New York State University Police

NEW YORK STATE UNIVERSITY POLICE	Subject **Computer and Internet - Acceptable Use Policy**	General Order Number
	DCJS Standards	Effective Date **March 2008**
		Revision Date **August 2012**
	Approval **Enrico D'Alessandro, Chief**	

I. PURPOSE

The purpose of this General Order is to establish guidelines with respect to employees' usage of computer hardware, computer software, and the Internet**.**

II. RESPONSIBILITY

It is the responsibility of every member of the New York State University Police at Morrisville State College to ensure that the guidelines contained within this document are observed and adhered to.

III. PROCEDURES

NEW YORK STATE UNIVERSITY POLICE at MORRISVILLE STATE COLLEGE COMPUTER AND INTERNET – ACCEPTABLE USE POLICY

This Policy Is the Current Guide Which Outlines the Safe and Acceptable Use for ***All*** *Computer Equipment, Which is Owned or Operated by the New York State University Police at Morrisville State College:*

This policy is meant to include all computer hardware such as: laptops, desktops, clients, servers, network drives, thumb drives, monitors printers, etc.

This policy is also meant to include all software packages such as: Traffic and Criminal Software (TraCS), Spectrum Justice System (SJS), Automated Issuance Management System (AIMS), License Plate Reader (LPR) Software, Livescan Server System, eJustice Portal, and any other such search engine or database, in which access has been gained by use of the New York State University Police ORI number.

INTRODUCTION

The New York State University Police at Morrisville State College Acceptable Use Policy specifies policy for the use of information resources and information technology systems. ***Enforcement of this acceptable use policy is consistent with the policies and procedures of this organization***.

Being informed is a shared responsibility for all users of New York State University Police information systems. Being informed means, for example:

- Knowing these acceptable use policies and other related rules and policies,
- Knowing how to protect your data and data that you are responsible for,
- ***Knowing how to use shared resources without damaging them,***
- Knowing how to keep current with software updates,
- Knowing how to report a virus warning, a hoax or other suspicious activity, and
- ***Participating in training.***

POLICY

Compliance with this policy is ***mandatory*** for all members of the New York State University Police at Morrisville State College. This policy applies to all New York State University Police information, computer systems and data that are used for official New York State University Police business regardless of its location.

1. Authorized Use

Users ***must use department owned or leased hardware*** to access Internet resources or searchable databases, which are associated with the ORI number of the New York State University Police at Morrisville State College. Accessing such resources or other restricted information from ***personal equipment is not authorized***. In addition, accessing such resources or other restricted information ***for non-business related purposes is not authorized*** by the New York State University Police at Morrisville State College.

Users ***must not*** use other users' passwords, userids, or accounts, or attempt to capture or guess other users' passwords. In addition, users ***must not*** hide their identity for malicious purposes or assume the identity of another user.

2. Privacy

All user files may be subject to access by authorized employees of the New York State University Police at Morrisville State College during the course of official business. ***Accordingly, users should have no expectation of privacy and their activity may be monitored.***

3. Restricted Access

Users must not attempt to access restricted files or portions of operating systems, security systems, or administrative systems to which they have not been given authorization. Accordingly, ***users must not*** access without authorization: electronic mail, data, programs, or information protected under state and federal laws. ***Users must not*** release another person's restricted information.

4. Proper Use of Resources
Users should recognize that computing resources are limited and user activities may have an impact on the entire network. ***Users must not:***

▪ misuse email - spread email widely (chain letter) and without good purpose ("spamming") or flood an individual, group, or system with numerous or large email messages ("bombing")

▪ Misuse business hardware - to stream audio, video or real time applications for non-business related purposes such as: use of a stock ticker or internet radio.

5. Protecting Information and Shared Resources
Users must:

▪ Follow established procedures for protecting files, including managing passwords, using encryption technology, and storing back-up copies of files.

▪ ***Protect the physical and electronic integrity of equipment,*** networks, software, and accounts on any equipment that is used for New York State University Police business in any location.

• ***Not visit non-business related websites***

• Not open email from unknown senders or email that seems suspicious.

• Not knowingly introducing worms or viruses or other malicious code into the system nor disable protective measures ie: antivirus, spyware firewalls.

• Not install unauthorized software.

• Not send restricted or confidential data over the Internet or off your locally managed network unless appropriately encrypted.

• ***Not connect unauthorized equipment or media***, which includes but is not limited to: laptops, thumb drives, removable drives, wireless access points, pdas, and mp3 players.

6. Civility
Users must not harass other users using computer resources or make repeated unwelcome contacts with other users. ***Users must not display material that is inappropriate in an office environment*** for example, material which is clearly inconsistent with the policies of the New York State University Police at Morrisville State College.

7. Applicable Laws
Users must obey ***all local, state, and federal laws*** including laws on copyright and other intellectual property laws.

GLOSSARY

Encryption –The cryptographic transformation of data to render it unintelligible through an algorithmic process using a cryptographic key.

Locally Managed Network – Safeguards in place:

• On a secure server

• Restrict administrator rights

Restricted Information – pertains to information which is not public information, but can be disclosed to or used by organization representatives to carry out their duties, so long as there is no legal bar to disclosure.

IV. ADDITIONAL INFORMATION

This Policy was originally put into place in March of 2008.
This Policy was updated in May of 2010
This Policy was updated in August of 2012
If you need any further training or assistance please notify your Supervisor.

Chief Enrico D'Alessandro	
LT David DuChene	
LT Eric Collins	
LT Paul Field	
Investigator Francis Lust	
Officer Conor Duffy	
Officer Luke Learned	
Officer Gregory Sanborn	
Officer Philip Netzband	
Officer Richard White	
Officer David Wilber	
Officer Nicole Wright	
Secretary Christine Maricle	
Parking Service Attendant Jean Hyde	