DEPARTMENT OF CORRECTIONS

Policy Number:	**103.210**
Title:	**Electronic Communications**
Effective Date:	**4/1/22**

PURPOSE: To govern access to, and the appropriate use of, electronic communications, to meet legal requirements for access to information, and to provide adequate protection for proprietary information.

APPLICABILITY: Department-wide

DEFINITIONS:

Computing ethics – accepted conduct to be observed while using electronic communications.

Electronic communication – any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic, or photopic system.

Electronic communication equipment and technology – equipment and technology used to perform electronic communication, including, but not limited to, telephones, computers, printers, facsimile machines, pagers, mobile devices, electronic mail (e-mail), instant messaging (IM), Internet access and browsers.

Global e-mail – e-mail sent to all staff groups or combinations of all staff groups.

Instant messaging (IM) – a type of communications service enabling one to create a private chat room with another individual in order to communicate in real time over the network.

Internet – an external medium through which information or electronic mail may travel.

Levels of Internet access

Default	Access to State of Minnesota websites only.
Standard	Access to State of Minnesota websites plus a list of approved websites.
Elevated	Access to all approved site categories except those in restricted categories.

Remote e-mail access – web access to e-mail account using a portable electronic device (Smartphone, Blackberry, iPad, etc.)

PROCEDURES:

A. Employee use of electronic communications is a privilege constituting the acceptance of responsibilities and obligations that are subject to state government policies and federal, state, and local laws. Employee use of electronic communications must be legal, ethical, and respectful of intellectual property, ownership of data, systems security mechanisms, and individual rights to privacy and freedom from intimidation, harassment, and annoyance. Employees may be subject to limitations on their use of electronic communications as determined by the appointing authority based on business need. Limited and reasonable incidental employee personal use that does not result in any additional costs or loss of time or resources is permitted.

B. Employee usage

1. The scope of an employee's e-mail and Internet access is granted based on the employee's responsibilities and business need. An employee is initially granted default Internet access. An employee may request elevated Internet access through the employee's supervisor by completing the Internet/E-Mail Access Request form (attached) and obtaining the appropriate authorization. Designated security posts/work stations at each correctional facility must have computers permanently set at the standard internet access. Remote e-mail access is only granted to staff not affected by the Fair Labor Standards Act provisions and those staff in specific positions/posts off facility grounds. Signed and approved Internet/E-mail Access Request forms are retained by the information technology (IT) department.

2. The appointing authority must designate certain workstations for employees to access approved websites within the employee's access level. The appointing authority must designate one computer with standard/elevated Internet access capabilities in a common area for staff use during non-work hours. The appointing authority must post a sign at the computer stating the computer is not to be used for work-related reasons during non-work hours and the IT staff reviews computer use.

3. Access to third-party e-mail sites is prohibited, except when there is an authorized business need to allow such access. To request access to a third party e-mail site, the employee's appointing authority/supervisor must complete the Third Party E-mail Access form (attached) and send it to the DOC chief security information officer/designee. Signed and approved Third Party E-mail Access forms are retained by IT.

4. The associate wardens' group must review and approve/disapprove requests for changes to the approved list of additional websites for standard Internet access. A representative for the associate wardens' group must notify the facility liaison at central office of approved requests. The facility liaison must ensure the approved website(s) are included in standard Internet access.

5. An employee must, upon request, grant the employee's supervisor "read only" delegate rights to the employee's e-mail account.

6. Employees are expected to exhibit sound judgment when using electronic communication equipment and technology and are expected to ensure all communications are appropriate in tone and content with the type of message conveyed. All electronic communications must be in accordance with department policies governing employee workplace conduct, be able to withstand public scrutiny, and not be embarrassing to individuals or the department (see Policy 103.220, "Personal Code of Conduct of Employees").

7. Employees are expected to lock their workstations when leaving their desks/offices for periods longer than five minutes or when directed by their supervisor or the department IT staff.

8. State law provides that an employee may use state time, property, or equipment to communicate electronically with other persons, including such examples as elected officials, the employer, or an exclusive bargaining representative, if it does not result in any loss of resources.

9. Limited and reasonable use of electronic communications equipment and technology for personal purposes is permitted if it does not result in an incremental cost to the state, including the value of time spent, or if such use results in an incremental cost that is so small as to make accounting for it unreasonable or administratively impracticable. It is expected that any personal use of such equipment or technology would be limited primarily to before and after work hours and during unpaid meal periods, and any use during business hours be limited to incidental use for emergency situations. Employees spending time that exceeds a limited and reasonable use on such personal activities during working hours are subject to disciplinary action.

10. Staff must receive authorization from the appointing authority in order to send global e-mails, to use Smartphone e-mail service, or IM service.

11. Employee participation on message and group discussion boards
In the event that employees participate in online, non-department, message, and group discussion boards (e.g., Google discussion groups, Yahoo discussion groups, Facebook, Twitter, or message boards), employees must not:
    a) Refer to crime victims or incarcerated persons by name.
    b) Reference characteristics of a specific case which would lead a reasonable person to recognize the identity of the crime victim.
    c) Disclose any incarcerated person's medical and psychological diagnoses made, or medical or psychological treatment conducted, while the incarcerated person was under department supervision or control.

12. Acceptable electronic communications are those that conform to the purpose, goals, and mission of the department (see Policy 100.010, "Mission, Values, Vision, and Goals of the Department of Corrections") and to each employee's job duties and responsibilities. Managers and supervisors are responsible for ensuring that employees appropriately use all electronic communication equipment and technology through training, supervising, and coaching. The following list, although not all-inclusive, provides examples of acceptable uses when utilizing any platform described as electronic communications outline in the definition section of this policy:
    a) Announcements of state laws, procedures, hearings, policies, services, or activities;
    b) Advisory, standards, research, analysis, and professional society or development activities related to the employee's department duties;
    c) Applying for, or administering, grants or contracts for state government research programs;
    d) Access to federal, state, or local government Internet home pages;
    e) Information access and exchange, for professional development or to maintain job knowledge or skills;
    f) Research and information gathering and
    g) Communications for administrative purposes.

13. Employee use of electronic communication equipment and technology must be able to withstand public scrutiny without embarrassment to the DOC or the State of Minnesota. Unacceptable electronic communications include such examples as the following, unless expressly authorized by the proper authority. If questionable, staff must consult their supervisor prior to proceeding. If unauthorized or questionable use occurs, supervisory personnel must be notified immediately:

a) Fund-raising, commercial (for-profit business), political or religious positions, chain letters, wagering/betting, illegal activities, violations of policy, and third party e-mail sites;
b) Tampering, vandalism, or reconfiguring of equipment/programs or subverting security or access levels;
c) Use of unauthorized data;
d) Use of offensive, biased, threatening, false/defamatory, racist, sexist, sexually explicit, obscene, or pornographic information;
e) Use of unauthorized software, including games, wallpaper, screen savers, picture, movie and sound files, etc. including software on any network directory;
f) Hard drive, CD, DVD, floppy disk, USB drive, or other technology device;
g) Non-staff who have not been given their own access codes, sending e-mails under another staff's identify, and/or Internet activity under another's codes;
h) Releasing, distribution, or sharing any protected information/data as outlined in data practices policy and law;
i) Representing the department without approval; and
j) Excessive use.

Inappropriate use may subject an employee to discipline. Illegal activities such as gambling or sexual harassment, subject the employee to automatic discipline, up-to and including discharge.

14. Employees must be aware that they might receive inappropriate, unsolicited e-mail messages (spam mail). Any such message must be deleted before opening if the employee does not believe the e-mail has come from a reputable person or organization. If an employee does open an e-mail and discovers it to be inappropriate in nature or a potential security threat (such as a virus), they must report it immediately to the DOC chief information security officer/designee. Employees must not forward or reply to these messages prior to consulting the chief information security officer/designee.

15. Personal use of telephones and facsimile machines is limited to local calls only, unless long distance calls can be charged to one's residence telephone or personal credit card.

16. Printing is limited to business related purposes.

17. Employees using state-purchased mobile devices and service must follow Policy 104.470, "Mobile Communications Devices."

C. Union usage

1. Electronic communication equipment and technology may be used by employee union representatives for certain union activities, including the posting of meeting notices, coordinating the grievance process, contract interpretation questions, union election results, and notification of arbitration decisions. E-mail access and union websites may be approved by the appointing authority or designee.

2. Electronic communication equipment and technology may not be used for union organizing activities, campaigning for union office, or solicitation of employees for union membership.

3. Union usage of electronic communication equipment and technology is subject to the same conditions as employee usage.

D. Monitoring usage

1. Employees should not consider e-mail to be either private or secure. The department reserves the right to monitor and audit the usage of all electronic equipment and technology.

2. All electronic documents, including e-mail, may be considered to be government data, subject to the Minnesota Government Data Practices Act. Employees must handle these documents in accordance with records retention policies and, under law, these documents may be made available to others, including the public, or may be made part of a court record.

3. Employee access may be reduced/suspended with or without notice by the appointing authority or designee.

4. Electronic monitoring of employee telephone communication only occurs if proper notice has been given in accordance with federal regulations.

E. Record retention schedules

1. The retention periods for e-mail and calendar items are 60 days and one year, respectively.

2. The retention periods for Microsoft Teams chats are one day for individual chats and 45 days for channel chats/posts.

   a) Individual chats: text conversations initiated in the "chat" section. These chats are separate from a specific team and can be initiated with any other state employee. These can be between two people or a group of people.

   b.) Channel chats: also known as "channel posts," chats within a particular team's channel. These are team-specific conversations that are relevant to a particular group or project.

3. Chats in the Zoom (FedRamp) and WebEx products are removed once the meeting is concluded and are not retained.

4. Some electronic communications may be considered official records of the department and, therefore, would need to be retained in accordance with the department's record retention schedule appropriate for this type, nature, and content of the record. The proper method to retain appropriate e-mails and chats is to save them to a designated directory. Improper disposal of official records may subject the employee and the department to legal sanctions and other administrative or legal consequences.

INTERNAL CONTROLS:

A. E-mail and Internet Access Request forms are retained in the appropriate IT file.

B. Third Party E-mail Access forms are retained in the appropriate IT file.

ACA STANDARDS: 2-CO-1F-06, 4-4101

REFERENCES: Minn. Stat. Chapter 13, "Minnesota Government Data Practices Act"
Minn. Stat. §§ 43A.38, subd. 4; 43A.39, subd. 2, 138.17,
State Policy: Appropriate Use of Electronic Communication and Technology, HR/LR Policy #1423
Policy 100.010, "Mission, Values, Vision, and Goals of the Department of Corrections"
Policy 105.200, "Information Technology Governance"
Policy 105.205, "Computerized Information Resources Security"
Policy 106.210, "Providing Access to and Protecting Government Data"
Policy 103.220, "Personal Code of Conduct of Employees"
Policy 104.470, "Mobile Communications Devices"
Stored Wire and Electronic Communications and Transactional Records Access (Federal Wire Tap Regulations), 21 U.S.C. 2701-2711

REPLACES: Policy 103.210, "Electronic Communications," 3/5/19.
All facility policies, memos, or other communications whether verbal, written, or transmitted by electronic means, regarding this topic.

ATTACHMENTS: Internet/E-Mail Access Request form (103.210A)
Third Party E-mail Access form (103.210B)

APPROVALS:
Deputy Commissioner, Community Reintegration and Restorative
Deputy Commissioner, Safety and Security Services
Assistant Commissioner, Organizational and Regulatory Services
Assistant Commissioner, Chief of Staff
Assistant Commissioner, Health, Recovery, and Programming