Information Technology Use

341.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the proper use of Department information technology resources, including computers, electronic devices, hardware, software and systems.

341.1.1 DEFINITIONS

Definitions related to this policy include:

Computer system - All computers (on-site and portable), electronic devices, hardware, software, and resources owned, leased, rented or licensed by the Vancouver Police Department or City of Vancouver that are provided for official use by its members. This includes all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the Department.

Hardware - Includes, but is not limited to, computers, computer terminals, network equipment, electronic devices, telephones, including cellular and satellite, pagers, modems or any other tangible computer device generally understood to comprise hardware.

Software - Includes, but is not limited to, all computer programs, systems and applications, including shareware. This does not include files created by the individual user.

Temporary file, permanent file or file - Any electronic document, information or data residing or located, in whole or in part, on the system including, but not limited to, spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, messages, photographs or videos.

341.2 POLICY

It is the policy of the Vancouver Police Department that members shall use information technology resources, including computers, software and systems, that are issued or maintained by the Department in a professional manner and in accordance with this policy.

341.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to emails, texts or anything published, shared, transmitted or maintained through file-sharing software or any Internet site that is accessed, transmitted, received or reviewed on any Department computer system.

The Department reserves the right to access, audit and disclose, for whatever reason, any message, including attachments, and any information accessed, transmitted, received or reviewed over any technology that is issued or maintained by the Department, including the Department email system, computer network and/or any information placed into storage on any Department system or device. This includes records of all keystrokes or Web-browsing history made at any Department computer or over any Department network. The fact that access to a database, service or website requires a username or password will not create an expectation of privacy if it is accessed through Department computers, electronic devices or networks.

Employees may not be asked or required to disclose login information for their personal social networking accounts or to provide access to their personal social networking accounts unless otherwise allowed under RCW 49.44.200.

341.4 RESTRICTED USE

Members shall not access computers, devices, software or systems for which they have not received prior authorization or the required training.

341.4.1 SOFTWARE

Members shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes in accordance with the software company's copyright and license agreement.

To reduce the risk of a computer virus or malicious software, members shall not install any unlicensed or unauthorized software on any Department computer. Members shall not install personal copies of any software onto any Department computer.

When related to criminal investigations, software program files may be downloaded only with the approval of the Information Technology (IT) staff and with the authorization of the Chief of Police or the authorized designee.

No member shall knowingly make, acquire or use unauthorized copies of computer software that is not licensed to the Department while on Department premises, computer systems or electronic devices. Such unauthorized use of software exposes the Department and involved members to severe civil and criminal penalties.

Any other introduction of software requires prior authorization from IT staff and a full scan for malicious attachments.

341.4.2 HARDWARE

Access to technology resources provided by or through the Department shall be strictly limited to Department-related activities. Data stored on or available through Department computer systems shall only be accessed by authorized members who are engaged in an active investigation or assisting in an active investigation or who otherwise have a legitimate law enforcement or Department-related purpose to access such data. Any exceptions to this policy must be approved by the Chief of Police or the authorized designee.

341.4.3 INTERNET USE

Internet usage is permissable under the guidelines outlined under the City of Vancouver Policy 605.6 - Use of Computers, Emails, Internet and Technological Resources.

See attachment: 341 COV Policy 605 - Use of Computers_Email_Internet_and Other Electronic Resources.pdf

Internet sites containing information that is not appropriate or applicable to Department use and which shall not be intentionally accessed include, but are not limited to, adult forums, pornography, gambling, chat rooms and similar or related Internet sites. Certain exceptions may be permitted

with the express approval of the Chief of Police, or the authorized designee as a function of a member's assignment.

341.5 PROTECTION OF AGENCY SYSTEMS AND FILES

All members have a duty to protect the computer system and related systems and devices from physical and environmental damage and are responsible for the correct use, operation, care and maintenance of the computer system.

Members shall ensure Department computers and access terminals are not viewable by persons who are not authorized users. Computers and terminals should be secured, users logged off and password protections enabled whenever the user is not present. Access passwords, login information and other individual security data, protocols and procedures are confidential information and are not to be shared. Password length, format, structure and content shall meet the prescribed standards required by the computer system and shall be changed at intervals as directed by IT staff.

It is prohibited for a member to allow an unauthorized user to access the computer system at any time or for any reason. Members shall promptly report any unauthorized access to the computer system or suspected intrusion from outside sources (including the Internet) to a supervisor.

341.6 INSPECTION OR REVIEW

Reasons for inspection or review may include, but are not limited to, computer system malfunctions, problems or general computer system failure, a lawsuit against the Department involving one of its members or a member's duties, an alleged or suspected violation of any Department policy, a request for disclosure of data, or a need to perform or provide a service.

The IT staff may extract, download or otherwise obtain any and all temporary or permanent files residing or located in or on the Department computer system when requested by a supervisor or during the course of regular duties that require such information.