The University of North Carolina Greensboro Police Department

General Order 1.5.1	Computer Equipment Use

Purpose and Scope

The purpose of this policy is to outline the acceptable use of computer equipment and information technology resources provided by The UNCG Police Department to its employees and/or authorized affiliates. Inappropriate use exposes the University to risks, including breach of personal computer security, exposure of restricted data, compromise of network systems/services, detriments to technology performance, and legal liability.

Policy

In support of its mission, the department and/or the University provides technology and electronic information systems, including but not limited to computer equipment, mobile devices, software, operating systems, storage media, and network accounts providing electronic mail, web browsing, and file transfer, that are the property of the University and/or department. These systems are to be used only for business and academic purposes in serving the interests of the UNCG Police Department or the University in the course of normal operations.

A. Definitions

- Chain Letters or Pyramid Schemes - One of a sequence of letters, each recipient in the sequence being requested to send copies to a specific number of other people.
- Computer Equipment - The necessary items used to process electronic data. This includes desktop computers; laptop computers; tablets; cell phones; power units; components such as mouse, keyboard, camera, speakers, cables, etc.
- Fair Use - Legal concept that allows the reproduction of copyrighted material for certain purposes without obtaining permission and without paying a fee or royalty. Purposes permitting the application of fair use generally include review, news reporting, teaching, or scholarly research.
- Mass Email Messages - Refers to the act of sending an email to many people in one single operation.
- Mobile Data Terminal (MDT) - Computer equipment (e.g., laptop) used in a vehicle to communicate with the Communications Center and utilize computer based police systems.

- Mobile Devices - A piece of portable computer equipment that can connect to the internet, e.g., department issued cell phones, tablets, etc.
- Network Related Resources - Refer to computer data, information, or hardware devices that can be easily accessed from a remote computer through a local area network (LAN) or enterprise intranet.
- Network Traffic - Computer network communications that are carried over wired or wireless networks between hosts.
- Port or Security Scanning - Method for determining which ports on a network are open. Security scanning is an inspection of the potential points of exploitation on a computer or network to identify security holes.
- Security Breaches - A security breach is any incident that results in unauthorized access to computer data, applications, networks or devices.
- Storage Media - Computer equipment that receives and retains electronic data for applications and users and makes the data available for retrieval.
- Third-party Vendor Application - A company or entity with a direct written contract to provide products or services to your customers on your organization's behalf.
- Umstead Act - Passed originally in 1939, was enacted by the North Carolina legislature to prevent state-owned agencies from selling merchandise in direct competition with private merchants. The act was passed in an attempt to prevent the government from competing with its tax paying citizens.

B. General Use and Ownership

It is the responsibility of every department employee and affiliate who deals with information and/or information systems to know these guidelines, and to conduct their activities accordingly.

There should be no expectation of privacy in the material stored, sent, or received when using the University network, department computer systems, mobile devices, or third-party vendor applications provided by the University and/or department (e.g., Google email services). For security, legal or policy compliance, quality of service, and network maintenance purposes, authorized individuals within University Information Technology Services (ITS) or the Technical Services Unit (TSU) may monitor equipment, systems, and network traffic. General content review will not be undertaken, although monitoring of content may occur for the reasons stated above.

Employees are responsible for exercising good judgment regarding the use of computer devices and information systems. Use of computer equipment is permitted, with the following restrictions:

- The use is lawful under federal or state law.
- The use complies with applicable University policies and guidelines.

- The use is not prohibited by Board of Governors or University policies, including rules regarding academic integrity, harassment (including sexual harassment), and discrimination on the basis of any federally protected characteristics.
- The use does not result in commercial gain or private profit (other than allowable under University intellectual property policies) and does not violate the North Carolina Umstead Act.
- The use does not violate federal or state laws or University policies on copyright, trademark, or software licensing.
- The use does not intentionally or unintentionally overload University computing equipment or systems, or otherwise harm or negatively impact the system's performance or the support of such systems.
- Communications originating from the user are identified as such and the user assumes responsibility for all communication originating from equipment or accounts assigned to that user. In the case of security breaches related to accounts or equipment belonging to the user, the user should contact their supervisor immediately to quickly respond and correct the situation.
- The use does not attempt to circumvent system security or in any way attempt to gain or provide unauthorized system or network access.
- All resources and data accessed are protected by the user according to the standards set forth in the University ITS Security of Networks and Networked Data Policy and University ITS Data Classification Policy (see list at end of this policy).
- The use must not interfere with an employee's job performance or activities.

C. Unacceptable Use

Under no circumstances is an employee of the UNCG Police Department authorized to engage in any activity that is illegal under local, state, federal, or international law, while utilizing computer equipment, and/or network related resources.

Employees may be exempted from "unacceptable use" restrictions during the course of their legitimate job responsibilities (e.g., IT administrators for the department performing duties or undercover investigations).

The list below provides a framework for activities that fall into the category of unacceptable use. It is not all inclusive, but is intended to give examples of the type of activities that are prohibited.

Prohibited System and Network Activities

The following activities are strictly prohibited, with noted exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the user or device.

- Unauthorized replication or use of copyrighted material, except where such copying qualifies as "Fair Use."
- Exporting software, technical information, encryption software or technology in violation of international or regional export control laws. Legal counsel and appropriate management should be consulted prior to export of any material that is in question.
- Intentionally or recklessly introducing or transmitting destructive or malicious programs such as viruses into the network or networked devices.
- Revealing account passwords to others or allowing use of accounts by others. This includes family and other household members.
- Using computer equipment to actively engage in procuring or transmitting material that is in violation of state/federal law or university policies.
- Originating from any university account or equipment commercial offers of products, items, or services in violation of the Umstead Act.
- Effecting security breaches or disruptions of network communication such as accessing data of which the employee is not an intended recipient, logging into a server or account that the employee is not expressly authorized to access, attempting to intercept others' passwords, or impersonating another user.
- Port scanning or security scanning is strictly prohibited, with one exception. Individual host port/security scanning is allowed only with permission from the administrator of the target host. Authorized ITS employees and TSU are permitted to port/security scan as part of their normal job duties.
- Executing any form of network monitoring which will intercept data not intended for the employee's host. Authorized ITS employees and TSU are permitted to monitor network traffic data as part of their normal job duties.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with or denying service to any user.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, by any means, locally or via the network.

Prohibited Email and Communications Activities

The following activities are strictly prohibited, with no exceptions:

- Forwarding restricted University email to unauthorized recipients.
- Sending unsolicited mass email messages without proper unit authorization, posting unsolicited and inappropriate list/web/news group messages, including the sending of "spam" (junk email) or other commercial advertising material to individuals.
- Any form of harassment via means such as email, instant messaging, telephone or paging, whether through language, frequency, or size of messages.

- Unauthorized use/deliberate disguising of the sender or forging of email header information. Alteration of content of an email message originating from another sender with intent to deceive.
- Hosting an email transport/relay service outside of supported and authorized ITS systems.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or otherwise misuse email resources.
- Creating or forwarding "chain letters" or "pyramid schemes" prohibited by law.
- Activities in violation of the University ITS Electronic Records Retention Policy (see list at end of this policy).

D. Enforcement

Penalties may be imposed under one or more of the following: The University of North Carolina at Greensboro ITS policy, departmental policy, North Carolina law, or the laws of the United States (see list at end of this policy).

Minor infractions of this policy or those that appear accidental in nature are typically handled informally by electronic mail or in-person discussions. More serious infractions are handled via formal procedures. In some situations, it may be necessary to suspend account privileges to prevent ongoing misuse while the situation is under investigation.

Offenses which are in violation of local, state, or federal laws may result in the restriction of computing privileges, and will be reported to the University and appropriate law enforcement authorities.

E. Computer Equipment Service and Support

24 hour computer equipment service is available year round from TSU. Computer equipment users should submit a web support ticket on the employee intranet or contact the on-call TSU personnel for all system, hardware, or software problems. Users may be instructed to take any mobile computer equipment (e.g., laptop, MDT, tablet, etc.) to TSU during regular business hours, if the problem does not interfere with required job duties.

F. Computer Equipment Replacement or Repair

In the event the mobile data terminal (MDT) needs to be replaced after normal business hours, a spare computer will be available. The user will record in their vehicle inspection form that the replacement MDT was checked out. At the end of their tour of duty, the user will return the MDT and note the return on their vehicle inspection form.

In the event a mobile device needs to be repaired and/or serviced a spare device may be available through TSU.

In the event computer equipment is damaged due to negligence and/or improper use the cost of such repair and/or replacement of the device could be the responsibility of the individual it is assigned.

G. Leave and Separation from Employment

When an employee resigns, retires, is separated from employment with UNCG Police, takes leave of 30 days or greater, or for any other reason at the discretion of the Chief of Police the employee will surrender all computer equipment. TSU will remove certain employee's access rights to the UNCG network and all UNCG Police systems and files. After the equipment is surrendered, the Logistics Officer will notify TSU of the following:

- Equipment issued (Tag#)
- Officers issued to
- Date of Issue
- Date of return
- Equipment replaced

H. Links to Related University ITS Policies

- Acceptable Use of Computing and Electronic Resources Policy
- Data Classification Policy
- Enterprise Systems Policy
- Standards for Computer and Related Technology (Supported Products List)
- Electronic Records Retention Policy
- Wireless Communications Policy
- University ITS Security of Networks/Networked Data Policy