Policy Name:	**INFORMATION AND TECHNOLOGY (IT) SECURITY**		
Policy #:	AD 9.19	**Last Updated:**	2021-10-21
Issued By:	SUPPORT SERVICES BUREAU	**Approved By:**	SURREY POLICE BOARD
		Review Frequency:	AS REQUIRED

RELATED POLICIES

AD 9.1 Authorized Use of Computing Environment and Electronic Communications

AD 9.17 Social Media

AD 9.18 Security and Confidentiality of Records and Information

1. PURPOSE

1.1. This Policy applies to all equipment and systems that are owned or leased by SPS, and to personal computing equipment that is used, with authorization, for SPS purposes, regardless of physical location.

1.2. This Policy is consistent with the *Police Act*, BC *Provincial Policing Standards*, BC *Human Rights Code*, provincial privacy legislation, and other SPS policies.

2. SCOPE

2.1. This policy applies to all sworn SPS Members and civilian Employees, including Contractors, Practicum Students or Volunteers responsible for ensuring that individuals who are granted access to SPS digital and technological resources have read and agreed to abide by this policy.

3. POLICY

3.1. The SPS recognizes that email and Internet access are useful and necessary services that enhance ability to communicate with others and provides improved service to the public. The purpose of this policy is to set appropriate standards for using SPS Information Management and Information Technology (IM/IT) resources.

3.2. The information transmitted on the Internet or stored on servers accessible via the Internet is generally an insecure environment and content may be viewed by non-intended audiences. Users must not knowingly access sites that may bring the SPS into disrepute. This applies to email as email may be intercepted by non-intended recipients and/or forwarded beyond the control of the sender. SPS has a responsibility to ensure email procedures are adhered to (see AD 9.1 *Authorized Use of Computing Environment and Electronic Communications* and AD 9.17 *Social Media*).

4. PROCEDURE

Review and Audit

4.1. The SPS IM/IT Section will routinely analyze network traffic for trends or anomalies.

i. breaches of policy and/or evidence of misconduct may be found during these searches intended to protect the SPS network.
ii. alleged breaches of policy or misuse of SPS email or the Internet may result in a labour process investigation, an investigation under the *Police Act*, and/or *Criminal Code*.

4.2. The SPS may access, audit, monitor, inspect, copy, store, and review SPS IT resources, without prior notice, upon receiving a complaint of misconduct regarding inappropriate email content, text or attachments, Internet usage, or the inappropriate release of confidential information.

i. When such and audit occurs, a log detailing all access will be maintained by the investigator conducting the audit.
ii. During an audit or an investigation, if there is uncertainty about the appropriateness of the content in an e-mail or on the network, consultation may occur with internal stakeholders and experts in this field. This may include:
    a) The Inspector i/c Special Investigation Section;
    b) The Inspector i/c the Employee Services Section;
    c) A union representative; and
    d) Any other police expert who can provide clarity around the appropriateness of such material.

Security Access – Internet and Email

4.3. Access to Internet sites is recorded, and users may be required to explain why they have accessed a particular site.

4.4. The Inspector in charge of IM/IT Section may revoke or restrict Internet access to any or all staff for valid technical reasons (e.g., bandwidth restrictions, virus/worm attack, disaster or emergency response, or other technical requirements).

4.5. Users accessing or disseminating information on the Internet must ensure that such information is factual and in compliance with SPS policies and the applicable federal and provincial legislation (e.g., FOIPPA). See AD 5.7 Human Rights and Respectful Workplace; AD 9.1 Authorized Use of Computing Environment and Electronic Communications; AD 9.17 Social Media Policy.

4.6. Users must comply with all applicable laws and regulations and respect the legal protection provided by copyright and licenses with respect to programs, software applications and data.

4.7. Third parties may be able to gain access to data, records or communications transmitted by e-mail, through an FOI request, a subpoena or summons in a court of law, internal usage monitoring, or interception on the Internet. As a result, Users must consider what information they are transmitting by e-mail. In addition, Internet and e-mail users shall not disclose user identifications, passwords, or any other non-public identifiers of anyone, including IT staff; or any detail of the SPS's security measures.

4.8. Users must protect all passwords.

i. Passwords must not be posted in or around the user's workstation.
ii. Users must not share identification or password codes for SPS digital equipment.

4.9 Users must not attempt to obscure the origin or destination of any transmission, or download material under an assumed Internet address, except for investigative purposes and with the written approval of the Inspector in charge of IM/IT Section.

4.10 Users must ensure equipment is locked or logged off when absent from the workstation. Anyone accessing another Employee's workstation or electronic device without authorization violates this policy and may be subject to discipline under the *Police Act* or Collective Agreement.

4.11 The SPS recognizes that SPS Members and civilian Employees, on occasion, will be working at home or remotely and may have custody or issued equipment to facilitate computer access. Users working at home or remotely are responsible for the security of SPS equipment, digital resources, and data.

APPENDIX A: DEFINITIONS

“Computing environment” means any electronic information, information system, application, device (including PCs, laptops, mobile devices, and telephones) or other computing technology that is connected to the SPS’s IT systems (including cloud-based services and mobile services).

“Contractor” means a person or persons who have access to SPS premises or Electronic communications system, as defined in this policy, for the purpose of providing services or supplies to SPS on a contractual basis.

“Electronic Communications” means any form of digital communications including, but not limited to, email, text/short message service, instant messaging, online chat, social media posts/tweets, blogs, online video/audio posts, telephonic, faxing, and audio/video conferencing.

“Electronic communications system” means the technology on which the electronic communications occurs.

“Employee” means any employee of SPS (including sworn Members and civilian staff).

"Inappropriate material" means materials including, but is not limited to, any material that is pornographic, sexual, or erotic, obscene, lewd, offensive or harassing, threatening, defamatory, racially offensive, promotes violence, hatred, abuse or neglect, or any material which can be reasonably interpreted as offensive or contravenes the BC *Human Rights Code*, *Criminal Code* or any other federal and provincial laws. This includes any material that may bring the reputation of the SPS into disrepute.

“Internet” (World Wide Web or www) means a series of interconnected worldwide computer networks, which are in turn, connected to conforming www sites that offer website information/services or offer e-mail services.

“Member” means a sworn Police Officer appointed by the Surrey Police Board.

“Mobile devices” means devices such as a smart phone (iPhone, Android, etc.), cell phone and tablets (iPads).

“Practicum Students” mean students of a program at a recognized education institution who are engaged at a SPS premises for study, research, work experience, etc.

"Sensitive Information" means personal, confidential, or protected information where the release is unauthorized, including any information which is reasonably likely to be withheld from access under the *Freedom of Information and Protection of Privacy Act* (FOIPPA).

“Social media” means websites and online applications that allow people and organizations to create, share, and exchange content or to participate in social networking.

“SPS premises” includes, but is not limited to, any property permanently or temporarily under the jurisdiction of SPS, including land, building, job sites, facilities, parking lots, equipment, vehicles, whether

owned, leased or used by SPS and wherever located. The work site of a seconded employee is considered an extension of the SPS workplace, and therefore SPS premises.

“SPS property” means all assets of the SPS, whether temporary, permanent, owned, leased or otherwise acquired, including real, personal or intellectual property, vehicles, chattels, materials, equipment and supplies.

“Supervisor” means a Team Leader, Manager, Staff Sergeant, Sergeant, Inspector, Superintendent, Deputy Chief Constable, Chief Constable, and any other person acting in a supervisory capacity who is accountable for a particular area or shift on behalf of the SPS.

"User" means any person authorized to access SPS e-mail or the Internet, including permanent, temporary, and limited term Employees, Contractors, Volunteers, Practicum Students.

“Volunteer” means a person serving SPS who is not an employee, as defined in this policy, and includes those individuals serving on any board(s), commission(s) or committee(s) established by SPS.

APPENDIX B: REFERENCES

BC *Human Rights Code*, R.S.B.C. 1996, c. 210

BC *Police Act*, R.S.B.C. 1996, c. 367