STATE OF WASHINGTON DEPARTMENT OF CORRECTIONS	APPLICABILITY **REENTRY/FIELD** FACILITY/SPANISH MANUALS		
	REVISION DATE 1/12/22	**PAGE NUMBER** 1 of 6	**NUMBER** **DOC 380.260**
POLICY	**TITLE** **SOCIAL MEDIA AND ELECTRONIC DEVICE MONITORING FOR SUPERVISION**		

REVIEW/REVISION HISTORY:

Effective: 5/2/19
Revised: 1/12/22

SUMMARY OF REVISION/REVIEW:

Updated terminology throughout

APPROVED:

Signature on file

CHERYL STRANGE, Secretary
Department of Corrections

12/29/21
Date Signed

REFERENCES:

DOC 100.100 is hereby incorporated into this policy; DOC 280.100 Acceptable Use of Technology; DOC 280.510 Public Disclosure of Records; DOC 420.365 Evidence Management for Work/Training Release; DOC 420.390 Arrest and Search; DOC 420.395 Evidence/Property Procedures for Field; DOC 460.130 Response to Violations and New Criminal Activity; DOC 460.135 Disciplinary Procedures for Work Release; DOC 850.030 Relationships/Contacts with Individuals

POLICY:

I. The Department has established procedures for the use of internet social media and monitoring/filtering software as a tool in the supervision and case management of individuals assigned to Reentry Centers, partial confinement, or community supervision.

II. For the purposes of this policy:

A. Monitoring of internet social media involves unconcealed use (e.g., use of an account which identifies the user as a Department employee) to review an individual's internet social media content as a part of general case management. This level of engagement includes no interaction between the employee and any other user.

1. For Department imposed conditions, only internet social media content that is considered public domain data (i.e., open to the public) will be monitored.

B. Investigation using internet social media involves unconcealed use to review an individual's internet social media content for approved information gathering if there is reasonable cause to believe the individual has committed a new crime or violated a condition of confinement/supervision. This level of engagement may include interacting with other internet social media users.

III. Exceptions to allow the use of an account which does not identify the user as a Department employee or concealed use of internet social media for case management require approval from the appropriate Assistant Secretary/designee through the chain of command.

IV. This policy does not cover use of social media sites for community engagement or an employee's personal use of social media while off duty.

DIRECTIVE:

I. General Requirements

A. Internet social media accounts used for case management will comply with DOC 280.100 Acceptable Use of Technology.

B. Only Department-approved monitoring/filtering software will be used for case management activities.

C. Employees will comply with all Department security and confidentiality requirements and related Terms of Service and Privacy policies.

D. Information obtained through monitoring and/or investigations will only be used for purposes of case management, supporting allegations for violations, and maintaining public safety.

E. Computer and internet social media use may be restricted, but not prohibited, unless ordered by a court or Indeterminate Sentence Review Board (Board).

F. No authorization is required for online searches of public domain data outside internet social media (e.g., Google, Bing).

G. Before using internet social media or monitoring/filtering software for case management activities, authorized employees must complete Department approved training on their use.

H. Before being given access to a social media application, authorized employees must accept the conditions established by the third party provider for the social account application.

II. Responsibilities

A. The following employees are authorized to monitor and/or investigate individuals assigned to Reentry Centers, partial confinement, or community supervision through internet social media and use of monitoring/filtering software:

1. Case managers
2. Community Corrections Specialists
3. Community Corrections Supervisors (CCSs)
4. Field Administrators
5. Reentry Center Administrator
6. Regional Administrators
7. Assistant Secretaries for Community Corrections and Reentry

B. Employees will not:

1. Use information obtained through monitoring/investigating internet social media use for unauthorized purposes.

2. Monitor and/or investigate an individual's internet social media activity:

   a. While the employee is off duty, or
   b. Using unauthorized means, including personal accounts, internet service providers, devices, and/or software.

3. Have contact with individuals under Department jurisdiction through social media beyond what is required in the performance of official Department duties per DOC 850.030 Relationships/Contacts with Individuals.

4. Look up an individual's internet social media profile solely because the individual is under Department jurisdiction.

5. Modify any Department-approved internet social media account, including changing the user name or using an alias.

6. Collect or maintain information on an individual's political, religious, or social views, associations, or activities unless there is a legitimate public safety purpose.

III. Monitoring

A. Internet social media and monitoring/filtering software will only be used for monitoring purposes as follows:

1. Case managers will monitor conditions that order the monitoring of internet social media, the use of monitoring/filtering software, and/or restriction on the use of internet social media by:

   a. A court or the Board, or
   b. The sending state, for individuals being supervised in Washington State under the Interstate Compact.

2. Case managers may impose a Department condition for internet social media monitoring, use of monitoring/filtering software, and/or restriction on the use of internet social media for individuals:

   a. With a current sex offense.

   b. With a prior sex offense that directly involved internet use or the use of a computer, computer related equipment, or communications device and service.

   c. On partial confinement other than a Reentry Center (e.g., Family and Offender Sentencing Alternative, Graduated Reentry).

B. For individuals being monitored through internet social media or monitoring/ filtering software, regular intervals for monitoring will be established. Monitoring frequency will comply with any requirements outlined in the condition, when applicable. Monitoring will be documented in chronological entries in the electronic file.

C. When monitoring/filtering software is used, the individual must complete and sign DOC 11-080 Social Media and Electronic Device Monitoring Agreement, which includes a complete and accurate inventory of all electronic devices they own/access.

1. Failure to declare a device will be addressed as a violation per DOC 460.135 Disciplinary Procedures for Work Release or DOC 460.130 Response to Violations and New Criminal Behavior when the device can reasonably be determined to have been used by the individual. The device will be added to the individual's inventory, and monitoring/filtering software will be installed.

2. Monitoring/filtering software will not be used on publicly accessible devices (e.g., internet cafes, public libraries, individual's employer).

D. Monitoring and/or filtering software must allow for:

1. Conducting initial and periodic reviews.

2. Identification of prohibited data and software changes once the monitoring/filtering software is installed.

3. Confirmation that the monitoring software is functioning correctly.

4. Detection of attempts to circumvent the monitoring software.

IV. Investigations

A. Use of internet social media for pre-sentence investigations and risk assessment reports ordered by a court is allowed without CCS approval.

B. With CCS approval, internet social media may be used for investigation purposes for any individual assigned to a Reenry Center, partial confinement, or community supervision.

1. The requesting employee must specify the reason for the request. The approval will specify the approved duration of use, which will not exceed 10 business days.

2. The CCS will document the approval, reason, and approved duration in a chronological entry in the individual's electronic file.

V. Evidence

A. If information gathered through internet social media or monitoring/filtering software will be used as evidence of a violation, the case manager will authenticate and validate the information in one or more of the following ways:

1. Self-admission
2. Screen shots
3. Polygraph
4. Account profile owner and internet protocol (IP) address identification information
5. Corroborating information
6. Electronic metadata
7. Digital Exchangeable Image File Format (EXIF) data, for photographs
8. Electronic devices
9. Email addresses
10. Supplemental reports (e.g., law enforcement, change of custody, transcripts)

B. Reentry Center infractions will be addressed per DOC 460.135 Disciplinary Procedures for Work Release. Violations of supervision will be addressed per DOC 460.130 Response to Violations and New Criminal Activity.

C. Information retained by Department employees as evidence of violations and/or new criminal activity will be collected, managed, stored, and retrieved per DOC 280.510 Public Disclosure of Records, DOC 420.365 Evidence Management for Work/Training Release, DOC 420.395 Evidence/Property Procedures for Field, and DOC 420.390 Arrest and Search, as applicable.

DEFINITIONS:

The following words/terms are important to this policy and are defined in the glossary section of the Policy Manual: Monitoring and Filtering Devices, Public Domain Data, Social Media. Other words/terms appearing in this policy may also be defined in the glossary section.

ATTACHMENTS:

None

DOC FORMS:

DOC 11-080 Social Media and Electronic Device Monitoring Agreement