Vermont Department of Public Safety
Policy and Procedure
GUIDELINES FOR GENERAL USE OF SYSTEMS OR INTERNET SERVICES

1. General Guidelines

1.1 Employees with access to systems or the Internet have the responsibility not to disclose their access codes or passwords.

1.2 No employee shall send e-mail that is, or appears to be, sent from another employee's e-mail or that attempts to mask identity.

1.3 State employees must conform to reasonable professional standards for use of Internet services as detailed in this guideline. This includes a prohibition against any activity that impairs operation of any state computer resource. Such activities include, but are not limited to, sending junk mail or chain letters, inserting computer viruses or mass mailings via e-mail.

1.4 Employees must respect intellectual property rights at all times when obtaining information over the Internet. Copyrighted or licensed information shall be used only with full legal right to do so.

1.5 Use of the Internet is for State business. The only exception is for personal use that **fully** complies with the limited personal use described by this policy. Any use that is not for State business or authorized limited personal use consistent with this policy may result in revocation Internet access, other appropriate administrative action, or disciplinary or corrective action.

1.6 Use of agency systems or printers for offensive or disruptive purposes is prohibited. This prohibition includes profanity, vulgarity, sexual content or character slurs.

1.7 Inappropriate reference to race, color, age, gender, sexual orientation, religions, national origin or disability is prohibited.

1.8 State agencies have the right to monitor the systems and Internet activities of employees. Monitoring may occur, but is not limited to, occasions when there is a reason to suspect that an employee is involved in activities that are prohibited by law, violate State policy or regulations, or jeopardize the integrity and/or performance of the computer systems of State government.

Monitoring may also occur in the normal course of network administration and trouble-shooting, or on a random basis.

1.9 Use of fee-for-service providers is not allowed unless the necessary approvals and funding have been obtained in advance. An employee who obligates a State agency to pay for services without prior approval may be held personally liable for those costs and may be subject to disciplinary action up to and including dismissal.

1.10 Prohibited activities also include, but are not limited to the following: Lobbying public officials or asking others to lobby in their behalf, printing and/or distributing information from the Internet that is obscene, potentially offensive, harassing or disruptive. Using or allowing others to use State Internet services or e-mail accounts to conduct transactions or advertising for a personal profit making business is strictly forbidden.

Agencies must ensure that systems administrators and technicians involved in monitoring, or who otherwise have access to systems and records that contain information that is subject to statutory, regulatory, or common law privilege or obligation to limit access, are appropriately trained on the requirement to respect such privilege or confidentiality and directed to do so.