorized USB drives, or other electronic media (CD's DVD's), shall not be connected to City-Owned equipment. Further, authorized USB drives shall not be connected to personal electronic equipment, not under the ownership of the City. If an employee requires the use of equipment in a location other than their workstation in order to complete their assigned work, the Department Head shall request such in writing.

**HELP DESK SERVICE TICKET SYSTEM:**

All users shall use the help desk ticket system to request service for the computer systems. This system assists the IT Staff in tracking and prioritizing work on the system. Generally, there will be a shortcut on the users' desktop for this purpose. Users can also send an email to [cityhelpdesk@alpena.mi.us](mailto:cityhelpdesk@alpena.mi.us) and a ticket will be created. Once created, all updates and activity including the technician assigned will be emailed to the user. Phone calls directly to the IT Department will not be addressed unless there is a supporting ticket already created.

**SYSTEM USES:**

- Computers and all equipment shall be used consistent with legitimate City business interests
- A user's computer is generally equipped with the appropriate software for their position. With the Department Heads permission, users may install and/or remove software programs/applications as their position or department requires. Users shall not install software/applications unrelated to their current position or department. If non-work related software/applications are found to be the cause of a computer issue (slow, locked, virus) the right to install software may be revoked.
- Physical abuse to the equipment shall not be tolerated.
- City computers shall not be used to participate in or conduct illegal activities including, but not limited to, gambling, file sharing, hacking, virus generation, and any other activities in violation of state and federal laws.
- It shall be the responsibility of the appropriate Department Head or the City Manager to interpret if uses of the computer system not mentioned above are acceptable or inappropriate as it relates to the position or department in which the employee works and determine the appropriate disciplinary action.

- Unless otherwise directed, all technical maintenance shall be performed by IT Staff
- Users shall store all data on the City Servers, generally identified as “H, P, J, U” etc. Users shall not store any data on the local computer. Data on the server is backed up and protected against loss, the local computer is not. The only case where data may be stored locally is in the case of an email archive file, but the user should be warned that this is not protected against computer failure and is not always recoverable.
- Users are provided with access to their personal “U” drive that no other users can see. This is provided for personal work files such as goals, internal memos, and letters etc. Users are urged not to use this drive for general department data as it cannot be accessed by department co-workers.

### **INTERNET ACCESS:**

Users are provided with access to the City’s internet service for work related purposes. It shall be the responsibility of the appropriate Department Head or the City Manager to interpret if the employee’s use of the internet is applicable to the position and determine the appropriate disciplinary action, if any is warranted. Access to most websites is allowed, but all activity is monitored and reports of usage by a user are made available to the Department Head or City Manager at their request.

Blocked websites (ie. pornographic, gambling) may need to be accessed by some positions (ie Police). The Department Head shall file a service ticket request to grant access to specific employees.

Generally, the Department Head shall be responsible for monitoring times in which the employee accesses the internet for personal use. Employees may access the internet for personal use during their breaks/lunches. Such personal use shall not cause undue stress on the system or internet connection, (ie. streaming movies, streaming music, large downloads).

Examples of prohibited uses of the City’s internet service include, but are not limited to:

- Sending/participating in chain letters
- Sending files in violation of copyright laws
- Uses that compromise the integrity of the City and its’ business
- Unauthorized use to purchase or sell goods or services unrelated to work during work hours
- Browsing or publishing to social networking sites unrelated to work during work hours
- Unauthorized file downloads
- Internet gambling
- Displaying, submitting, or accessing inappropriate material (adult, sexually oriented, etc.)
- Use of access codes or passwords to misrepresent oneself in any manner
- Any other immoral or unlawful purpose

**USERNAME AND PASSWORD:**

Generally, each username shall follow the format of first name with first initial of last name (johnd or janed) with all lower-case letters. In some cases, this may change due to previous or existing users with the same name and initial.

Passwords are required to be in the following format:

- Shall be a minimum of eight (8) characters AND
- Shall contain 2 of 3 types of characters: at least one capital letter, one symbol, one number

Passwords shall not be the same as the username. Passwords will expire after ninety (90) days. Passwords shall not be identical or contain previous parts of the 10 previous passwords used (ie: Apple42, Apple43).

Users are advised to not use words found in the dictionary or proper names. If standard words are used, it is suggested that multiple words without spaces are used. (ie: instead of “Puppies37” use “theBrownPuppies37”)

Passwords shall NOT be written down at the users’ workstation.

A user shall not share their password so another user can login to the system. If access to specific directory or software is needed for another user who does not have it, then a service ticket should be filed to request that a particular user be given rights to a directory or software.

IT Staff does not know user passwords and cannot look them up, they can only reset them. If a user is in need of assistance or maintenance is required on their computer, IT Staff may request the user’s name and password. IT Staff is the only personnel that users should give their password to.

Each user is responsible, and will be held accountable for, all activity that can be traced to their user account.

The system shall enforce a limit of no more than 3 consecutive invalid access attempts by a user. The system shall automatically lock the account for a 10 minute time period, after which the user may try again.

**EMAIL:**

All the guidelines and restrictions set forth in the Internet Access section shall generally apply to email usage.

Users can access their City email account using the Outlook application on their computer. They can also access their email from any computer using the web application. This can be reached by directing a browser to the City’s home page at [www.alpena.mi.us](http://www.alpena.mi.us) and clicking on “Employee Email” at the top right hand side. Additional documentation and training for accessing web email is available upon request.

Users should obey the same standard general etiquette and guidelines for email communication as with standard mail and letters. (ie. Using all capital letters is not recommended, being curt or rude should be avoided, etc.)

All City email on servers or local computers is subject to Freedom of Information Act requests. Users are cautioned about using their City email address for their default personal communication on a regular basis or for use as their login information for personal shopping, invoicing, bill payments, etc. Email shall not be considered confidential correspondence.

While email is generally considered a dependable and sometimes legally binding method of communication, it is not a guaranteed source of communication, nor should it be construed as instantaneous. If a user is expecting a response, and has not received one in a timely manner, communication other than email should be attempted.

The IT Staff maintains a back-up copy of all email for 60 days. It is the users' responsibility to maintain and organize their own mailbox and if it becomes full, they must maintain a local mailbox for archiving purposes. Users can be trained in the archiving process by submitting a request for service ticket.

The User is responsible and accountable for the content and initial recipients of their communications.

Users shall not send or forward messages containing a virus warning. The IT staff should be contacted immediately. They will provide further instruction.