The City University of New York

535 East 80th Street
New York, NY 10075

January 26, 2010

MEMORANDUM

To: All CUNY Employees

From: Senior Vice Chancellor Frederick P. Schaffer
Associate Vice Chancellor Brian Cohen

Re: New Amendments to New York Laws on protecting employee private information, including social security numbers

---

We write to advise you of recent amendments to New York State laws adding provisions protecting individuals' private information, including social security numbers. This memo summarizes the key aspects of these laws and the CUNY Revised Information Technology Security Procedures. The University is committed to protecting the personal private information of our students, faculty and staff. It is the continuous responsibility of all University employees to prevent unauthorized disclosure of private information—regardless of the form in which the information is stored—electronic or paper. Anyone who has experienced the loss or theft of private personal information knows the difficulties it can cause.

Summary of new laws

A new section (96-a) of the NY Public Officers Law became effective January 1, 2010. The section prohibits the State from intentionally communicating to the general public or otherwise making available to the general public in any manner an individual's social security number unless otherwise required by law. Among other things, the section also prohibits the State from requiring an individual to provide a social security number unless certain safeguards are in place such as requiring the transmission of a social security number over the internet only when there is a secure connection or the social security number is encrypted. In addition, the law prohibits the State from including an individual's social security number, except the last 4 digits, on any materials to be mailed to that individual, or in any electronic mail that is copied to third parties, unless State or federal law requires the social security number to be on the document mailed.

An amendment to New York's Labor Law Section 203-d also prohibits an employer from communicating or displaying an employee's private information, including social security numbers, unless otherwise required by law.

Under Section 203-d, an employer may not unless otherwise required by law:
(a) Publicly post or display an employee's social security number
(b) Visibly print a social security number on any identification badge or card (including time cards)
(c) Place a social security number in files with unrestricted access, or
(d) Communicate an employee's personal identifying information to the general public.

The section defines "personal identifying information" as including--social security numbers, home address or telephone numbers, personal email addresses, internet identification name or passwords, parent's surname prior to marriage, or driver's license numbers.

CUNY IT Security Procedures on Protecting Private Information

The University's Revised Information Technology Security Procedures ("IT Security Procedures") protect private personal information as mandated by State and federal laws. The IT Security Procedures, last revised and issued on March 26, 2009, include the requirements of these new laws (see security.cuny.edu under Info Security Policies)

Under the IT Security Procedures, access to Non-Public University Information must be restricted to individuals on a need to know basis who are full-time and regular part-time employees (with certain limited exceptions). (Section II)

Employees who are permitted access must protect the Non-Public University Information by using approved passwords and encryption. (Section III, 10-13). **Social security numbers must not be stored, transported, or taken home on portable devices (e.g. laptops, flash drives) of any type without specific approval of both the Vice President of Administration or the equivalent at the College or in the Central Office department and the University Information Security Officer. Where approval is granted, the information MUST BE ENCRYPTED AND PASSWORD PROTECTED.** (III.13)

Although the transfer of encrypted social security numbers on portable devices is permitted, we strongly urge you not to do so because of the security risks that may be involved. Likewise, paper records containing social security numbers should remain at the office in a secure location not accessible to the public.

Employees who violate the law and/or the IT Security Procedures may be subject to disciplinary action.