1.3. A.10 Staff Use of State Technology and Electronic Equipment

I Policy Index:

Date Signed:	***05/09/2016***
Distribution:	***Public***
Replaces Policy:	***N/A***
Supersedes Policy Dated:	***01/02/2016***
Affected Units:	***All Units***
Effective Date:	***05/09/2016***
Scheduled Revision Date:	***November 2016***
Revision Number:	***12***
Office of Primary Responsibility:	***DOC Administration***

II Policy:

Department of Corrections staff members will use state technology at their disposal in an appropriate manner.

III Definitions:

Electronic Equipment:
For the purposes of this policy, electronic equipment is any mobile communication device, two-way radio, Smartphone/Remote Access Device (RAD) (includes but is not limited to Blackberry, iPhones, and Androids) lap top, tablet, non-stationary audio and/or video recording equipment (which includes hand-held video camera, still/digital camera, camera phone, tape recorder, other image or voice capturing devices, etc.).

Social Media:
Web-based technology that allows interactive dialogue and includes but is not limited to, print, broadcast, digital and online services, such as blogs, collaborative projects, content communities and social networking sites. Social media sites include but are not limited to Face book, LinkedIn, MySpace, Plaxo, Twitter, Tumblr, Instagram, Google and blogs, as well as video and photo- sharing sites such as Flickr and YouTube.

State Technology:
Telephone (including landline and wireless/mobile services) and computer services, including internet, intranet and email owned or leased by the State of South Dakota.

Security Perimeter:
Fences and/or walls (including the exterior wall of a building) that provide for the secure confinement of offenders within a facility. All entrances and exits of a security perimeter are under the control of facility staff, thereby preventing an offender from leaving the facility unsupervised or without permission.

Senior Security Officer:
The Deputy Warden at the South Dakota State Penitentiary, Mike Durfee State Prison and the South Dakota Women's Prison. The Senior Security Officer is responsible for the same duties at ancillary units that fall within the supervision of the main facility.

Staff Member:
For the purposes of this policy, a staff member is any person employed by the DOC, full or part time, including an individual under contract assigned to the DOC, an employee of another State agency assigned to the DOC, authorized volunteers and student interns.

IV Procedures:

1. Staff Member Use of State Technology:

A. Staff members' use of state technology will be in accordance with all applicable DOC, Bureau of Information and Telecommunications (BIT) and Bureau of Human Resources (BHR) policies.

B. The use of state technology by staff will occur only with the general knowledge and consent of the Secretary of Corrections, Warden or Director.

1. Any unauthorized or inappropriate use of state technology by a staff member is grounds for disciplinary action, up to and including termination.

2. Staff members should not expect privacy or confidentiality when using state technology.

2. Prohibited Uses of State Technology:

A. The use of state technology by staff for the following uses is strictly prohibited:

1. As part of or furtherance of any illegal activity.

2. For sending, receiving, storing, accessing or recording any image which is lewd, obscene or pornographic, except for investigative purposes or part of a staff member's official duties.

3. To photograph, videotape, record, broadcast, or transmit a visual image or audio recording of any person without their express written consent, unless for an authorized purpose within the scope of the staff member's duties.

4. Uses that are in any way disruptive or harmful to the reputation or business of the state, reflect unfavorably on the state, destroy confidence in the operation of the state, or adversely affect public trust in the state (See DOC policy 1.1.C.1 *Code of Ethics*).

5. Furthering, engaging in, or conducting non-state business (commercial or personal business activities).

6. Promotion of political or religious activities or non-agency sanctioned fund-raising.

7. To engage in wagering, betting or gambling.

8. Harassment, threatening, stalking, illegal discrimination or the disparagement of others.

9. For the receipt, storage, display or transmission of material that is, or may be reasonably regarded as violent, discriminatory, racist or sexually explicit; including but not limited to any depiction, photograph, audio recording or written word except for investigative purposes or part of a staff member's official duties.

10. To engage in excessive instant messaging, participation in chat rooms or playing recreational computer games.

11. To facilitate the unauthorized release of protected confidential or personally identifying information pertinent to an offender or staff member for unauthorized purposes.

B. When in doubt about the appropriate use of state technology, staff should consult their supervisor for clarification.

3. Maintenance of State Technology:

A. Maintenance of state technology is primarily provided by the Bureau of Information and Telecommunications (BIT), which provides the DOC with database services and network data storage. The DOC may enter into contract with private technology providers for database services, data storage and access to software.

1. The provider will ensure the maintenance of the system and/or software, and the availability, security and reliability of information stored on databases it manages.

B. Staff is responsible for immediately reporting any issues/problems, including suspected breaches in the security of a DOC database or unauthorized access to DOC data/information to their supervisor.

C. Staff is responsible for removing/deleting any unnecessary or outdated files assigned to them and notifying their supervisor of any outdated files they may be aware of which they do not have permission to modify/delete.

D. Staff is responsible for the security of any removable, rewritable CD, DVD, Universal Serial Bus (USB) flash drive, zip drive, thumb drive or other removable data storage device used to store DOC related data.

1. Information originating from a DOC network, database, drive or file that contains personally identifiable information not in the public domain and if improperly disclosed, could be used to steal a person's identity, violate the individual's right to privacy, or otherwise bring harm to the person, will not be transferred or saved to any removable data storage device without proper authorization.

4. Staff Member Use of Personal Electronic Equipment at Work:

A. The Secretary, Warden, Director or designee may limit a staff member's access and use of personal electronic equipment during work hours.

B. Staff members may use/possess personal electronic equipment during work hours under the following conditions:

1. The personal electronic equipment does not negatively interfere with the performance of the staff member's job duties.

2. It is understood the DOC is not responsible for any staff member's personal electronic equipment that becomes damaged, lost or misplaced.

3. Staff members will not use personal electronic equipment in a manner that is considered by their supervisor to be disruptive or that negatively impacts the staff member's ability to adequately perform their assigned work duties.

4. When in doubt about the appropriate use of personal electronic equipment at work, staff will consult their supervisor for clarification.

C. Staff members bringing any electronic equipment (includes state owned/issued Remote Access Device (RAD)) inside the secure perimeter of a DOC facility housing offenders must have prior approval from the Warden, Senior Security officer or designee.

1. Electronic equipment not authorized by the Warden, Senior Security officer or designee must be left at the control room or stored in a secure location outside the secure perimeter.

2. Staff is not permitted to photograph or visually record offenders with personal electronic equipment. Exceptions may be granted when such activity is for official purposes or the material generated is for official use.

a. Use or possession of unauthorized wireless miniature/micro-cameras that can be concealed within clothing or other objects for the purpose of capturing a visual recording of unauthorized images or photos of offenders or other material by a staff member within a DOC facility is prohibited.

3. Staff authorized to possess a RAD within the security perimeter will ensure the RAD is password protected, has a lockout feature enabled after 10 failed password attempts, and an inactivity timer set for a maximum of 15 minutes.

5. Lost/Damaged Electronic Equipment:

A. Staff will immediately report any lost, damaged or stolen state owned or leased electronic equipment to his/her supervisor. In the case of a lost or stolen state issued RAD, staff will:

1. Immediately notify BIT, and

2. Change the Active Directory password, and

3. Notify the cellular company providing service to the RAD to have it deactivated.

B. Staff will immediately report any electronic equipment (personal or state owned) or data storage device that is lost or otherwise unaccounted for within the secure perimeter or on the grounds of a DOC owned or leased facility, or is lost or unaccounted for while the staff member is supervising offenders (community service, emergency response, etc.)

C. If the initial report is made verbally, the staff member will follow up with an Informational Report to their supervisor.

D. If the report involves state owned or leased electronic equipment, the staff member's supervisor will forward the report to the appropriate senior level supervisor as soon as possible.

6. Staff Member Use of Social Media:

A. The Warden, Director, Secretary of Corrections or designee may grant individual staff members approval to use state technology and equipment to create blogs, micro blogs, wikis, social networks containing DOC related information, or to officially participate (post/contribute or monitor) social media sites hosted on the technology infrastructure of the State of South Dakota/DOC or Internet on behalf of the DOC during work hours. Such activity is limited to approved purposes.

B. The DOC may limit authorized staff's connection and exchange of information to specified social media websites. Questions regarding the appropriateness of a social media site will be directed to the staff member's supervisor. Approval may be based on whether the content of the site is consistent with and supports the mission, vision and values of the DOC.

C. Staff member use of state technology and equipment while representing the DOC on social media or participation in social media on behalf of the DOC will be consistent with state and federal law, as well as applicable DOC, BHR and BIT policy (See *BIT Social Media policy*).

D. An appropriate level of professionalism will be maintained by staff members accessing, creating, posting/contributing social media on behalf of the DOC with state technology and equipment. Staff conduct will be consistent with the mission of the DOC (See DOC policy 1.1.A.1 *Mission, Vision and Values*) and will not violate the standards of staff conduct as described in DOC policy 1.1.C.1 *Code of Ethics.*

1. Staff will not post/contribute copy, save, transfer, divulge or otherwise release information or content generally considered proprietary, restricted or confidential by the DOC, or violate the state's privacy or confidentiality laws. Information contained on social media sites is widely accessible and difficult to retract. Such information is typically considered public record. The same standards of conduct apply to social media platforms as apply to traditional forms of communication such as e-mails. Questions regarding information that may be considered confidential should be directed to the staff member's supervisor.

2. Staff will not be disrespectful toward fellow staff members or offenders while posting/contributing to social media.

3. Staff will not release personally identifiable information that is not in the public domain and, if improperly disclosed, could be used to steal a person's identity, violate the individual's right to privacy or otherwise bring harm to the person.

    a. The provisions contained within SDCL §§ 24-2-20 and 26-11A-30 apply toward the release of information pertaining to an offender.

    b. Staff will not post photographs or video material that identify an offender or staff member without proper permission and informed consent granted by the offender (and parent or guardian if the offender is under the age of 18) or staff member, as required by DOC policy (See DOC policy 1.1.A.4 *Relationship with News Media, Public and Other Agencies*) and state law.

4. Staff will not engage in conduct or post/contribute information that reflects unfavorably on the DOC and/or the state, or that may destroy confidence in the operation of the DOC or state, or adversely affect the public trust in the DOC or state (See DOC policy 1.1.C.1 *Code of Ethics*).

5. Staff posting/contributing content within social media will not claim to represent the DOC or its policies or comment on pending litigation or legal matters involving the DOC or state without proper authorization.

6. Staff engaged in social media activities on behalf of the DOC will not use vulgar, obscene, offensive language or terms, conduct personal attacks against fellow staff or offenders, or negatively target a specific individual(s) or group(s). Posts will be appropriate and meaningful and the staff member's conduct will be professional and respectful.

E. Violation by any staff member of any of the above standards may be grounds for disciplinary action, including and up to termination from employment (See DOC policy 1.1.C.1 *Code of Ethics*).

F. Discussions (posted content) on DOC managed technology infrastructures will be reviewed by the DOC Communications and Information Manager or staff member authorized to manage and monitor the content of the social media site. The Communications and Information Manager or authorized staff has authority to approve or disapprove the posted content. Inappropriate material will be removed as soon as possible by the Communications and Information Manager, authorized staff member or BIT staff. Supervisors should review material posted by staff on DOC managed technology infrastructures periodically and as they deem necessary.

G. The DOC does not monitor staff personal use of social media. However, the DOC may investigate and take responsive action when it becomes aware of, or suspects staffs' conduct or communication on a social media site adversely impacts the DOC, violates applicable DOC policies, is inconsistent with the mission, vision and values of the DOC, or compromises the staff member's ability to adequately perform their assigned duties.

V Related Directives:

SDCL § 24-2-20 and 26-11A-30.

DOC policy 1.1.A.1 -- *Mission, Vision and Values*
DOC policy 1.1.A.4 -- *Relationship with News Media, Public and Other Agencies*
DOC policy 1.1.C.1 -- *Code of Ethics*

Policies - South Dakota Bureau of Personnel
BIT Social Media policy

VI Revision Log:

May 2006: New policy.
June 2007: **Revised** the definition of staff member.
May 2008: **Revised** formatting of policy in accordance with DOC policy 1.1.A.2 Policy and Operational Memorandum Management policy. **Replaced** "lock engaged" with "Key guard" in subsection (B3b of Staff Member Use of Personal Electronic Equipment at Work section) to be consistent throughout policy and **replaced** "device exists" with "function exists" in same section to be consistent throughout policy.
May 2009: **Reviewed** with no significant changes.
May 2010: **Revised** formatting of Section 1.
May 2011: **Added** "digital" and "other image or voice capturing devices," to definition of Electronic Equipment. **Added** definition of "Social Media". **Added** "or inappropriate use of" and "up to and" to Section 1 A. 2.**Added** "3. State employees should not expect privacy or confidentiality when using state resources/equipment to Section 1. A. **Added** "BlackBerry" to Section 1 A. 4.**Renumbered** Section 1 B. to 4. **Added** "B. Security Perimeter" to Section 1. **Added** "or designee" and "BlackBerry, or other electronic equipment" to Section 1 B. 1.**Removed** "state owned/leased" from Section 1 B. 1. **Added** "or other unauthorized electronic equipment" and "outside of the secure perimeter." to Section 1 B. 2. **Added** "a. Unauthorized cell phones stored in the control room or other secure location within the facility should be turned "Off" or placed on "Mute" to Section 1 B. 2. **Deleted** "Other Prohibited Uses of Electronic Equipment by staff members" and **Added** new Section 2. "Prohibited Uses of State Owned/Leased Electronic Equipment" **Moved** "When in doubt about the appropriate use of state owned/leased electronic equipment, staff members will consult their supervisor for clarification" from Section 1 C. to Section 2. B. **Deleted** "to acknowledge/record commemorate awards, retirements or other special events" from Section 3 A. **Added** "from the Warden, Superintendent or designee and the staff members supervisor" and **Deleted** "of their supervisor(s)" from Section 3 A **Added** "possess" and **Deleted** "cell phone" and **Added** "electronic

equipment" to Section 3 B. **Deleted** "1. The staff member's supervisor has given permission to use the cell phone at work." from Section 3 B. **Deleted** "cell phone" and **Added** "personal electronic equipment" to Section 3 B. 1. **Deleted** "The Warden or Superintendent must give advance authorization for personal cell phone to be taken inside of the security perimeter." from Section 3 B. 3 **Deleted** "a. Unauthorized cell phones must be left at the control room or stored in a secure location." from Section 3 B. 3. **Deleted** b. "Cell phones that are permitted within the security perimeter will have their "Key guard" engaged, if such a functions exists with the phone." from Section 3 B. **Added** "or other personal electronic equipment" and **Renumbered** B. 3. c. in Section 3 to 3. B. 2. **Added** "will not" **Deleted** "of" and **Deleted** "any other purpose". **Added** "inappropriate uses or in a manner that is disruptive or interferes with the performance of the staff member's job duties" **Deleted** "is prohibited" in Section 3 B. 3. c. and **Renumbered** to 3. B. 3. **Deleted** "Any unauthorized use of personal electronic equipment by a staff member is grounds for disciplinary action, including termination" from Section 3 C.1. **Added** "at work" to Section 3 B. 4.**Renumbered** from previous Section 3. C. 2. **Added** "state owned or leased" to Section 4 A. **Added** "Staff will immediately report any authorized electronic equipment (personal or state owned) lost within a DOC facility, on grounds owned or leased by the DOC, at a DOC work site or anywhere inmates may recover and access the lost equipment." to Section 4 B. and **Renumbered** B. to C. and C. to D. **Added** "state owned or leased" to Section 4 D.
June 2012: **Revised** the definition of Social Media. **Added** "and in accordance with all applicable DOC and DHR policies" in Section 1 A. **Added** "Director" or designee to Section 3. **Added** "or misplaced during the performance of the staff member's duties" to Section 3 B. 2. **Added** "considered" and "by their supervisor" to Section 3 B. 3. **Deleted** "With permission from" and "or designee" and **Added** "immediate" and "may limit a" and **Deleted** "may bring" and **Replaced** with "access and use" in Section 3 A. **Added** new Section 5.
May 2013: **Changed** title of policy from "Restrictions on Electronic Equipment" to "Staff Use of State Technology" **Deleted** "cell phones" and **Replaced** with "smart phone/Remote Access Device (RAD) which include Blackberrys, iPhones and Androids) labtop, tablet" in definition of "Electronic Equipment". **Added** "Tumblr, Instagram, Google and blogs" to definition of "Social Media". **Added** "Bureau of Information and Telecommunications" to Section 1 A. **Deleted** "cell phone/Blackberry" and **Replaced** with RAD throughout policy. **Deleted** "will have the "key guard" engaged" and **Replaced** with "should be password protected, have a lockout feature after 10 failed password attempts and have the inactivity timer set for a maximum of 15 minutes" in Section 1 B. 2. A**dded** 11. to Section 2 A. **Added** "or stolen" and 1-3 to Section 4 A. **Added** "create or contribute to blogs, micro blogs, wikis, social networks or other" and **Deleted** "sites" and **Replaced** with "hosted on the technology infrastructure of the State of SD/DOC or on the Internet" in Section 5 A. **Added** "authorized" in Section 5 C. **Added** "post" and "or otherwise release" and "proprietary, restricted" to Section 5 C. 1. **Added** "or comment on pending litigation or legal matters" in Section 5 C. 4. **Added** "Posts will be appropriate and meaning and staff conduct will be professional and respectful" in Section 5 C. **Added** D. to Section 5.
October 2013: **Changed** Review Date from May to November. **Deleted** "resources/equipment" and **Replaced** with "technology" in Section 1 A. 3. **Added** "(includes state owned/issued RADs)" in Section 1 B. **Deleted** a. "RADs stored in the control room or other secure location within the facility should be turned off or placed on mute" in Section 1 B. 1. **Added** "staff authorized to use/possess" in Section 1 B. 2. **Added** new Section 3. and **Renumbered** Sections that followed. **Added** "or data storage device that is lost or otherwise unaccounted for" in Section 5 B. **Deleted** "during work hours" and **Replaced** with "Approval is limited to approved sites" in Section 6. A. **Added** "contribute" "save" and "content" in Section 6 C. 1. **Deleted** "in demeanor, tone or through actions" and **Deleted** "accessing, creating" and **Replaced** with "posting/" and **Deleted** "information that may endanger the well being of fellow staff, offenders or the public" and **Replaced** with "personally identifiable information that is not in the public domain and, if improperly disclosed could be used to steal a person's identity, violate the individual's right to privacy or otherwise bring harm to the person" in Section 6 B. 2.
October 2014: **Added** "the DOC may enter into contract with private technology providers for database services, data access/storage and software" in Section 3 A. **Deleted** "BIT" and **Replaced** with "the provider" in Section 3 A. 1. **Deleted** "managed by BIT" in Section 3 B. **Moved** C. in Section 1 to Section 4. **Added** "containing DOC related information or participate (post/contribute) to and **Added** "during work hours" and **Deleted** "and for work related purposes only, i.e. conducting investigations, communicating with certain groups or individuals, located offenders who have absconded or run away" and **Replaced** with "for

approved purposes" in Section 6 A. **Added** "use of social media on behalf of the DOC" in Section 6 B. and C. **Added** "or post/contribute information" in Section 6 C. 3. **Added** "without proper authorization" in Section 6 C. 4.

November 2015: **Added** "except for investigative purposes or part of a staff member's official duties" to Section 2 A. 2. and 9. **Added** "or that negatively impacts the staff member's ability to adequately perform their assigned work duties" in Section 4 B. 3. **Added** 2. and a. to Section 4. C. **Added** D. to Section 4. **Added** "officially" and **Added** "or on the Internet" to Section 6 A. **Added** new B. to Section 6. **Added** "while representing the DOC or participating in social media" and **Added** "BIT Social Media policy" to Section 6 C. **Added** b. to Section 6 D. 3. **Added** "DOC Communications and Information Manager or staff member authorized to manage and monitor the content of the social media site" and **Deleted** "DOC" and **Added** "The Communications and Information Manager or authorized staff shall approve the posted content" and **Added** "by the Communications and Information Manager, authorized staff member or BIT" to Section 6 E.

May 2016: **Deleted** reference to STAR and the STAR Superintendent.

Denny Kaemingk (original signature on file)	*05/09/2016*
Denny Kaemingk, Secretary of Corrections	Date