	LOWER MERION TOWNSHIP POLICE DEPARTMENT **Ardmore, Pennsylvania**
	Policy 3.17.8

Subject:		Distribution:
J-NET User Role and Access		**All Personnel**
Date of Issue:	Expiration Date:	Rescinds:
06-07-2018	**Until Amended or Rescinded**	**Policy 3.17.8 (06-01-2014)**
References:		
CALEA: N/A; PLEAC: 2.4.2		
By Authority of:		
		**Superintendent of Police**

PURPOSE

The purpose of this policy is to establish guidelines that adhere to the JNET (Pennsylvania Justice Network) user roles and defined user agreements.

POLICY

The Pennsylvania Justice Network (JNET) is the Commonwealth's primary public safety and criminal justice information broker. JNET's integrated justice portal provides a common online environment for authorized users to access public safety and criminal justice information. This critical information comes from various contributing municipal, county, state, and federal agencies. JNET provides this agency with the ability to conduct secure investigations in a web-based environment. Access to JNET's secure web portal is dependent upon policy, secure connectivity, and role-based entitlements. It shall be this Department's policy that all authorized JNET users adhere to all JNET Policies and/or user agreements.

PROCEDURE

A. JNET User Authorization and Role Determination

1. Authorization for JNET Access shall be determined and approved by the appropriate Unit Commander.

2. JNET Access is a multi-tiered application with different levels. Officer roles shall be determined by job assignment. The two roles currently assigned are "Criminal History" and "Criminal Justice". Generally, all JNET approved employees will be assigned the "Criminal Justice" role. Officers assigned to the Investigations Unit and Platoon Investigators will be granted the "Criminal History" role. Any query in criminal history must associate with an investigation (incident report) to satisfy the audit procedures and JNET policy.

B. Account Set Up, End-User Agreement and Testing

1. Once approved for JNET Access, officers shall undergo training and pass the JNET testing procedure for account completion. Officers will then be issued a password to provide controlled access.

2. JNET users shall only access the system through authorized terminals.

3. JNET users shall read and sign the online user agreement and/or any other JNET access requirements.

C. JNET User Agreement and Use

1. Each JNET User Shall:

a. Obtain authorization and complete all required training.

b. Comply with all JNET policies, procedures and standards.

c. Not permit, and shall report unauthorized access or use of JNET information.

d. Use secure electronic communications when communicating JNET derived data.

e. Not use “backdoor” (any unapproved) methods to access the JNET portal. Only the access point provided by this agency shall be used.

f. Safeguard all JNET information of which you have knowledge or to which you have access, this includes, JNET information, which could be cached, stored, and/or printed during your JNET session.

g. Use JNET for **OFFICIAL PURPOSES ONLY.** JNET data shall not be used for personal use under any circumstances. Personal use is defined as querying or viewing records that are not relevant to your official purposes. Personal use of JNET data will result in disciplinary action.

h. JNET information may be distributed within the police department on a “NEED TO KNOW” basis for legitimate and official law enforcement purposes. Dissemination of JNET derived data to the public or other unauthorized recipients is strictly prohibited.

i. Report suspected cases of misuse by other employees.

j. Cooperate with misuse investigators from: JNET Office, Pennsylvania State Police, Pennsylvania Office of the Inspector General, Pennsylvania Office of the Attorney General, Federal Bureau of Investigation; and/or this agency.

D. JNET Facial Recognition System (JFRS) Access and Use ***(PLEAC 2.4.2 k)***

1. JFRS compares uploaded facial images with those existing in the WebCPIN and PennDOT databases.

2. Access and use of JFRS shall be limited to those officers authorized by the Investigations Unit Commander.

3. To access and utilize JFRS, JNET users must first have the Criminal History role and complete the JFRS training segment in JNET.

4. Appropriate use of JFRS results (images) is covered by the JNET User Agreement and JNET Privacy Policy.

E. Policy Violations

1. JNET user's access may be suspended or revoked for violating any part of the JNET User Agreement or any other department policy.

2. Unauthorized use will result in disciplinary action

RESPONSIBILITY

It is the responsibility of all supervisory personnel to ensure that all personnel under their immediate supervision comply with this policy.

This page intentionally left blank.