POLICY TITLE: PRISONER USE OF COMPUTERS AND/OR ACCESS TO THE INTERNET **POLICY NUMBER: 24.10** **CHAPTER 24: PROGRAMS AND SERVICES**		**PAGE 1 OF 8**
STATE of MAINE **DEPARTMENT OF CORRECTIONS** **Approved by Commissioner:** Dr. Joseph R. Fitzpatrick		**PROFESSIONAL STANDARDS:** **See Section VII**
EFFECTIVE DATE: **August 24, 2017**	**LATEST REVISION:**	**CHECK ONLY IF APA [ ]**

I. AUTHORITY

The Commissioner of Corrections adopts this policy pursuant to the authority contained in Title 34-A M.R.S.A. Section 1403.

II. APPLICABILITY

All Departmental Adult Facilities

III. POLICY

It is the policy of the Department to allow approved prisoners to use Department computers and/or access authorized resources on the internet for the purposes of enhancing education and reentry planning in adult facilities as determined by the Commissioner, or designee.

IV. CONTENTS

Procedure A: Computer Use and/or Internet Access, General
Procedure B: Eligibility and Approval
Procedure C: Mandatory Conditions
Procedure D: Implementation of Prisoner Computer Use and/or Internet Access
Procedure E: Supervision and Monitoring of Computer Use and/or Internet Access
Procedure F: Audits of Computers Used by Prisoners
Procedure G: Responding to a Security Breach
Procedure H: Termination of Computer Use and/or Internet Access

V. ATTACHMENTS

Attachment A: Prisoner Computer Use and/or Internet Access by Facility
Attachment B: Prisoner Computer Use and/or Internet Access Agreement

VI. PROCEDURES

Procedure A: Computer Use and/or Internet Access, General

1. The Commissioner, or designee, shall determine the adult facilities permitted to allow eligible prisoners to use Department computers for education and/or reentry planning purposes (see Attachment A, Prisoner Computer Use and/or Internet Access by Facility list).

2. The Commissioner, or designee, shall determine the adult facilities permitted to allow eligible prisoners internet access on Department computers for education and/or reentry planning purposes (see Attachment A, Prisoner Computer Use and/or Internet Access by Facility list).

3. This policy does not pertain to prisoner use of computers and/or internet access for legal work as governed by Department Policy (AF) 24.4, Library Services, use of computers generally available to prisoners in a facility library or housing unit, or computer use by prisoners associated with a facility job.

4. A prisoner's use of a Department computer and/or access to the internet is considered a privilege and not a right.

5. The Department's Manager of Correctional Information Technology (IT) Operations, or designee, is responsible for the overall management of computer use and internet access by approved prisoners, which shall include, but is not limited to:
   a. installation and maintenance of computer hardware;
   b. installation and maintenance of computer software;
   c. installation and configuration of internet connection(s);
   d. implementation of security controls;
   e. securing and maintaining appropriate licenses;
   f. updating hardware, software, internet connections and security controls, as necessary;
   g. setting up network folders and authorizing access to appropriate internet sites;
   h. blocking access to other internet sites;
   i. ensuring that prisoners cannot use computers or the internet to access any confidential information or any Departmental sites or programs, including, but not limited to, the Department's website, PowerDMS, CORIS, etc.;
   j. maintaining a list of authorized internet sites and notifying applicable staff of any changes to the list;
   k. ensuring that prisoner user accounts, prisoner User IDs, and prisoner passwords are set-up;

l. managing prisoner user accounts to include expiration dates, size limitations, etc.;

m. ensuring appropriate staff monitor computer use and internet access by prisoners to improve service levels and prevent unauthorized computer use and/or internet access by prisoners;

n. ensuring that any security breaches related to prisoner computer use and/or internet access are reported and, if necessary, investigated;

o. ensuring that reports of investigations of security breaches are forwarded to appropriate staff;

p. overseeing audits of computer use and internet access by prisoners; and

q. providing any necessary technical assistance to staff that are responsible for supervising computer use and/or internet access by prisoners.

6. A prisoner shall not be provided direct or indirect access to staff passwords, administrative passwords, authorized codes (Login ID), staff accounts, or system manuals intended for staff use only.

7. A prisoner shall not be allowed to possess any removable data storage device (e.g., a USB drive/flash drive, floppy disk, memory stick, re-writable CD) that is not issued by Department staff for an approved education or reentry planning purpose.

Procedure B: Eligibility and Approval

1. A prisoner enrolled in a Department approved educational course may be approved for:

   a. computer use if computer use is necessary for accomplishing the required work;

   b. internet access if internet access is necessary for accomplishing the required work, including access to applicable online college resources, e.g., online writing labs, etc.; and/or

   c. a college email account if the college provides college email accounts to students for educational purposes and provided that the prisoner gives the designated facility education staff the username and password/passcode required to access the email account.

2. A prisoner may be approved for computer use and/or internet access if the prisoner is engaged in a Department approved reentry plan in which computer use and/or internet access is necessary for facilitating reentry.

3. If a prisoner meets either of the above requirements, is approved for computer use and/or internet access as part of the prisoner's individualized case plan as set forth in Department Policy (AF) 23.4, Assessment and Case Management, and signs the Prisoner Computer Use and/or Internet Access Agreement

(Attachment B), then the case manager shall modify the plan, to include, but not be limited to:

a. the purpose of the computer use;

b. the purpose of the internet access, if applicable;

c. use of a college email account, if applicable;

d. use of a USB drive/flash drive, if applicable;

e. expected duration of the prisoner's user account; and

f. any conditions in addition to the mandatory conditions.

4. A prisoner who has been approved for computer use and/or internet access as set out above may be allowed use of a USB drive/flash drive on an as needed basis in the classroom for approved education purposes, if approved in the prisoner's individualized case plan.

5. A prisoner who is classified community custody and has been approved for computer use and/or internet access as set out above may be issued a USB drive/flash drive for approved education and/or reentry planning purposes, if approved in the prisoner's individualized case plan.

6. If a prisoner is approved for computer use and/or internet access, the signed Prisoner Computer Use and/or Internet Access Agreement shall be maintained in the prisoner's Case Management Record.

Procedure C: Mandatory Conditions

1. A prisoner approved for computer use and/or internet access shall:

a. not use a computer or the internet to violate copyright laws;

b. not use a computer or the internet to harass or threaten anyone;

c. not use a computer or the internet for any other illegal activity;

d. not use a computer or the internet to commit a disciplinary violation;

e. not use a computer or the internet to access pornography;

f. not access any materials that would not be allowed to be received via the mail as set out in Department Policy (AF) 21.2, Prisoner Mail, Procedure E;

g. not upload any program or introduce any virus into any computer, system, or program;

h. not impersonate any other person, falsely represent himself or herself, or make any other false statement in connection with computer use or internet access;

i. not intentionally or negligently destroy or damage or cause a malfunction of any computer, peripheral equipment, or USB drive/flash drive; and

j. not consume food and/or beverages when using or around a computer or peripheral equipment.

2. A prisoner shall only use work stations and computers designated for prisoners.

3. A prisoner shall not access any internet site that is not authorized by the Department.

4. A prisoner shall only use a computer and/or access the internet for authorized purposes as specified in the prisoner's individualized case plan.

5. A prisoner is never authorized by his or her case plan to use a computer and/or access the internet for conducting business activities, doing legal work, writing personal letters, playing computer games, listening to music, instant messaging, accessing social media or chat rooms, or sending or receiving email other than through a college email account for educational purposes as set out in the prisoner's individualized case plan.

6. A prisoner shall not use a computer and/or access the internet to contact anyone who the prisoner has been ordered to have no contact with or who is a victim of a crime committed by the prisoner, if applicable.

7. A prisoner shall not use or possess a USB drive/flash drive unless approved in the prisoner's individualized case plan.

8. A prisoner shall not download or print documents unless authorized by the facility staff supervising the educational program or reentry planning, as applicable.

9. A prisoner is not allowed to repair or modify any computer or peripheral equipment, USB drive/flash drive, software, system, or program, except as part of a Department approved training program or when specific approval has been granted by the Department's Manager of Correctional IT Operations, or designee.

10. A prisoner is prohibited from using a computer and/or accessing the internet on behalf of another prisoner or allowing another prisoner access to his or her prisoner user account, prisoner User ID, prisoner password, or USB drive/flash drive, if applicable.

11. A prisoner is required to exit all applications and log off the computer when finished using the computer.

12. A prisoner shall be responsible for compensating the Department for any losses, costs, or damages to a Department computer, peripheral equipment, USB drive/flash drive, software, system, or program due to the prisoner's intentional act or negligence.

13. A prisoner's computer use and/or internet access is not confidential and may be viewed or otherwise monitored by appropriate staff at any time.

14. If the prisoner inadvertently accesses any site or any material that is not authorized, the prisoner is required to immediately report that access to staff supervising the program.

15. A prisoner who violates a condition may be subject to termination of approval for computer use and/or internet access, disciplinary or other administrative action, and/or criminal prosecution.

Procedure D: Implementation of Prisoner Computer Use and/or Internet Access

1. Once a prisoner is approved for computer use and/or internet access (and has signed the Prisoner Computer Use and/or Internet Access Agreement), the case manager, or other designated staff, shall notify the Department's Manager of Correctional IT Operations, or designee, who shall set up the prisoner's user account.

2. Designated education staff or the case manager, as appropriate, shall assign the prisoner a User ID and password(s), if applicable. The staff shall maintain a list of User IDs and passwords assigned to prisoners.

3. Designated education staff or the case manager, as appropriate, shall issue the prisoner a USB drive/flash drive, if applicable. The staff shall maintain a list of USB drives/flash drives issued to prisoners.

Procedure E: Supervision and Monitoring of Computer Use and/or Internet Access

1. Designated education staff or the case manager, as appropriate, shall manage computer use and/or internet access by prisoners by setting priorities on the use of the Department's computers and internet access.

2. Designated education staff or the case manager, as appropriate, shall remind the prisoner of the mandatory conditions and any additional conditions for computer use and, if applicable, internet access and/or use of a USB drive/flash drive.

3. For a prisoner who has not been issued a USB drive/flash drive, but is allowed the use of one in the classroom for approved education purposes, only designated education staff may handle the USB drive/flash drive. The staff shall maintain a signed log, which shall include the prisoner's name and MDOC number, the purpose for the use, and the date and times during which the drive is used.

4. Designated education staff or the case manager, as appropriate, shall monitor computer use and/or internet access by the prisoner to ensure appropriate use. Security staff may monitor computer use and/or internet access by the prisoner to ensure appropriate use. As part of the monitoring, staff may inspect a computer, a USB drive/flash drive, electronic files, downloaded or printed material, internet sites accessed, etc. at any time for any reason.

5. If any staff becomes aware of or suspects that a prisoner has violated any condition of computer use and/or internet access, the staff shall act immediately to stop any ongoing violation. The staff shall take appropriate action in response

to any violation, including, but not limited to, suspending the prisoner's computer use or internet access, initiating disciplinary action, and reporting the violation to appropriate staff. If criminal activity is suspected, the staff shall secure and preserve the computer, peripheral equipment, and the USB drive/flash drive, if applicable, in its current state and immediately notify the facility correctional investigative officer (detective) and/or the Shift Commander.

6. Education staff, case managers, or other designated staff shall ensure that computers are kept secured from any access by prisoners when the computers are not authorized for prisoner use.

Procedure F: Audits of Computers Used by Prisoners

1. Each facility Chief Administrative Officer, in collaboration with the Department's Manager of Correctional IT Operations, shall designate a facility staff member to be responsible for overseeing the management of computer use and/or internet access by prisoners at the facility.

2. That staff shall ensure that all computers used by prisoners are audited by facility staff at least quarterly. Auditing facility staff may request assistance from the Department's Manager of Correctional Information Technology (IT) Operations, or designee.

3. Staff conducting an audit shall document the audit and forward the results to the Department's Manager of Correctional IT Operations, or designee, at the end of each quarter.

4. The Department's Manager of Correctional IT Operations, or designee, shall compile a Department-wide report and forward the report to each facility Chief Administrative Officer and the Associate Commissioner of Correctional Programs.

Procedure G: Responding to a Security Breach

1. If any staff becomes aware of or suspects a security breach in connection with prisoner computer use and/or internet access, the staff shall immediately report the incident to the facility staff member responsible for overseeing the management of computer use and/or internet access by prisoners at the facility. That staff shall notify the facility Chief Administrative Officer, or designee, and the Department's Manager of Correctional IT Operations, or designee.

2. The Department's Manager of Correctional IT Operations, or designee, in consultation with the facility Chief Administrative Officer, or designee, shall determine the appropriate course of action.

3. If it is determined that an investigation is necessary, the Department's Manager of Correctional IT Operations, or designee, shall notify other appropriate Central Office staff, who shall assign the investigation to appropriate staff.

4. The investigating staff shall complete a report on the findings of the investigation and forward the report to the Associate Commissioner of Correctional Programs, the facility Chief Administrative Officer, or designee, the Department's Manager of Correctional IT Operations, or designee, and the Department's Director of Operations, or designee.

Procedure H: Termination of Computer Use and/or Internet Access

1. A prisoner's computer use and/or internet access shall be terminated if the prisoner is released from institutional confinement or transferred to a facility or placed in a housing unit in which the prisoner will not be immediately allowed computer use or internet access.

2. The computer use and/or internet access of a prisoner approved for computer use and/or internet access for an educational program shall be terminated if the prisoner is no longer enrolled in a course and will not be enrolled in a course in the immediate upcoming fall, winter or spring semester, as applicable.

3. The computer use and/or internet access of a prisoner approved for computer use and/or internet access for reentry planning shall be terminated if the prisoner is no longer involved in reentry planning.

4. The prisoner's Unit Team may terminate a prisoner's computer use and/or internet access for any violation of the conditions.

5. The Commissioner, or designee, may terminate a prisoner's computer use and/or internet access at any time for any reason at his or her complete discretion.

6. If computer use and/or internet access has been terminated, education staff, the case manager, or other designated staff, shall notify the Department's Manager of Correctional IT Operations, or designee, who shall cancel the prisoner's user account. If applicable, designated staff shall confiscate the USB drive/flash drive issued to the prisoner.

7. If applicable, designated education staff or the case manager, as appropriate, shall make arrangements to transfer any electronic documents created by the prisoner upon the prisoner's release from institutional confinement.

VII. PROFESSIONAL STANDARDS

None