

You will not access the internet via any means without pre-approved, written permission from your Residential Community Transition Team (RCTT). This includes wireless connection devices, phone line, cellphone, tablet, laptop, or communications software or hardware. If permitted, you will only use for the purposes approved by the RCTT. Noncompliance will be reported to the court and may result in consequences.

You must adhere to the following rules if you are permitted to access the internet.

- Only access the websites that are approved by your RCTT. If the purpose of internet access is for seeking employment, the only exception allowed is any website you are redirected to when attempting to apply for a job posted on an approved website (e.g., using monster.com and being redirected to the company website to complete an application).
- Log any site visited, including websites that may have been accidentally visited. Submit the log weekly to your case manager or as directed.
- The computer must be located in an area of your house visible to anyone who enters the home from the primary entrance and the screen positioned so that it is visible to anyone in that room.
- Unless given permission by the court, you must be in the presence of an approved chaperone at all times when using a device with internet access.
- The computer must be equipped with a new or clean hard-drive that has been authorized by an Internet Technology (IT) employee/contract staff at the Special Commitment Center (SCC).
- Any additions, modifications, or changes to the system must be pre-approved in writing by your RCTT.
- There will be no extra hard-drives, modems, Wi-Fi, or other forms of communication software or hardware installed on the computer, in your possession, or located at your home and readily available to you.
- Only the internet browser that is approved by your case manager may be used.
- The “Pop-Up” blocker will be engaged.
- Do not browse the internet in “private”, “stealth”, or “incognito” mode.
- Do not browse the internet using a proxy server or any other software that hides, conceals, or otherwise alters your computers identification or IP address.
- Neither you nor anyone else will delete/erase, alter, or attempt to delete or alter your internet browser history, cache, temporary internet files, and/or cookies without the consent of a RCTT member.
- Compliance/accountability reports will be emailed on a weekly basis to your case manager at:

- Immediately terminate internet use if any website you access or material viewed violates or potentially violates either the rules or court order and notify your RCTT of the incident.

Email account

You may maintain one email address which you will provide to your RCTT along with both your login and password information. The address can be used for both personal and job related emails.

Your email account is subject to verification and review by any member of your RCTT at any time. You will NOT delete any email without the consent of a member of your RCTT.

Peripheral devices

Any approved device will not employ encryption technology.

Any data storage device (e.g., flash memory drive, CD-RW, floppy disc, etc.) must be approved by your RCTT/Special Commitment Center IT prior to your purchase or use. Any data storage device must remain in your possession and not be possessed or accessed by a third party without the consent of your RCTT, with the exception of your RCTT reviewing your data storage device to monitor compliance.

You will not delete any information, file, or program from the data storage device without the approval of your RCTT.

ACKNOWLEDGEMENT

I fully understand what is expected and the possible consequences of any failure to comply with these rules. I understand I will be subject to polygraphs regarding my adherence to the rules. I must keep a signed copy of the Less Restrictive Alternative Internet Rules.

Name	Signature	Date
Case manager	Signature	Date
Civil Commitment Unit employee	Signature	Date

The contents of this document may be eligible for public disclosure. Social Security Numbers are considered confidential information and will be redacted in the event of such a request. This form is governed by Executive Order 16-01, RCW 42.56, and RCW 40.14.

Distribution: **ORIGINAL** - Case manager file
COPY - Supervised individual, Sex Offender Treatment Provider, SCC representative, Imaging file