



SOCIAL MEDIA AND ELECTRONIC DEVICE MONITORING AGREEMENT

Boxes checked are applicable to the individual under the Department's jurisdiction identified in this document.

- Must provide a complete and accurate inventory of all computers, computer-related equipment, and communications devices and services including cellular/smartphones, tablets, Personal Digital Assistants (PDAs), electronic pagers, backup systems, and services below.

Type <small>(e.g., smartphone, computer)</small>	Manufacturer/ Make	Model number	Serial number	Passcode

- Inventory must be complete, accurate, and current at all times. The individual is prohibited from using or accessing any electronic or communication device or service not reported and specifically approved for use by the Department or its designee.
- Will not use or own any device which allows internet access other than those authorized by the Department and listed on this document (e.g., satellite dishes, PDA, electronic game, web television, internet appliances, cellular/smart phones).
- Must allow the case manager to install computer monitoring/filtering software on any computer used by the individual.
- Must inform other people who use the individual's devices that the devices are subject to searches pursuant to the condition of supervision.
- Individual is approved to use the following marked item(s):
 - Web browsing
 - Email - all email accounts must have prior approval
 - Interpersonal communication (e.g., chatting, texting, instant messaging)
 - Producing web content (e.g., website, social networking site pages including Facebook/Twitter, YouTube, podcasting, blogging, vlogging)
 - Internet-related phone communication (e.g., Voice Over Internet Protocol)
 - File sharing (e.g., including, but not limited to, Peer-to-Peer, Internet Relay Chat, attachments to emails, iTunes)
- Prohibited from purchasing, playing, registering, or participating in any online gaming without the prior written permission of the Department or its designee.
- Must provide the Department or its designee with all usernames and user passwords for email, electronic bulletin boards, chats, instant messaging, newsgroups, user groups, and peer-to-peer file sharing programs authorized by the Department for use. If password protection is required on any systems or files used for work purposes, the password will be provided upon request of the Department or its designee.
- Will not possess an unauthorized computer (i.e., any computer that has not been disclosed or approved by the Department).
- Permitted to use computer systems at the educational facility where the individual is enrolled for education-related purposes only.
- Permitted to use computer systems at the place of employment for employment purposes only.
- Fully responsible for all material, data, images, and information found on owned computer or any devices subject to monitoring/search at all times.

