Sentencing Guidelines Commission
ADMINISTRATIVE POLICY

USE OF INTERNET

SUBJECT: Use of Internet Systems

AUTHORIZING SOURCE: RCW 42.52 Washington State's Ethics in Public Service Law Ethics Law), and WAC 292-110-010, Use of State Resources.

EFFECTIVE DATE: April 24, 2000

APPROVED BY: _____
Executive Director

PURPOSE:

This policy outlines the Sentencing Guidelines Commission's requirements for the use of computing resources, information technologies, and networks owned or managed by the Sentencing Guidelines Commission (SGC). This includes the Internet system. Internet access and services are provided to employees of the Sentencing Guidelines Commission for the sole purpose of assisting them in performing official duties.

SCOPE:

This policy applies to all SGC employees who use computing resources, information technologies, and networks owned or managed by the Sentencing Guidelines Commission. All such individuals, by virtue of their use of SGC computer resources and information technologies, accept the responsibility for using these resources only for appropriate SGC activities.

APPROPRIATE USE:

Sentencing Guidelines Commission computer resources, information technologies, and networks may be used for legitimate SGC purposes only. Internet access and services are provided for official Sentencing Guidelines Commission business activities.

INAPPROPRIATE USE:

Sentencing Guidelines Commission computer resources, information technologies, and networks, including Internet access shall not be used for the following prohibited activities.

APPROVED
Executive Ethics Board
Date: 9/20/05

1. Accessing the Internet for personal business, personal interest or any other non Sentencing Guidelines Commission business use. This includes, but is not limited to:

- Ordering or selling items on the Internet, except as specifically approved by SGC business purposes;
- Participating in any online contest, promotion, or sweepstakes;
- Participating in non-business related chat/forum groups, list services, or newsgroups;
- Transmitting political material and/or engaging in political activities that violate state law (state law prohibits the use of state facilities or public resources for the purposes of assisting in an election campaign; and
- Gambling, or soliciting money for religious or political causes, or for non Sentencing Guidelines Commission's events.

2. Creating, posting, transmitting, or voluntarily receiving:

- Obscene or pornographic material;
- Offensive, libelous, threatening, or harassing material; and
- Degrading statements based on race, national origin, gender, sexual orientation, age, disability, religious, or political beliefs.

3. Using hypertext to link SGC web sites to other Internet/World Wide Web (WWW) sites whose content may be in violation of the mission or policies of the Sentencing Guidelines Commission.

4. Using E-mail products other than those provided and supported by the SGC. The prohibited products include (but are not limited to) Hotmail, Juno, and AOL. Checking personal e-mail using SGC networks and communication lines is also prohibited because of the risk of compromising the security and integrity of state and information software.

5. Using disk storage facilities, free or otherwise, provided by some vendors over the Internet.

6. Using state provided equipment or Internet connectivity to launch or perpetuate denial of service attacks against any server or network system; or as a tool to illegally gain access to another computer or network system.

EXCEPTIONS:

Notwithstanding the prohibitions outlined in the "Inappropriate Use" section of this policy statement, SGC employees may make occasional but limited personal use of computer systems only if:

1. There is no cost to the state; and
2. The use of state resources does not interfere with the performance of the officer's or employee's official duties;

APPROVED
Executive Ethics Board
Date: 9/20/05

3. The use is brief in duration and does not disrupt or distract from the conduct of state business due to volume or frequency; and

4. The use does not compromise the security or integrity of state information or software.

PRIVACY:

System users are responsible for maintaining appropriate access restrictions for their files, as well as protecting their passwords. An employee who knowingly allows another person to use his or her username or password may be found responsible for any inappropriate use on the part of that person.

SANCTIONS:

Evidence of illegal activities or policy violations will be turned over to the appropriate authorities as soon as possible after detection.

REVISED 5/30/01

APPROVED
Executive Ethics Board
Date: 9/20/05