TRANSIT POLICE
SOCIAL MEDIA

Effective Date: August 8, 2012
Revised Date: December 11, 2018, January 25, 2023
Reviewed Date:
Review Frequency: As Required
Office of Primary Responsibility: Senior Manager – Strategic Services

POLICY

[See also Transit Police policies: OM010 – Media Relations, AC140 – Complaints, AF160 – IT Access Control, SOP46 – Social Media Use]

Definitions

Apparent/Overt Use – In the Apparent/Overt Use engagement level, law enforcement's identification need not be concealed. Within this engagement level, there is no interaction between law enforcement personnel and the subject/group. This level of access is similar to an officer on patrol. Information accessed via this level is open to the public (anyone with Internet access can "see" the information). Law enforcement's use and response should be similar to how it uses and responds to information gathered during routine patrol. An example of "apparent/overt use" would be agency personnel searching Twitter for any indication of a criminal-related flash mob to develop a situational awareness report for the jurisdiction. *[Source: February 2013, US Bureau of Justice Assistance (BJA)—with the support of the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC), "Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations", page 14.]*

Blog – A self-published diary or commentary on a particular topic that may allow visitors to post responses, reactions, or comments. The term is short for "Web log."

Chief Officer – The Transit Police Chief Officer or delegate.

Covert Use – During the Covert Use engagement level, law enforcement's identify is explicitly concealed. Law enforcement is engaging in authorized undercover activities for an articulated investigative purpose, and the concealment of the officer's identity is essential. An example of Covert Use is the creation of an undercover profile to directly interact with an identified criminal online. Another example is an agency lawfully intercepting information from a social media site, through a court order, as part of authorized law enforcement action. *[Source: February 2013, US Bureau of Justice Assistance (BJA)—with the support of the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC), "Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations", page 14.]*

Deputy Chief Officer Operations – The Transit Police Deputy Chief Officer in charge of Operations or delegate.

Deputy Chief Officer Administrative Services – The Transit Police Deputy Chief Officer in charge of Administrative Services or delegate.

Discreet Use – During the Discreet Use engagement level, law enforcement's identify is not overtly apparent. There is no direct interaction with subject or groups; rather, activity at this level is focused on information and criminal intelligence gathering. The activities undertaken during the Discreet Phase can be compared to the activities and purpose of an unmarked patrol car or a plainclothes officers. An example of Discreet Use is an analyst utilizing a nongovernmental IP address to read a Weblog (blog) written by an unknown extremist who regularly makes threats against the government. Bloggers (those who write or oversee the writing of blogs) may use an analytical tool to track both "hits" to the blog and IP addressed of computers that access the blog, which could potentially identify law enforcement personnel to the blogger. This identification could negatively impact the use of the information and the safety of law enforcement personnel, who would not want to reveal that they are accessing the blog for authorized law enforcement purposes. *[Source: February 2013, US Bureau of Justice Assistance (BJA)—with the support of the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC), "Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations", page 14.]*

Senior Manager Strategic Services – The Transit Police Manager in charge of communications or delegate.

Member – A Designated Constable (all ranks), the Chief Officer or a Deputy Chief Officer of the Transit Police.

Metro Vancouver Transit Police ("Transit Police") – The operating name for the South Coast British Columbia Transportation Authority Police Service (Designated Policing Unit and Designated Law Enforcement Unit).

Page – For the purpose of this policy, a page refers to the specific portion of a Social Media website where content is displayed, and managed by an individual or individuals with administrator rights.

Police Act – The BC *Police Act*, [RSBC 1996], c.367, and the regulations thereto, including the *Transit Police Complaints and Operations Regulation*, all as amended from time to time.

Post – The content a user shares on a Social Media site or the act of publishing content on a site.

Profile – Information that a user provides about themselves on a social networking site.

Social Media – A category of Internet-based resources that integrates user generated content and user participation. This includes, but is not limited to social networking sites (Facebook, WeChat), professional networking sites (LinkedIn), micro-blogging sites (Twitter, Snapchat, Tumblr), photo- and video-sharing sites (Instagram, TikTok, YouTube), wikis (Wikipedia), blogs and news sites (4chan, Reddit).

Social Networks – Online platforms where users can create profiles, share information and socialize with others using a range of technologies.

Speech – Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.

Transit Police Image – Any crest, insignia, flag or other symbol representing the Transit Police or Transit Police Board; the name of the police service or police board, any picture, photography or other graphic representation that depicts the Transit Police or Transit Police Board, its staff and board members, facilities, activities or equipment (including uniforms and police vehicles).

Transit Police Personnel – Sworn police officers, community safety officers, and civilian professionals who work for the Transit Police.

TSML – TransLink Security Management Limited, a subsidiary of the South Coast British Columbia Transportation Authority and legal entity/employer for the Metro Vancouver Transit Police.

Wiki – A website that is developed collaboratively by a community of users, allowing any user to add and edit content.

Authority

1. Pursuant to the *Police Act*, the Chief Officer is responsible for the general supervision and command over the Transit Police, including implementing measures to ensure protection of the reputation, security and confidentiality interests of the Transit Police and its personnel.

2. Transit Police police officers must comply with the *Police Act* and expected conduct requirements for a police officer on and off duty.

General

3. The Transit Police will utilize Social Media where appropriate to assist the Transit Police with matters including but not limited to community outreach, problem solving, investigations, crime prevention, recruiting, media relations, reporting, time sensitive notifications, and police events involving the public. Like all forms of communications, Social Media must be utilized by Transit Police Personnel in a clear and responsible manner to ensure that the clarity of the messaging is maintained and to prevent misinterpretation and erroneous messaging from occurring.

4. Transit Police Personnel are entitled to use Social Media in their private lives; however, their status as staff with the Transit Police requires that their personal use of Social Media (including content of their postings) not jeopardize the integrity and reputation of the Transit Police or the reputation or safety of other persons. The Transit Police will provide direction to Transit Police Personnel on the prohibited use of Social Media and provide guidelines to Transit Police Personnel in protecting their personal and professional reputation.

5. Unless otherwise so determined by the Chief Officer, the Senior Manager Strategic Services is delegated authority for the oversight and administration of Social Media

use for Transit Police business. All Transit Police Social Media accounts (used for non-investigation purpose) will be as so authorized by the Senior Manager Strategic Services (or as otherwise determined by the Chief Officer).

6. The Transit Police author of a page, post or profile will be responsible for the information contained and will be accountable for the accuracy of such information.

7. Transit Police Personnel will be explicitly prohibited from use of any electronic device (e.g., laptop, mobile phone), Transit Police issued or personal, to post, upload or download any Transit Police or job related information to any Social Media account, unless it is a Social Media account approved by the Senior Manager Strategic Services and the user posting is so authorized pursuant to this policy. Examples include, but are not limited to, releasing or using:

   (1) Confidential, sensitive, or copyrighted information that Transit Police Personnel have access to due to employment with the Transit Police including, but not limited to, Transit Police Images;

   (2) Data from any ongoing criminal or administrative investigation including statements, memos, photographs, video or audio recordings;

   (3) Photographs of suspects, arrestees or evidence from any crime scene;

   (4) Personal statements about an on-duty or off-duty incident or issue including a use of force incident or criminal investigation; and

   (5) Comments related to pending prosecutions.

8. When using Social Media, Transit Police Personnel will act in a professional manner consistent with the Transit Police Commitment and Values, the *Police Act*, and in compliance with relevant legislation. Transit Police Personnel will not disclose any information that is confidential or proprietary to the Transit Police, its law enforcement partners, TransLink or any third party who has disclosed information to the Transit Police, without permission of the applicable party, or as otherwise permitted by Transit Police policy.

9. The content of the Transit Police Social Media accounts will adhere to applicable laws, regulations and policies, including, but not limited to, the *Freedom of Information and Protection of Privacy Act* and the Transit Police media, information technology and records management policies.

   (1) Transit Police Personnel must consult with the Information Management Analyst and/or Transit Police Senior Legal Counsel when release of personal information (including images) is being considered.

10. Transit Police Personnel will promptly notify their Supervisor upon becoming aware of or having knowledge of a posting or any website or webpage that violates the provisions of this policy; or any situation where information, pictures or data representing the Transit Police is posted to an unapproved site or account. The Supervisor will be responsible for reporting to the Deputy Chief Officer

Administrative Services and Senior Manager Strategic Services of any such policy violations.

11. The Transit Police will provide appropriate training to Transit Police Personnel assigned Social Media functions on behalf of the organization or conducting investigations using Social Media.

PROCEDURES

Transit Police Non-investigative Use of Social Media

12. Using the official approval form (Form AZ0880 – General Account Authorization), Transit Police Personnel will obtain permission from the Senior Manager Strategic Services prior to representing the Transit Police via a Social Media account in the performance of an authorized duty. Unless already directly assigned by the Senior Manager Strategic Services, Transit Police Personnel will be required to submit a request to the Senior Manager Strategic Services detailing:

    (1) The purpose and anticipated outcome of the Social Media presence;

    (2) The social media platform to be used, equipment required, and availability of funds (if applicable) within the section;

    (3) The target audience;

    (4) The plan to monitor the social media platform, including the vetting and capturing of inappropriate and/or investigative information; and

    (5) Any other relevant information.

13. Unless otherwise so determined by the Chief Officer, the Strategic Services Section will be responsible for regularly monitoring of all approved Transit Police Social Media accounts in order to ensure appropriate usage and representation of the Transit Police. The Senior Manager Strategic Services may order deactivation of a Transit Police Social Media account, and will inform the Chief Officer upon a deactivation of account.

    (1) The Senior Manager Strategic Services will maintain a list of Social Media accounts approved for Transit Police business, as well as retain in records the approved Forms AZ0880.

14. Where possible, each approved Transit Police Social Media account will:

    (1) Include a link to the Transit Police website;

    (2) Include an introductory statement that clearly specifies the purpose and scope of the Transit Police presence on the website;

(3) Prominently display the Transit Police contact information to ensure an avenue for prompt follow up to any submitted information or intelligence; and

(4) Notify users requiring emergency assistance to contact 911.

15. Transit Police Social Media, where the public can add comment, will state that the opinions expressed by visitors to the page(s) do not necessarily reflect the opinions of the Transit Police. Pages will need to clearly indicate that posted comments will be monitored and that the Transit Police reserves the right to remove obscenities, off-topic comments, and other inappropriate material; and that any content posted or submitted for posting is subject to public disclosure.

16. The Transit Police will endeavour to only use any likeness or reference to any Transit Police Personnel, on any Social Media site, with the staff person's consent. Should a staff person find their likeness has been used, or they have been referenced on any Transit Police Social Media site without their consent, they may request the removal of same by submitting a written request containing the particulars to the Senior Manager Strategic Services.

    (1) Given the public service nature of Transit Police work, it is expected that on-duty photographs of Members may be taken and used internally as well as for external promotional purposes. However, the Transit Police will maintain a Photograph Prohibition List in consideration of those Transit Police Personnel who are working in specialized positions/assignments for which they need to ensure privacy of their image/information for investigative and security reasons. Transit Police Personnel planning to apply to such a specialized position/assignment in the future may also request to be placed on the Photograph Prohibition List (following the prescribed process).

17. Transit Police Personnel should be aware that an individual may be subject to civil litigation for:

    (1) Publishing or posting false information that harms the reputation of another person, group or organization (defamation);

    (2) Publishing or posting private facts and personal information about someone without their permission that has not been previously revealed to the public, is not of legitimate public concern, and would be offensive to a reasonable person;

    (3) Using someone else's name, likeness, or other personal attributes without that person's permission for an exploitative purpose; or

    (4) Publishing the creative work of another, trademarks, or certain confidential business information without the permission of the owner.

18. Transit Police Personnel are encouraged to exercise sound judgment on usage, and maintenance and discretion in contributing to Social Media sites where information is available to numerous users. This is especially encouraged on personal sites to ensure a distinct separation between personal and organizational views.

19. Transit Police Personnel should be aware that social networking sites will be monitored and, if found to be used inappropriately, that disciplinary action may result for the involved Transit Police Personnel.

20. Social Media content (Transit Police or personal) communicated using Transit Police equipment and technology is subject to public records laws and all relevant records retention schedules apply to this content.

21. Any intelligence received through the use of Social Media will be forwarded to the Watch Commander or designate for follow up as soon as possible.

22. Those Transit Police Personnel authorized to represent the Transit Police on a Social Media site for non-investigative purpose will:

    (1) Conduct themselves at all times as representatives of the Transit Police and adhere to the *Police Act,* the *Criminal Code of Canada,* Transit Police and TSML policies and standards of conduct and professional behaviour;

    (2) Observe and abide by all copyright, trademark, and service mark restrictions in posting Transit Police Images and other materials to electronic media;

    (3) Identify themselves as staff of the Transit Police; and

    (4) Not make statements about the guilt or innocence of any suspect or arrestee, or comment on pending investigations or prosecutions, nor post, transmit, or otherwise disseminate confidential information related to the Transit Police.

        a. Any exception to s. 22(4) will require the Transit Police representative to obtain authorization from the Senior Manager Strategic Services prior to making a post (the Senior Manager Strategic Services will consult with Operations, Legal Services Section, and Executive as appropriate to the matter.)

Transit Police Investigative Use of Social Media

Investigations

23. This policy is not intended to limit the use of any Social Media site or resource to gather information or intelligence at the “apparent/overt use” engagement level; for example, where the Transit Police is not required to create a profile or account, such as browsing twitter feeds, open Facebook pages, or any other open source information.

24. Transit Police Personnel will need to obtain authorization before creating profiles or accounts on any Social Media site(s) for investigative purposes. This includes, but is not limited, to: missing persons, wanted persons, criminal intelligence, covert accounts/personas, and crimes perpetrated online (e.g., cyber-bullying, cyber-stalking, sexual predators); and photographs or videos of a crime, posted by a suspect or witness.

(1) The investigating Member will submit an authorization request using Transit Police form OZ0420 for a "discreet use" account and form OZ0380 for a "covert use" account.

(2) The authorizing Watch Commander may confidentially inform the Senior Manager Strategic Services of creation of profiles or accounts on Social Media for investigative purposes, as appropriate.

[Refer to Transit Police SOP46 – Social Media Use and Appendix A for Social Media Guidelines, and Transit Police forms OZ0380 and OZ0420 for additional information and requirements.]

25. When Social Media is used for Transit Police investigative purposes, such use will be recorded by the investigator in the relevant General Occurrence (GO) report and information gathered will be recorded and retained in conjunction with the security requirements and retention provisions applicable to the investigation, and as required by law. (Where appropriate, consider if the file should be made "private" or "invisible" on PRIME, in particular where "discreet use" and "covert use" accounts are established. Refer to Transit Police Policy AF130 – Making Records Private and Invisible.)

    (1) To confirm authenticity of the information gathered, the investigator will need to place into records the following, but not limited to: screen capture, hash value and date/time stamp. The Transit Police record management system designated for online investigations will be used by the investigator.

26. When using Social Media in the course of an investigation, Transit Police Personnel will take into account the following considerations:

    (1) The investigator may be asked for the complete account information, including but not limited to the name or identify used, profile or account information, any pictures, chat conversation, emails and other relevant information;

    (2) All equipment used may be subject to a subpoena or disclosure request;

    (3) The investigator may be required to disclose or testify with regards to their computer experience, technical knowledge, ability and training in technology, the Internet and Social Media; and

    (4) The investigator may be required to testify with respect to the legal requirements or terms of use policies and privacy rights of individuals who post information on social networks where such information may or may not be protected under Canadian law.

27. When "discreet use" or "covert use" accounts are established for investigative purposes, the investigator will make a hard copy operational record of the account information, user names, and passwords to prevent the loss of critical investigative information. The investigator will secure the record in a sealed envelope, marked with the project name (or number), date, investigator name, and list of persons authorized to access the record. The investigator will submit the sealed envelope, via their Watch Commander, to the Inspector Operations in charge of the General

Investigation Unit (GIU), for securing in a restricted/locked filing cabinet or safe designated in the GIU area. This protocol may be amended in the manner prescribed by the Deputy Chief Officer Operations to address operational and security requirements.

28. The use of "discreet use" and "covert use" accounts must be conducted from an approved or covert computer/electronic device to prevent the discovery of the police investigation by tracking the account to a Transit Police computer. The Transit Police IT Unit will be consulted to provide guidance and advice to Transit Police officers seeking use of this resource.

29. Where a "covert use" account is developed with the intention that it will be used to facilitate an in-person/undercover (UC) operation, the creation and use of that account will only be undertaken in consultation with the BC Municipal Undercover Program and the police of jurisdiction. The Inspector Operations or designate will be required to maintain a record of the consultation and outcome.

Recruiting and Security Clearances

30. Any use of Social Media (other than the Transit Police official accounts) for recruiting outreach purposes requires the authorization of the Senior Manager Strategic Services (and Senior Manager Human Resources when related to exempt staff recruitment), unless otherwise determined by the Chief Officer.

31. When using Social Media for hiring background investigations, the following procedures apply:

    (1) The Transit Police may include publically available Internet-based content searches when conducting background investigations of potential employment candidates; and

    (2) The search methods and vetting techniques will be applied uniformly to all candidates.

32. When conducting hiring background investigations and security clearances, Transit Police Personnel will attempt to ensure that information gathered from Internet-based sources is confirmed through secondary sources. If it cannot be confirmed, it must be recorded as such.

Personal Use of Social Media by Transit Police Personnel

33. Transit Police Personnel are free to express themselves as private citizens on Social Media sites. However, as Transit Police Personnel have a fiduciary duty to the Police Service and legal employer, personnel should guide their actions accordingly. A Transit Police staff person's expression must not: impair working relationships of the Transit Police; compromise confidentiality; impede the performance of their or another staff person's duties; impair discipline; reduce workplace harmony amongst co-workers; ridicule, malign, disparage, or otherwise express bias against any race, religion; or, be likely to negatively affect the public perception or reputation of the Transit Police. Members must also be mindful of the code of conduct provisions of the *Police Act*.

NOTE: See TSML Policy No. 001 – Director and Employee Code of Conduct, Transit Police Policy AB100 – Respectful Workplace, and TransLink Enterprise – Acceptable use of Corporate Computing Systems.

34. Transit Police Personnel will not post to their personal Social Media any photographs, video, audio or other media that was captured or related to on-duty activities, without obtaining through the chain of command, written permission from the Senior Manager Strategic Services or Chief Officer.

35. Transit Police Personnel will not post, transmit, or otherwise disseminate on Social Media any information to which they have access, as a result of their employment, without obtaining through the chain of command, written permission from the Senior Manager Strategic Services or Chief Officer.

36. When communicating on Social Media in their private lives, all Transit Police Personnel will be strongly cautioned against disclosing their employment/occupation with the Transit Police. Further, Transit Police Personnel should use caution when disclosing their own personal information such as names, dates of birth, addresses, hometown, family information and any other personal identification information. (It is recommended that Transit Police Personnel review section 1 of Appendix "A" of SOP46 - Social Media.)

37. Transit Police Personnel will not be permitted to post information pertaining to any other Transit Police Personnel without that staff person's permission.

38. In consideration of this policy and provisions within, Transit Police Personnel are cautioned against:

    (1) Posting personal photographs or providing similar means of personal recognition which would be prejudicial to the maintenance of discipline or likely to discredit the reputation of the Transit Police and its personnel. If in doubt, personnel should consult their Supervisor;

    (2) Posting any form of visual or personal identification if the staff person works, or may reasonably be expected to work, in undercover operations, or any area where such identification may compromise their personal safety, the safety of other personnel or the integrity of any investigation;

    NOTE: A Member who openly posts personal information on Social Media which identifies them as a police officer must accept that such exposure may limit their ability to work in covert and undercover capacities in the future.

39. The Transit Police reserves the right to request Transit Police Personnel to remove any such photograph or representation which the Transit Police deems to be inappropriate.

40. Due to the ease of access and global exchange of information, Transit Police Personnel must be cognizant that their communications may be exposed to breaches of confidentiality, the privacy of individuals may be threatened and their communications subpoenaed for court purposes. Commentary offered off-duty may

be mistakenly associated to a police officer professionally. Accordingly, while off duty, Transit Police Personnel are prohibited from the following:

(1) Speech involving themselves or other Transit Police Personnel which reflects behaviour that would reasonably be considered reckless or irresponsible;

(2) Engaging in speech that may provide or be utilized as grounds to undermine or impeach an officer's court testimony or credibility; and

(3) Divulging information gained as a result of their authority or employment, making any statements/speeches/appearances/endorsements or publishing materials that may reasonably be considered to represent the views or positions of the Transit Police, without express authorization (Senior Manager Strategic Services or Deputy Chief Officer Administrative Services).

41. As privacy settings and Social Media sites are constantly in flux, Transit Police Personnel are cautioned that all information posted on such sites may be subject to public viewing. Personnel must be aware that any material they post on Social Media sites becomes the property of the individual site, and may be used for a purpose unintended (e.g., advertising).

42. Transit Police Personnel will be cautioned that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by any person or organization including defence counsel, Crown Counsel or the Transit Police at any time, without prior notice.

Complaints on Transit Police Social Media Sites and Pages

43. Complaints regarding Transit Police Personnel should not be reported on the Transit Police Social Media sites, but rather via the way identified on the Transit Police website ("Contact Us" page). If a complaint is received on a Transit Police Social Media account, Transit Police Personnel will handle the complaint according to the current Transit Police complaint procedures (see Transit Police policy: AC140 – Complaints).

44. In the event that the complainant names a specific Transit Police staff person, or is particularly controversial or of a sensitive nature, the Transit Police representative assigned to that Transit Police Social Media site will:

(1) Make a screen capture, and forward the complaint to the Transit Police Professional Standards Unit;

(2) Post a new comment to the Social Media post to inform the complainant and other followers of the existence and purpose of the Professional Standards Unit, sharing contact information for the Unit; and

(3) Consult with the Senior Manager Strategic Services and Deputy Chief Officer Administrative Services, as appropriate to the complaint matter.

Review

45. At least annually, the appointed Transit Police subject matter expert (or external person where so determined by the Deputy Chief Officer Administrative Services) will conduct a review of online investigative use by Transit Police Personnel for compliance with policy and legal requirements.

46. Review reports and any recommendations will be submitted to the Deputy Chief Officer Administrative Services and Deputy Chief Officer Operations.

Investigator Training Requirements

47. The Deputy Chief Officer Operations will determine any necessary training that a Member is required to take in order to be approved to operate a “discreet use” or “covert use” investigative account.

48. A Training Log will be maintained by the Training Section identifying those Members who have completed the required training.

References

Police Act, [RSBC 1996], c. 367
Transit Police Policy: AB100 – Respectful Workplace
Transit Police Policy: AC140 – Complaints
Transit Police Policy: AF130 – Making Records Private or Invisible
Transit Police Policy: AF160 – IT Access Control
Transit Police Policy: OM010 – Media Relations
TransLink Enterprise Policy E-01: Acceptable Use of Corporate Computing Systems [March 2017]
TSML Policy No. 001: Director and Employee Code of Conduct [July 2013]
Int’l Association of Chiefs of Police (jointly produced by Center for Social Media and National Law Enforcement Policy Center) model policy on social media [2010]
R. v. Hamdan, 2017 BCSC 867 (CanLII) [2017-05-24]