MONTPELIER POLICE DEPARTMENT

POSITION, EQUIPMENT, DATABASE SYSTEMS AND TECHNOLOGY USE	Related Policies: City of Montpelier Personnel Plan Manual Cellular Telephone Policy Duty to Disclose Criminal Threat Assessments, Security Assessments, and Report Caveats
This policy is for internal use only and does not enlarge an employee's civil liability in any way. The policy should not be construed as creating a higher duty of care, in an evidentiary sense, with respect to third party civil claims against employees. A violation of this policy, if proven, can only form the basis of a complaint by this department for non-judicial administrative action in accordance with the laws governing employee discipline.	
Applicable Vermont Statutes:	
CALEA Standard:	
Date Implemented: December 28, 2020	Review Date: December 28, 2021

I. Purpose: It is the purpose of this policy to establish guidelines to avoid the abuse of position as public employees, and to control the access and use of Montpelier Police Department (MPD) and/or City resources such as computer systems, technology and equipment. This policy provides specific guidelines and rules governing the use of the professional office of personnel and all Department equipment including, but not limited to, vehicles, uniform items, badges and ID cards, firearms, phones, protective equipment such as helmets and protective vests, reports (electronic or physical), Mobile Data Terminals (MDTs), Dispatch terminals, computers, laptops, department-issued phones, and other computer hardware and software, including Internet browsing, e-mail, and file transfer or download.

The continuing success of the Montpelier Police Department depends largely on public trust and confidence as the Department's reputation and integrity necessitates adhering to the highest standards of ethical conduct. For example, MPD requires computer systems to perform tasks essential to its operation and the safety and welfare of employees and the residents of the City. The use of these computerized systems shall be in compliance with laws, policies and service provider licensing agreements and contracts. All authorized data, information or software contained in any Department computerized information system is considered the property of MPD. The Department will provide members with access to these systems and share information with non-Department members in compliance with Department policies, First Amendment considerations and applicable laws.

II. Policy: It is the policy of this agency to safe guard the profession, both the City's and Department's reputations, and all City and Department equipment and information. Supervision should allow for reasonable recreational use of the internet for personnel so

long as it does not impede work or assigned duties, however under no circumstances shall an employee use any department resource for inappropriate or unauthorized personal use or to provide or share information to another party for inappropriate, unauthorized or personal use. All personnel shall also take great care to ensure their positions as public servants are not used for personal gain, advantage or benefit.

III. Definitions:

A. Announce Office: Informing a person or group of one's position as a City employee or police officer.

B. Department Resource: For purposes of this policy, Department Resources refer to any item belonging to the City or Department.

C. Computerized Information or Account System: Refers to the various systems the Department utilizes in the performance of official duties. These accounts refer to database systems such as NCIC, Valcour, Planit, communications platforms, mobile phones, etc.

D. Escaping Incident: Using one's position of public trust to escape a potential infraction (e.g. avoiding tickets, investigation or arrest).

E. Need-to-know: Having access to information which is necessary to perform official duties.

F. Personal Use: Items or information used for personal gain or for situations beyond the scope of an employee's official duties. Some examples of personal use include, but are not limited to, using equipment for preferential treatment (e.g. identifying one's position for favor or to escape incident), accessing database information beyond having an official need-to-know, accessing information for personal gain for civil litigation or a criminal investigation, accessing information so to meet or develop an interpersonal relationship, and accessing information to harass or target.

G. Recreational Use: Utilizing Department computers and internet access for leisure activities not related to City or Department business such as paying personal bills, accessing music, movies or videos, sending emails from personal accounts, accessing personal social media sites, doing homework or studying, etc.

IV. Procedure:

A. Personnel shall not announce their office for the purposes of personal gain or escaping incident. MPD acknowledges officers may elect to carry their service weapon while off duty and may elect to take police action in emergency situations when off duty. As such, sworn personnel may identify themselves to on-duty law enforcement personnel when they take or offer to assist first responder personnel in taking police action, and/or for safety purposes (e.g. if an officer is armed and is involved in a traffic stop and should alert the investigating officer).

B. Personnel may take advantage of promotions or discounts advertised to the general public or profession (e.g. savings, coupons or discounts for first responders or veterans, etc.).

C. All Department resources are expected to be used for official City business. Allowable uses of computer systems and information include the following:

1. Performance of job functions;
2. Communication of information in a timely manner;
3. Coordinate meetings for City or Department business;
4. Communicate with other City departments; and
5. Communicate with outside organizations or individuals as required to perform an employee's job function.
6. Reasonable recreational internet use which does not impede work or assigned duties.

Prohibited uses of systems and information include, but are not limited to, the following:

1. Illegal activities;
2. Slander;
3. Defamation;
4. Political endorsements;
5. Commercial activities;
6. Installation of non-business software including games or entertainment software;
7. Using any City resource, software or hardware to conduct unapproved non-city business or for inappropriate personal purposes such as pornographic or hate-based websites;
8. Without prior approval and/or written permission from MPD and/or the City, the computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g. viruses, Trojan horse programs, etc.) or other unauthorized materials. Further, at all times users are responsible for the professional, ethical and lawful use of computer systems. Personal use of computers and these systems are privileges that may be revoked any time; or
9. To violate any other City policy.

D. Personnel shall follow the user agreements or requirements of all database systems.

E. Reports and systems containing confidential or sensitive information shall be controlled. Access for individuals without a work-related need to know is prohibited. Physical reports with such information shall be destroyed by a shredder when the reports are no longer needed per legal requirements and/or Department policy.

F. The computer network, administrative access, subscriptions, computerized information and account systems, etc. are the property of City and/or MPD and are to be used for legitimate business purposes. Users are provided access to these networks and systems for the performance of their jobs and shall not use them for personal use. All users have a responsibility to use computer resources and the internet in a professional, lawful and ethical manner. Abuse of the computer network or the internet may result in disciplinary action including possible termination, civil liability and criminal liability.

G. Any information obtained through any computerized information or account system (or report) may contain confidential data/information. Members who access information through a Department computerized information or account system will be held responsible should such information be used in violation of the law and/or Department policy, rules or regulations. Personnel will also ensure the proper disposal of such information as prescribed.

H. Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources. As such, users must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, uploading or downloading large files, accessing streaming audio and/or video files, and spending excessive amounts of time on the Internet for recreational purposes such as shopping, utilizing personal social media, playing games or engaging in online chat groups, or otherwise creating unnecessary loads on network traffic associated with unauthorized uses of the internet. Supervision may allow for reasonable recreational use of the Internet, however such use shall not impede assigned work or duties. The Department reserves the right to limit such usage if it observes or perceives individual or systemic abuses towards this privilege.

I. Unless expressly authorized to do so, personnel are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to MPD. Unauthorized dissemination of such materials may result in disciplinary action and/or civil and criminal penalties under state and federal laws.

J. Personnel shall not access physical or electronic folders, information, confidential files or cases, etc. without a valid need-to-know. This includes disciplinary folders and active or closed investigations, cases or calls for service regarding other personnel or personal acquaintances.

K. Users expressly waive any right of privacy in anything they create, store, send or receive using the Department's computer equipment or internet access. Users consent to allow Department and/or City personnel access to and review of all materials created, stored, sent or received through any Department network or Internet connection and on any Department or City resource.

L. The Department has the right to conduct auditing checks, monitor and log any and all aspects of its computerize information or account systems, including but not limited to, monitoring internet sites used by users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users on Department or City equipment or by means of Department or City email systems.

M. The Department may conduct random audits and checks of internet usage, resources, or computerized information or account systems, etc., but it shall not specifically target or single out any personnel for any monitoring or audits of system activity without a valid reason. The Department shall document any audits it conducts and notify personnel of the audit.