216. PERSONAL COMMUNICATION DEVICES

RICHFIELD POLICE DEPARTMENT POLICY

Effective Date:	08/09/16
No. of Pages:	3
Serial Number:	10-116
Authority:	Chief Jay Henthorne

NOTE: This policy is for internal use only and does not enlarge an employee's civil or criminal liability in any way. It should not be construed as the creation of a higher standard of safety or care in an evidentiary sense, with respect to third party claims. Violations of this policy, if proven, can only form the basis of a complaint by this Department, and then only in a non-judicial administrative setting.

I. PURPOSE

The purpose of this policy is to establish guidelines and standards for the use of personal communication devices (PCDs), issued by the City of Richfield or personally owned, while on-duty or when used for authorized work purposes.

II. POLICY

It is the policy of the Richfield Police Department to use computers and PCDs in the course of police operations to enhance productivity, effectiveness and communications. The Richfield Police Department allows employees to utilize department-issued PCDs and to possess personally owned PCDs in the workplace subject to certain limitations. Any PCD used while on-duty, or used off-duty in a manner reasonably related to the business of the Department, will be subject to monitoring and inspection consistent with the standards set forth in this policy.

The inappropriate use of a PCD while on-duty may impair officer safety. Additionally, employees are advised and cautioned that the use of a personally owned PCD either on-duty or after duty hours for business-related purposes may subject the employee and the employee's PCD records to civil or criminal discovery or disclosure under applicable data practices laws and rules of civil or criminal procedures.

All police personnel using a PCD for business-related purposes will do so in a professional manner prescribed in accordance with this policy. Willingly or intentionally falsifying information while using a PCD is strictly prohibited under Department policy and State Law. Employees shall not copy data or distribute data without proper authorization.

Employees who have questions regarding the application of this policy or the guidelines contained herein are encouraged to seek clarification from supervisory personnel.

III. DEFINITIONS

For purposes of this Policy, the terms defined in this section have the meaning given them:
PERSONAL COMMUNICATION DEVICE (PCD): Devices including, but not limited to, mobile telephones, personal digital assistants (PDAs), wireless capable tablets and similar wireless two-way communications and/or portable Internet access devices. PCD use includes, but is not limited to, placing and receiving calls, text messaging, blogging and microblogging, emailing, using video or camera features, playing games and accessing sites or services on the Internet.

IV. OWNERSHIP, PRIVACY

Employees shall have no expectation of privacy with regard to any communication made with or stored in or through PCDs issued by the Department. Personnel shall have no expectation of privacy in their location should the device be equipped with location detection capabilities. The use of any department-provided PCD, computer, Internet service, telephone service or other wireless service is without any expectation of privacy that the employee might otherwise have in any communication,

including the content of any such communication. Communications or data reception on personal, password-protected, web-based e-mail accounts and any other services are subject to monitoring if department equipment is used.

In accordance with this policy supervisors are authorized to conduct a limited administrative search of electronic files without prior notice, consent, or a search warrant on department-issued PCDs. Administrative searches can take place for work-related purposes that may be unrelated to investigations of employee misconduct and, as reasonably practicable, will be done in the presence of the affected employee. All such searches shall be fully documented in a written report.

V. PROCEDURE

DEPARTMENT-ISSUED PCD

Depending on an employee's assignment and the needs of the position, the Department may at its discretion issue a PCD. Department-issued PCDs are provided as a convenience to facilitate authorized work-related business but may also be used for limited personal use. Such devices and the associated telephone number shall remain the sole property of the Department and shall be subject to inspection or monitoring (including all related records and content) at any time without notice and without cause.

Employees provided with a department-issued PCD are responsible for the device's proper care (see Policy #129, Accountability for Department Equipment).

Officers should not normally provide the number of their department-issued PCD to members of the public. Exceptions may be made when immediate future contact between an officer and a victim, witness, or other person may be important. Personnel shall not provide the PCD number of any other member of this agency to a member of the public without that member's authorization.

Personnel shall not use department-issued PCDs to share messages or visual or audio recordings with social or other print or electronic media that would undermine departmental integrity, or bring disrepute to the department or its members.

Any use of a Department-issued PCD perceived to be illegal, harassing, offensive, to reflect badly on the Richfield Police Department, or interfere with normal police operations will be considered a violation of this policy.

PERSONALLY OWNED PCD

Employees may carry a personally owned PCD while on-duty subject to the following conditions and limitations:

a) Carrying a personally owned PCD is a privilege, not a right.
b) The Department accepts no responsibility or liability for loss of or damage to a personally owned PCD.
c) The device should not be used for work-related purposes except in exigent circumstances, (e.g. unavailability of radio communications). Employees have a reduced expectation of privacy when using a personally owned PCD in the workplace and have no expectation of privacy with regard to any department business-related communication.
d) The device shall not be utilized to record or disclose any business-related data, including photographs, video or the recording or transmittal of any data or material obtained or made accessible as a result of employment with the Department, without the express authorization of the Chief of Police or the authorized designee.
e) All work-related documents, e-mails, photographs, recordings or other public records created or received on a member's personally owned PCD should be transferred to the Richfield Police Department and deleted from the member's PCD as soon as reasonably practicable.

Work-related information including data created, received, recorded or stored on a personally owned PCD in the course of department duties is considered government data subject to the requirements of the Minnesota Government Data Practices Act and discovery obligations (Minn. Stat.§ 13.01 et seq.).

SUPERVISOR RESPONSIBILITIES

Supervisors should ensure that members under their command are provided appropriate training on the use of PCDs consistent with this policy. Supervisors should monitor, to the extent reasonably practicable, PCD use in the workplace and take prompt corrective action if an employee is observed or reported to be improperly using a PCD. An investigation into improper conduct should be promptly initiated when circumstances warrant.

USE WHILE DRIVING

The use of a PCD while driving can adversely affect safety, cause unnecessary distractions and present a negative image to the public. Officers operating emergency vehicles should restrict the use of these devices to matters involving official duties and, where reasonably practicable, stop the vehicle at an appropriate location to use the PCD (Minn. Stat. § 169.475).

Except in an emergency, employees who are operating non-emergency vehicles shall not use a PCD while driving unless the device is specifically designed and configured to allow hands-free use (Minn. Stat.§ 169.475). Hands-free use should be restricted to business-related calls or calls of an urgent nature.

INTERNET USE

Internet access is available as a resource for work-related assistance. Limited personal use of the Richfield Police Department's computer system, including e-mail and the internet, is permitted. Internet use must be professional and shall not be used to visit inappropriate sites or send inappropriate messages (unless necessary for investigatory purposes).

Accessing or transmitting materials (other than those required for police business) that involves the use of obscene language and images, sexually explicit materials, or messages that disparage any person, group, or classification of individuals is prohibited whether or not a recipient has consented to or requested such material.

EMAIL

The Richfield Police Department issued email is the primary means of communication within the Department. It shall be used in a professional and responsible manner. Employees shall not permit unauthorized persons to use the Department's email system.

SECURITY

Transmission of business-related electronic messages and information on PCDs shall be treated with the same degree of propriety, professionalism, and confidentiality as official written correspondence or verbal communication.

No Employee shall access or allow others to access any file or database unless that person has a need and a right to such information.

Employees shall not install or disable any device, hardware or software on a department-issued PCD without prior authorization from their supervisor and IT staff. Repairs to department-issued PCDs shall be made by Department authorized and approved sources.

Employees are responsible for maintaining the confidentiality of passwords and the security of their assigned PCDs. Employees shall inform their supervisor of any password breach or any other security or data breach.

To avoid breaches of security, employees shall log off any PCD that has access to the agency's computer network, electronic mail system, the internet, or sensitive information whenever they leave their workstation.

By Order Of:

Chief of Police