USE OF ELECTRONIC COMMUNICATION SYSTEMS

1. GENERAL

A. Information carried by electronic communication systems should be compared to a post card, rather than a sealed letter.
B. Outlook and the HRM Internet gateway are communication systems and work tools owned by the Halifax Regional Municipality. The use of these systems and the information which travels across them are therefore subject to corporate audits. Similarly, the HRP Computer Network system is owned by the Halifax Regional Police and, therefore, the information which travels across this system is also subject to random audits by HRP.
C. The *Freedom of Information and Protection of Privacy Act (FOIPOP)* carries with it regulations for accessing information, including electronic records. When using HRM email and HRP Vmail accounts, local Intranets, the HRM Internet and the HRP RMS and CAD systems as a means of communication, HRP staff are also reminded that there is no expectation of privacy and all transactions made via these systems are subject to routine scrutiny and freedom of information applications made under FOIPOP.
D. The *Criminal Code of Canada* carries indictable offences associated with improper use of the Internet

2. POLICY

A. Because others may easily read or access it, electronic communication should not be regarded as a private communication.
B. Personal e-mail accounts shall not be accessed using the HRP Network to minimize the potential for computer virus contamination and computer hackers.
C. A limited amount of personal Internet use is acceptable provided:
    i. Access time is ristricted to before and after regular working hours. Internet use during regular working hours shall be limited to work-related searches or searches being conducted for educational or presentation research purposes.
    ii. Appropriate Internet sites only are visted, keeping in mind the Internet activity can be monitored.
D. Work-related messages sent through Outlook and the HRP Computer Network should be limited to specific recipients to whom the contents of the messages applies.
E. Where e-mails are sent which contain information related to an investigation, members are reminded that these e-mails form part of the investigation and therefore the sender of the email is responsible to print a hardcopy of the email and forward the copy for inclusion in the associated Masterfile. Members are also reminded these emails are subject to FOIPOP requests and, therefore, must be written in a professional and respectful manner at all times and which would be a credit to the image of HRP should they become subject to a FOIPOP application.

F. Messages of a personal or social nature are not only inappropriate but also delay communication between sites and take up much needed space on HRM servers. Therefore, communications sent via the HRP Computer Network and the HRM Outlook System shall be of a professional nature at all times. Employees discovered contravening this policy shall be subject to displinary actions.

G. HRP employees should be aware that Internet access and e-mail use are privileges, not rights

H. The following activities are strictly prohibited from being conducted on the Internet and HRM Computer Network systems, including issued cell phones, and may, depending on the circumstances, constitute abuse and could result in diciplinary action:

   i. Any inappropriate activity including, but not limited to, the sending or receiving of:

      1. Pornographic material, unless approved as part of an undercover police investigation;
      2. Hate literature;
      3. Inappropriate text or graphic files (i.e., jokes and computer graphics containing sexual, racial or otherwise objectionable overtones);
      4. Files dangerous to the integrity of the HRP and HRM computer networks;
      5. Files or material which could infringe on another employee's workplace rights;
      6. Copyright materials without the express permission from the owner of the copyright.

   ii. Impolite, abusive, racist, or otherwise objectionable language.

   iii. The sending of communications:

      1. For private gain or for any use other than intended by the Halifax Regional Municipality;
      2. That violate municipal, provincial or federal by-laws or statues;
      3. That violate the Code of Conduct and Discipline of the *Nova Scotia Police Act Regulations* (i.e., being insubordinate, disobeying, omitting or neglecting to carry out a lawful order without adequate reason, including one given electronically to personnel, etc.) and that would likely bring discredut to the reputation of the HRP.
      4. Of particular note, members are reminded of Section 5(1)(e) of the Code of Conduct and Discipline of the Nova Scotia Police Act Regulations which makes it a disciplinary default for any member who:

         a. Improperly discloses information:

            i. Without proper authority, communicating to any person any information which the member possesses as a member of a police force,

            ii. Making an anonymous communication to any police authority or any member of a police force, or

            iii. Signing or circulating a petition or statement in respect of a matter concerning the police force, expect through

the proper official channel of correspondence of the member's duties, as a representative of a certified police union, association or federation

iv. The distribution of material of a confidential or sensitive nature.
v. Vandalizing, destroying, or compromising data belonging to another (including the uploading or creation of computer viruses).
vi. The playing of computer games.
vii. Accessing HRP data for personal reasons.

I. See related policy on **ANNOUNCEMENTS VIA EMAIL AND OTHER FORMS OF ELECTRONIC COMMUNICATIONS.**

HRP EMPLOYEES

J. Unless an employee has be authorized to use an alternative name and identifying information and to conduct inappropriate Internet activity for the purpose of conducting an undercover police investigation, HRP employees with E-mail and Internet access must provide accurate information about their name, title and department when using HRM Internt access and Outlook.
K. When authorization has been given to use an alternate name and identifying information, the employee shall advise their immediate supervisor of such use and provide him/her with the alternative name and identification, where deemed appropriate.
L. When repsonding to messages received through e-mail and Internet, HRP employees are bound by the same standards of professionalism, promptness, accuracy and courtesy as would apply to the more traditional forms of communication. In this regard, employees who responde to these forms of communication:
    i. Shall:
        1. Adhere to related policy on **EXTERNAL CORRESPONDENCES;**
        2. Limit messages sent from MDCs to those pertaining to official police business only;
        3. Respond in writing on HRP letterhead when the nature of the response is deemed to involve classified materials or is being addressed directly to a high-ranking government official.
    ii. May respond via e-mail when the request was made directly to that person and the response is brief.
M. If an employee is sending e-mail which involves a lengthy attachment(s) (i.e., in excess of 15 pages) to HRP personnel, the sending of the e-mail must be approved by the HRM Systems Administrator prior to being sent. The sender of the e-mail shall also ensure a cautionary statement advising recipients of the attachment's length is included in the message portion of the e-mail.

3. DEFINITIONS

A. ***Electronic Communications:*** for the purpose of this policy, refers to the any transactions involving information being accessed/queried, forwarded or retained using HRM or HRP electronic communication system and includes but is not limited to:

i. Outlook email (email)
ii. Versa mail (Vmail)
iii. Car-tocar communication via CAD
iv. Cellular telephone communications using HRP-owned/leased cellular phones
v. VMOBILE
vi. RMS, CAD, PRMV, CPIC queries
vii. Intratnet and Internet transactions
viii. Any other system available by staff to access government-stored information.

Effective Date of Last Revision	July 16, 2025
Policy Owner	Supt. Greg Robertson

By Order Of:

Don MacLean

Chief of Police