Policy Name:	**AUTHORIZED USE OF COMPUTING ENVIRONMENT AND ELECTRONIC COMMUNICATIONS**		
Policy #:	AD 9.1	**Last Updated:**	2021-08-08
Issued By:	SUPPORT SERVICES BUREAU	**Approved By:**	SURREY POLICE BOARD
		Review Frequency:	AS REQUIRED

RELATED POLICIES

AD 2.3 Conflict of Interest

AD 5.7 Human Rights and Respectful Workplace

AD 9.17 Social Media

AD 9.18 Security and Confidentiality of Records and Information

1. PURPOSE

1.1. To identify and inform Surrey Police Service (SPS) Employees, Volunteers, Practicum Students, and Contractors of their responsibilities and requirements for the use of the SPS Computing Environment and Electronic Communications (e.g., electronic mail, Internet, intranet, phones, and other electronic systems).

1.2. To support federal, provincial and SPS privacy and security requirements for all computing environment and electronic communications.

1.3. To provide specific requirements for Members to check and respond to emails and voice mails during their work shift.

2. SCOPE

2.1. This Policy applies to all SPS Employees (including Members and civilian staff), Volunteers, Practicum Students, and Contractors.

3. POLICY

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

3.2. SPS's Computing Environment and Electronic Communications Systems must be used in a manner consistent with the SPS's policies, its values, the *Police Act,* BC *Provincial Policing Standards*, BC *Human Rights Code*, and federal and provincial laws.

3.3. All electronic communications equipment and software, and information and data installed or created on SPS electronic equipment is the property of the SPS. This includes all programs, documents, spreadsheets, databases, and methods or techniques developed using SPS equipment and/or software.

3.4. All electronic documents related to the SPS, including emails that are electronically created, received and retained by employees, or that are printed on paper and placed in a paper file are considered under legislation to be "Records" of the SPS and as such are subject to all of the access and privacy provisions of the *Freedom of Information and Protection of Privacy Act (*FOIPPA) and all record systems policies, such as those governing disclosure of CPIC and PRIME records.

3.5. Other than for approved SPS operational, administrative, or investigative purposes, and as authorized in legislation or related SPS policy, information or data on electronic equipment may not be:

i. printed and disclosed;
ii. electronically copied to removable media, including diskettes, CDs, memory sticks or any other type or form of storage device;
iii. downloaded or shared electronically to another individual or agency, whether public or private; or
iv. shared on communications or collaborative platforms (e.g., Zoom, MS Teams, etc.).

3.6. Requests for information from a source outside the SPS, must be referred to the Supervisor of the individual receiving the request and the Manager, Information and Privacy (see AD 9.18 Security and Confidentiality of Records and Information).

3.7. Any collection, access, use, transmission, or disposal of SPS related information (including records, reports, emails, data, etc.) or use of the SPS Computing Environment or Electronic Communications Systems, whether for personal or business use, may be audited, inspected, monitored, or investigated to:

i. maintain, repair, and manage the SPS Computing Environment and Electronic Communications Systems for efficient operation;
ii. respond to and remediate a security or privacy incident;
iii. meet legal requirements to produce records, information, and metadata;

iv. ensure accessibility of the SPS Computing Environment and Electronic Communications Systems for the continuity of work processes;
v. improve business processes and manage productivity;
vi. investigate reasonable concerns about user misconduct; and
vii. ensure compliance with statutory and policy requirements.

Personal Use

3.8. Personal use of the SPS computing environment or electronic communications systems is acceptable on the following basis:

i. personal use is done on personal time with no adverse effect on the individual's performance of work duties or responsibilities;
ii. the personal use does not violate any SPS Policy, or federal or provincial law or standard;
iii. software, music, movies, entertainment videos and other unapproved bandwidth intensive applications cannot be viewed, downloaded, or saved while connected to the SPS network or its cellular network;
iv. charges are not incurred by SPS for personal use;
v. there is no adverse impact on the availability of IT resources for SPS business purposes;
vi. no accessing information for personal gain or advantage that is not publicly available; and
vii. electronic communications are not made which could harm SPS's intellectual property rights (e.g., trademarks) or reputation.

Prohibited Use

3.9. The following uses of Computing Environment and Electronic Communications Systems by any Employee, Volunteer, Practicum Student, or Contractor is prohibited:

i. activities that are illegal or fraudulent under federal or provincial law;
ii. unauthorized downloading, installation or copying of copyrighted material (including software) for which SPS does not have a licence;
iii. accessing SPS data, an SPS application or using an SPS account for a purpose other than conducting SPS business (other than as expressly authorized in Personal Use 3.8. above);
iv. unauthorized downloading, installing or use of unapproved software or cloud services;
v. accessing data, a system, or an account for a purpose other than conducting SPS business;
vi. introduction of malicious programs into the network or server (e.g. viruses, password breakers and keystroke recorders);
vii. sharing account passwords or allowing use of SPS accounts by others;
viii. use of SPS's system to procure or send or willingly receive material which is not permitted under AD 2.3 Conflict of Interest, AD 5.7 Human Rights and Respectful Workplace, AD 9.18 Security and Confidentiality of Records and Information, AD 9.17 Social Media, or other policies;
ix. unauthorized access or use of SPS data or applications;
x. use of unauthorized cloud services or mobile applications for conducting SPS business;

xi. distributing personal information or any other privileged, protected, confidential, or sensitive information, without authorization;
xii. distributing unsolicited messages, including the sending of "junk mail/text" or advertising material to individuals who did not specifically request such material;
xiii. any form of harassment via email, telephone, texting, or any other electronic communications, whether through language, frequency, or size of messages; and
xiv. impersonation of another sender or another sender's email address.

3.10. These restrictions apply to the use of any SPS electronic communications at any time.

4. PROCEDURE

4.1. Authorized use and access are defined as the level of access to a specific system granted by the Information Management Services (IMS) Inspector or delegate, or the PRIME Coordinator, and is subject to clearance and training. If in doubt about authorization, Employees, Contractors, Practicum Students, or Contractors should consult their Supervisor.

4.2. SPS Electronic Communication Systems and the data or records stored therein, may only be accessed and used for an authorized purpose, and shall not be accessed or used for personal reasons except as defined in S. 3.8., or to benefit the Employee, Volunteer, Practicum Student, or Contractor or another person outside of the scope of their engagement with the SPS.

4.3. Members are required to review their SPS computing and communications devices (e.g., email and work voice mail messages) at least once per their scheduled work shift.

Use of Personal Devices (Cellphones)

4.4. To protect the integrity of investigations**,** Employee accountability, prosecution disclosure requirements, Member safety, and compliance with laws, Members must not use personal electronic communications devices of collecting work-related audio, audio and video, or photographic images.

4.5. Except in exigent circumstances, a Member must not use a personal communication or recording device, text from and/or to their private personal numbers, or email between personal account addresses, in relation to SPS operational, investigative or business matters without prior authorization. Exigent circumstances exist where there is strong possibility of losing the opportunity to record evidence and access to SPS equipment is not available.

4.6. If a personal device is to be or has been used for recording or communications in relation to an operational, investigative, or business matter without prior authorization, the Member intending to or having done so must, as soon as practicable:

i. notify their Supervisor;
ii. transfer a complete copy of the recorded or communicated data to the relevant SPS operational, investigative, or business file on SPS equipment; and

iii. after the recorded or communicated data has been transferred, delete the same on the personal device.

4.7. Personal electronic devices must not be connected to SPS network or equipment systems without prior authorization, other than as required to transfer recorded or communicated data to SPS equipment.

Security

4.8. The IMS will assign a User Identification (UserID) to each authorized User. Each User will create a confidential password that will not be shared with another person.

4.9. Users are accountable for all activities that occur under their UserID. Users are responsible for immediately reporting any known or suspected compromise of their UserID or password. If an irregularity is suspected, the IMS will examine logs to determine if unauthorized usage has occurred. Passwords must not be left unsecured or left where another person can access them.

4.10. All Users are responsible for changing their own passwords at least once every ninety (90) days. Passwords should be easy for the User to remember, but difficult for others to determine. Password parameters will be set by IMS.

4.11. Employees who are required to share or transmit data that is Protected "B" must ensure that the data is encrypted as per IMS protocols.

4.12. IMS will provide for the performance of random audits of computer-related activities including all computer network traffic, including email, Internet, and MDT activity on all storage mediums. Audits may also be performed if requested by a Member of the Executive Leadership Team or delegate.

4.13. Users must report suspicious activities or procedure violations to their Supervisor, who in turn will submit a brief report to the Inspector, Employee Services Section for appropriate action.

4.14. The disclosure to a third party of any electronic communications, received by an SPS Employee, that has been identified by the sender as confidential is strictly prohibited, except as authorized by the sender of the communication or as otherwise required by law.

4.15. For the purposes of this policy, the IMS Inspector or delegate may access, monitor, review, copy or disclose all Electronic Communications made by Employees, Volunteers, Practicum Students, and Contractors within the SPS Computing and Communications Environment. The IMS Inspector or delegate may also access or monitor user activities within the Electronic Systems, including archived records of present and former Employees, Volunteers, Practicum Students and Contractors, without the User's consent.

Working Remotely

4.16. The SPS recognizes that Employees, Volunteers, Practicum Students and Contractors will, on occasion, work at home or remotely. They must obtain authorization from their Supervisor prior to doing so.

Supervisors must ensure that IMS security requirements are satisfied prior to authorizing an Employee, Volunteer, Practicum Student or Contractor to access SPS data remotely. Employees, Volunteers, Practicum Students and Contractors are responsible for the security of SPS computing resources and data.

4.17. Employees, Volunteers, Practicum Students and Contractors who can access information remotely must not store work-related information on a non-SPS computer or data storage device.

E-mail

4.18. Given the sensitive nature of many SPS e-mails, a confidentiality disclaimer must be included, notifying unintended recipients of requirements placed upon them if they mistakenly receive an SPS email. Outgoing emails must include a confidentiality disclaimer in the signature block, while e-mail replies and forwards should contain pertinent contact information (see the approved disclaimer in Appendix A).

4.19. Employees, Volunteers, Practicum Students and Contractors must not send global emails (entire SPS distribution list) unless approved by the Chief Constable, a Deputy Chief Constable, the Manager, Strategic Communications, or delegate. The bottom of global emails must state: "*Approved for distribution by [Name*]".

4.20. Employees, Volunteers, Practicum Students, and Contractors must use an email signature block format that has been approved by the Strategic Communications Unit.

4.21. Employees must not use a personal email account for any SPS work-related purposes without prior authorization.

4.22. Employees must surrender all SPS controlled computing environment and electronic communications in their possession to the appropriate personnel upon termination of their employment.

Audit

4.23. The SPS has the right to audit its computing environment and electronic communications to ensure compliance with this policy. Its computing environment, tools and applications are the property of SPS and are subject to the *Freedom of Information and Protection of Privacy Act*. SPS may monitor, copy, access or disclose any information that is stored, processed, received, or transmitted on its computing environment.

4.24. SPS reserves the right to access, audit, monitor, inspect, copy, store and review its computing environment, without prior notice, upon receiving a complaint of misconduct regarding inappropriate e-mail content, text or attachments, Internet usage, or the inappropriate release of confidential information.

4.25. SPS has the right to edit and remove inappropriate information or contributions to its computing environment and electronic communications systems.

Expectations / Further Actions

5. Any Employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Volunteers, Practicum Students, and Contractors may be denied access to SPS's computing environment and electronic communications systems and may have their relationship with SPS terminated.

APPENDIX A: EMAIL DISCLAIMER

*"*This message and attachments are confidential and may contain privileged information. They are for the use of the intended recipient(s) only. Access, disclosure, copying, distribution, and reliance on this message and attachments by unauthorized recipients are prohibited and may be a criminal offence and/or a violation of the *Freedom of Information and Protection of Privacy Act*. If you mistakenly have received this message and attachments, please notify the Surrey Police Service and delete or destroy all copies.*"*

APPENDIX B: DEFINITIONS

"BCPPS" means the British Columbia *Provincial Policing Standards* issued pursuant to the *Police Act*.

"Commercial activity" means any transaction related to advertising or promoting goods or services, providing a business opportunity, or directing a recipient to information which is considered to have a commercial purpose.

"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 Members and civilian staff).

"Executive Leadership Team" means the Chief Constable and the Deputy Chief Constables.

"Inappropriate material" means materials including, but not limited to, any material that is pornographic, sexual or erotic, obscene, lewd, offensive or harassing, threatening, defamatory, racially offensive, promoting violence, hatred, abuse or neglect, or any material which can be reasonably interpreted as offensive or contravenes the BC *Human Rights Code,* the *Criminal Code* or any other federal or 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.

Protected "B" means sensitive information or assets that if compromised could cause serious injury or harm to an individual, organization, or government.

"Sensitive information" means personal, confidential, or protected information where the release is unauthorized, including any information which is reasonably likely to be excluded 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” for the purposes of this policy 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 term Employees, contract personnel, Contractors, consultants, Volunteers, other personnel at the SPS, and all personnel affiliated with third parties.

“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.