COMMUNITY COLLEGE SYSTEM OF NEW HAMPSHIRE
INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

I. Policy Statement

Information technology resources are used by individual employees, students, and other persons affiliated with the Community College System of New Hampshire

x

7.1.2 Installing software or hardware on or modifying the software or hardware configuration of a CCSNH-owned IT asset without appropriate authorization from CCSNH Chief Information Officer.

7.1.3 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 CCSNH.

7.1.4 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CCSNH or the end user does not have an active license is strictly prohibited.

7.1.5 Violation of federal, state or local laws and regulations regarding access and use of information resources (e.g., Family Education Rights and Privacy Act, Gramm-Leach-Bliley Act, Computer Fraud and Abuse Act, code of professional conduct, etc.).

7.1.6 Except for Internet browsing, accessing data, a server or an account for any purpose other than CCSNH educational or business purposes, even if access is otherwise authorized, is prohibited.

7.1.7 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate CCSNH official should be consulted prior to export of any material that is in question.

7.1.8 Introduction of malicious programs into the networI1 (i)-2essrIiIihe net4.364 (.g.)]TJ

7.1.11 Using any kind of program, script, or command designed to interfere with a user's computer or network session or collect, use or distribute another user's personal information.

7.1.12 Port scanning, security scanning and executing any form of network monitoring that will intercept data not intended for the IT User's host.

7.1.13 Circumventing user authentication or security of any host, network or account.

7.1.14 Introducing honeypots, honeynets, or similar technology on the CCSNH network.

7.1.15 Interfering with or denying service to any user other than the IT User's host (for example, denial of service attack).

7.1.16 Providing information about, or lists of, CCSNH employees or students except as expressly authorized.

7.2 Email and Communication Activities

CCSNH faculty and staff must use their assigned CCSNH email address for all email communication to ( )Tj [(( )Te)4 a(s)-1 ((a)4 (ndo t)-2 (he)4 (r)3 (fr)3 (f)3 vi)-2 (c)4 (i)-12 (a)4 (l)-
addresses.

hei CCSNH tec(nol)-2 (og)-10 (y)20 ((r)-7 (e)4 (s)-1 ou(r)3 cz)-6 (e)4 (s)
ca(h)26 (a)6 (((h)26 ()-6 ir)-5 (c)6 (o)2 (mmu)-8 ne)]TJ -0.004 Tc 0.00

orterpy-16 eridsesf ndy-1.-1 (t)-16 (y-16 po)-14 e.