NEW YORK STATE Corrections and Community Supervision **DIRECTIVE**	TITLE **Use of Electronic Mail (Email)**		NO. 2824 DATE 07/27/2021
SUPERSEDES DIR# 2824 Dtd. 07/25/17	DISTRIBUTION A	PAGES PAGE 1 OF 5	DATE LAST REVISED
REFERENCES (Include but are not limited to) Personal Privacy Protection Law; Freedom of Information Law; Arts and Cultural Affairs Law; Executive Orders 2 and 7; ACA Expected Practice 1-ABC-1E-06; Directives #2011, #2810; ITS Policy No. NYS-P14-001; Employees' Manual	APPROVING AUTHORITY		

I. PURPOSE AND GOALS: Email is one of the Department of Corrections and Community Supervision's (DOCCS) core internal and external communication methods. The purpose of this policy is to ensure that email systems used by Department staff support Agency business functions to their fullest capacity. This policy advises staff and management of their responsibilities and provides guidance in managing information communicated by email.

II. ACCESS TO EMAIL SERVICES: Email services are requested by the direct supervisor for a new or current employee by contacting the Computer Security Coordinator (CSC) responsible for reviewing and authorizing this access. The supervisor may request internal-only DOCCS email access or, if appropriate, email access that allows for outside communications.

Requests that are processed by the CSC and approved by appropriate DOCCS management will be completed by the Office of Information Technology Services (ITS) User Access Management. All DOCCS users who receive a network account automatically receive an O365 (Outlook) email account. If a user's network ID changes, that user's existing email account is associated with the new network account. A new email account is not issued. Additional information and guidelines relating to the access of all available DOCCS computer resources is available by referencing Directive #2810, "Information Security Policy," and ITS Policy No: NYS-P14-001, "Acceptable Use of Information Technology Resources," which may be found at www.its.ny.gov.

III. USE OF EMAIL

A. Email services, like other means of communication, are to be used to support Departmental business. Staff may use email to communicate informally with others in the Department so long as the communication meets professional standards of conduct. Authorized staff may use email to communicate outside of the Department when such communications are related to legitimate business activities and are within their job assignments or responsibilities and the employee has been authorized for network email access that allows outside communications. Staff will not use email for illegal, disruptive, unethical, or unprofessional activities for personal gain, or for any purpose that would jeopardize the legitimate interests of the State.

Pursuant to Governor Cuomo's Executive Order No. 2, "Review, Continuation and Expiration of Prior Executive Orders," one of the Executive Orders issued by former Governor David A. Patterson that is being continued is Executive Order No. 7, issued June 18, 2008, "Prohibition Against Personal Use of State Property and Campaign Contributions to the Governor." Employees should make themselves familiar with this mandate, in particular, the section pertaining to the personal use of State property as contained in Section B, "Prohibition Against the Personal Use of State Property," paragraph (d), which states:

"*State computers shall be used only for official business, except that state computers may be used for incidental and necessary personal purposes, such as sending personal electronic mail messages, provided that such use is in a limited amount and duration and does not conflict with the proper exercise of the duties of the State employee."*

B. Email may be used for limited communications between local union representatives for general union business such as scheduling membership meetings and informing the union membership of upcoming meetings between labor and management, as well as which topics will be on the agenda for said meetings. Furthermore, email may also be used for local union representatives to communicate with management about issues related to the labor management process, provided they have an existing email account. Email may not be used to promote union issues or for union campaign purposes. Email accounts are established to meet Agency operational needs. Email accounts will not be established to facilitate union representative communications. The use of email to promote, advertise, or solicit for any political party, entity, or cause is strictly prohibited.

C. Email may not be addressed and transmitted to all correctional facilities (other than job postings and directive distributions) unless it has been reviewed and approved by the appropriate Central Office Executive staff member.

D. All employees with email access should check for incoming messages on a regular basis. Outlook email accounts, maintained by ITS, are considered "stale" when an email has not been sent from the account for 30 days. Mailboxes are inactivated when an email is not sent within 59 days. Facility Superintendents and Community Supervision Bureau Chiefs will be notified on a bi-weekly basis of "stale" mailboxes and provided instructions for retaining mailboxes if necessary.

E. All email communication will be in Arial font, size 12, color black.

IV. UNACCEPTABLE USES OF INFORMATION TECHNOLOGY RESOURCES[1]

A. Using State information technology resources to circulate unauthorized solicitations or advertisements for non-State purposes, including religious, political, or not-for-profit entities.

B. Using State information technology resources for commercial purposes or purposes in support of "for-profit" activities or other outside employment or business activity (e.g., consulting for pay, business transactions, etc.).

C. Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using State information technology resources.

D. Personal email accounts shall not be used for DOCCS business.

[1] Information Technology Resources are defined as "equipment or services used to input, store, process, transmit, and output information, including, but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, internet, email, and social media sites."

V. OCCASIONAL OR INCIDENTAL PERSONAL USE

A. Occasional or incidental personal use of information technology resources is permitted, provided such use is otherwise consistent with this policy and the requirements of Executive Order No. 7[2], is limited in amount and duration, and does not impede the ability of the individual or other users to fulfill the State Entity's responsibilities and duties, including but not limited to, extensive bandwidth or resource or storage utilization. The State Entity may revoke or limit this privilege at any time.

B. For example, users may make occasional and incidental personal use of information technology resources to schedule a lunch date, cancel a sports practice, check their bank accounts or other personal investments, or to communicate with a volunteer charity organization.

C. Your judgment regarding incidental and occasional personal use is important. While this policy does not attempt to articulate all required or proscribed behavior, it does seek to assist in the exercise of good judgment by providing the above guidelines. If you are unclear about the acceptable personal use of a State-provided resource, seek authorization from your immediate supervisor.

VI. GUIDELINES FOR PERSONAL USE OF SOCIAL MEDIA

: Staff should be sensitive to the fact that information posted on social media sites clearly reflects on the individual and may also reflect on the individual's professional life. Consequently, staff should use discretion when posting information on these sites and be conscious of the potential perceptions of and responses to the information. It is important to remember that once information is posted on a social media site, it can be captured and used in ways not originally intended. It is nearly impossible to restrict, as it often lives on in copies, archives, back-ups, and memory cache.

VII. ELECTRONIC EMAIL SIGNATURE

A. An employee signature is not required for all email communication.

B. All employees with email access who choose to utilize an electronic signature will create a signature that will be identical in format as other account holders.

C. Email signatures will contain the employee's name, title, agency, division (optional), facility, area office, address, contacts, and website address.

Sample: **Central Office/Division/Facility/Area Office/Board of Parole**

Name (Arial, bold, size 12, color black)

Title (Arial, regular, size 10, color black)

Department of Corrections and Community Supervision (Arial, bold, size 10, Grey 93/126/149)

Division Name/Facility/Area Office/Board of Parole (Arial, regular, size 10, color black)

Address (one line) (Arial, regular, size 10, color black)

Phone Number I Phone Number 2 I Email Address (Arial, regular, size 10, color black)

www.doccs.ny.gov (Arial, regular, size 10, Grey 93/126/149)

[2] Executive Order No. 7, "Prohibitions Against Personal Use of State Property and Campaign Contributions to the Governor," states, among other things, that "State computers shall be used only for official business, except that State computers may be used for incidental and necessary personal purposes."

VIII. VIOLATIONS OF EMAIL USE: Non-compliance with this policy may result in a violation of the Department's Employees' Manual and/or other related directives. Staff should report any misuse of the Department's email system or violations of this policy to their supervisor or appropriate Department staff.

IX. PRIVACY, CONFIDENTIALITY, AND ACCESS

A. Email messages are not personal and private. The Department can neither assure the privacy nor the confidentiality of email messages that may be created, sent, or stored. Email system administrators will not routinely monitor an individual staff member's email and will take reasonable precautions to protect the privacy of email. However, program managers and technical staff may access an employee's email:

1. For a legitimate business purpose (e.g., the need to access information when an employee is absent for an extended period of time).
2. To diagnose and resolve technical problems involving system hardware, software, or communications.
3. To investigate possible misuse of email when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.

B. A staff member is prohibited from accessing another user's email without their permission and the necessary delegation settings.

C. Email messages sent or received in conjunction with Agency business may:

1. Be releasable to the public under the Freedom of Information Law (FOIL).
2. Require special measures to comply with the Personal Privacy Protection Law.

D. All email messages including personal communications may be subject to discovery proceedings in legal actions.

X. SECURITY: Email security is the joint responsibility of technical staff and email users. Users must take all reasonable precautions, including safeguarding passwords, to prevent the use of the account by unauthorized individuals.

XI. MANAGEMENT AND RETENTION OF EMAIL COMMUNICATION: Applicable to records communicated via email: Email created in the normal course of official business and retained as evidence of official policies, actions, decisions, or transactions are records subject to records management under the Arts and Cultural Affairs Law and specific program requirements and may be subject to disclosure under NYS FOIL Law. See Directive #2011, "Disposition of Departmental Records."

Mainframe email is not archived and the retrieval of deleted messages from this system is a costly and unreliable process. Therefore, any user of the mainframe email system is required to print and retain any email that is to be included as part of an official record. Such emails include policies/directives, official correspondence, work schedules and assignments, meeting agendas, drafts circulated for review, and final reports/recommendations.

XII. RECORD RETENTION

A. Any email message (mainframe or IP-based) that is needed to meet operational, legal, audit, research, or other requirements shall be printed and filed with related paper records and other documentary materials. Such email records shall be retained and managed in an existing, accessible filing system, outside the email system, in accordance with the appropriate program unit's standard practices.

B. Records communicated via email will be disposed of within the recordkeeping system in which they have been filed in accordance with a Records Disposition Authorization (RDA) approved by State Archives and Records Administration (SARA). Program managers should consult with the Agency Records Management Officer concerning RDA's applicable to their program's records. See Directive #2011.

Users should:

1. Dispose of copies of records in email after they have been filed in a recordkeeping system.
2. Delete records of transitory or little value that are not normally retained in recordkeeping systems as evidence of Agency activity.

Email is not archived. Any user of the system is required to print and retain any emails that are required to be included as part of an official record, including policies/directives, official correspondence, work schedules and assignments, meeting agendas, drafts circulated for review, and final reports/recommendations.

XIII. ROLES AND RESPONSIBILITIES

A. Agency Executive Management: Will ensure that policies are implemented by program unit management and unit supervisors. Program unit managers and supervisors will develop and/or publicize recordkeeping practices in their area of responsibility, including the routing and format of records communicated via email. They will train staff in appropriate use and be responsible for ensuring the security of physical devices, passwords, and proper usage.

B. State Office for Information Technology Services (ITS): Is responsible for email security, backup, and disaster recovery.

C. Superintendents, Division Heads, or Area Supervisors: Are responsible for notifying the CSC when an employee leaves (transfers, retires, resigns, etc.) and no longer requires network and email access at their particular facility or office. The CSC is then responsible for notifying ITS.

D. All Email Users Should:

1. Be courteous and follow accepted standards of etiquette.
2. Protect others' privacy and confidentiality.
3. Protect their passwords.
4. Remove personal messages, transient records, and reference copies in a timely manner.
5. Comply with Agency and unit policies, procedures, and standards regarding Departmental communications.

XIV. POLICY REVIEW AND UPDATE: The Executive Deputy Commissioner and the Deputy Commissioner for Strategic Planning and Population Management will periodically review and update this policy as new technologies and organizational changes are planned and implemented. Questions concerning this policy should be directed to the Executive Deputy Commissioner.

Statewide technology policies, standards, and guidelines may be found at the following website: http://www.its.ny.gov/tables/technologypolicyindex.