Attachment I

Queensland Police Service

Use of Social Media Policy

Version 1.2 – 2021

Contents

1. Introduction

1.1 Policy statement

1.1.1 The Queensland Police Service (Service) has a strong tradition and is committed to social media as a channel for service delivery and public engagement. Social media permits timely information sharing to help keep our community safe. Organisational benefits include community assistance with investigations and/or operations, enhanced transparency, accountability, public engagement and confidence, and shaping of public perception.

1.1.2 The Service recognises and respects the rights of its members to participate on social media for official, professional, and personal or non-work-related purposes.

1.1.3 Official use of Service social media shall be professional and aligned with the vision, values and purpose of the QPS Strategic Plan. However, members must ensure all use of social media, whether official, professional or personal, is consistent with respective codes of conduct, standards of practice, and procedural guidelines outlined at s. 1.3.2 below.

1.1.4 This policy should be reviewed every two years by the policy owners, Media and Public Affairs.

1.2 Application

1.2.1 This policy applies to all members, on or off duty, on leave (with or without pay), including permanent, temporary, casual and volunteer employees. It also applies to those on secondment to and/or from the Service, and contractors working within or for the Service.

1.3 Scope

1.3.1 This document sets policy on:

- the official use of Service social media platforms to achieve organisational goals;
- the governance framework for official Service social media platforms;
- risk management strategies relating to information security, privacy and intellectual property infringement;
- operational considerations for Service social media issue and crisis management;
- the standards required of members authorised to represent the Service on social media; and
- personal use of social media by members.

1.3.2 This policy is to be read in conjunction with:

- *Police Service Administration Act 1990* (PSAA);
- *Public Sector Ethics Act 1994* (PSEA);
- Code of Conduct for the Queensland Public Service (Code of Conduct);
- Standard of Professional Practice; and
- Media Guidelines.

1.3.3 This policy is also to be read in conjunction with the Queensland Government Social Media Guide developed by the Department of the Premier and Cabinet (DPC), applicable to all Queensland Government departments and agencies.

1.3.4 The External Digital Media Strategy guides and informs how we utilise social media. The strategy specifies activities, benchmarks best practice and measures of success. Challenges and future opportunities are identified to promote agility and flexibility to confront the everchanging social media landscape.

1.4 Objectives

1.4.1 The objectives of this policy are to:

- develop acceptable use standards and governance for participation on social media;
- build social media expertise and skills, establish best practice and streamline approval processes; and
- enable the planning of adequate resources to develop, support and maintain social media activities around identified business needs.

1.4.2 The objectives of official use of social media are to:

- encourage public assistance in crime prevention, investigation, detection and disruption;
- provide information which contributes to public safety;
- raise public awareness to promote community perceptions of safety;
- engender community confidence in police by publicising examples of good work;
- enhance organisational reputation;
- extend organisational reach by leveraging this growing digital platform; and
- build community partnerships through social media engagement.

1.4.3 This policy does not supersede existing provisions relating to assumed identities for investigative or intelligence purposes (refer s. 9 of this policy); or replace traditional modes of communication and engagement with the community (refer s. 7.5 of this policy).

1.5 Key principles

1.5.1 The Service shall comply with the Queensland Government Enterprise Architecture (QGEA) Principles for the use of social media networks and emerging technologies.

1.5.2 Members who administer or contribute to official social media or third-party sites in an official or professional capacity are to:

- be apolitical, impartial and professional;
- be respectful and courteous
- deal appropriately with information, recognising that some information must remain confidential, such as personal and/or operational information as well as that classified sensitive or protected;
- be inclusive and sensitive to diversity within the Queensland public;
- avoid conflicts of interest;
- make proper use of Service resources; and
- uphold the Code of Conduct, Service values and the integrity and good reputation of the Service.

1.5.3 Members who administer or contribute to a social media or third-party site for personal or non-work-related reasons in a private capacity are to:

- avoid conflicts of interest; and
- uphold the Code of Conduct, Service values and the integrity and good reputation of the Service.

1.5.4 The Code of Conduct and the Standard of Professional Practice do not preclude a member from contributing to public discussions on community and social issues in a private capacity provided

reasonable steps are taken to ensure that the commentary is clearly represented as their personal views and not those of the Service and/or the Government.

2. Social media overview

2.1 Definitions

2.1.1 The term social media is defined as websites and applications that enable users to create and share content or to participate in social networking[1]. By its very nature social media is not a 'broadcast only' communication channel and encourages people to engage in two-way communication. Social media is immediate, and responses need to be timely.

2.1.2 Social networks (e.g. Facebook) and messaging applications (e.g. Messenger, WhatsApp) allow registered users to create profiles, share information, upload photos and videos, send messages, and connect with other users. Globally, Facebook is the largest social network. It provides a space for sharing agency content and building a following of campaigns and activities. Groups can also be created to communicate shared interests within a closed online community. Messenger and WhatsApp are subsidiaries of Facebook.

2.1.3 Micro-blogging sites (e.g. Twitter) allow registered users to publish and share short messages that can include images, videos or online articles. Twitter enables engagement with a large number of people in a targeted way. It allows members to broadcast or share 'tweets' or short messages through status updates. Users can follow people, organisations or hashtags (#) denoting a certain topic of interest. Short messages are required in Twitter using shortened links to promote specific campaigns, events, activities, articles, expertise etc.

2.1.4 Professional social networks (e.g. LinkedIn) are designed primarily for the business community. They allow registered users to establish and document networks of people they know and trust professionally and build relationships with people who are interested in what the agency does. Groups and pages can be created to communicate agency messages with targeted audiences, for example future employees or industry experts. It also allows broadcasting of messages like other social networking sites.

2.1.5 Image broadcasting and publishing sites (e.g. YouTube, Instagram, Flickr) allow users to upload and share videos and photos, and post comments about them. YouTube allows the creation of channels for showcasing videos, activities and external videos that may relate to agency content. Instagram provides agencies with an effective way to distribute, share and promote images and videos and is growing in popularity. Slideshows of images can be shared on Flickr, a photo management tool.

2.1.6 Opinion based sites (e.g. myPolice Queensland Police News (myPolice News)) permit users to build weblogs to provide lengthy commentary, news, editorials or opinion. Users can subscribe to receive blog postings as email alerts.

2.2 Official use of social media

2.2.1 Official use of social media[2] is any use of a Queensland Government-managed social media account, profile or presence by an authorised user. Comments made through the official social media accounts are representative of the agency and made by those authorised to do so. Official social media represents the Service from either a corporate, regional or district perspective. The use of social media and digital engagement should be held within a wider communication and engagement strategy and should not be a replacement for traditional media or engagement activity.

2.2.2 Official use of social media shall be conducted by members who have received requisite training, with demonstrated commensurate skills and experience. Media and Public Affairs (MPA) shall provide and/or coordinate training for Members approved and authorised to administer in an official

[1] QGEA Glossary https://www.qgcio.qld.gov.au/publications/qgea-glossary/social-media-definition

[2] QGEA Glossary https://www.qgcio.qld.gov.au/publications/qgea-glossary/official-use-of-social-media-definition

capacity, corporate, regional or district level social media. Authority to use official Service social media accounts is limited to MPA members and appointed administrators of regional/district Facebook pages and myPolice News pages upon successful completion of requisite training.

2.3 Professional use of social media

2.3.1 Professional use of social media[3] (e.g. LinkedIn) is based on a person's area of expertise and association with other practitioners in that field. Care should be taken by the members not to disclose any classified or inappropriate information. Members should provide disclaimers disassociating their views from those of the Service and provide a general statement that it is general information only and not to be relied upon as an official source.

2.4 Personal use of social media

2.4.1 Personal use of social media[4] is defined as individual or private use and not attributable as an official or professional use. Official social media profiles and profiles based on Service email addresses are not to be used for personal social media publication or interaction.

[3] QGEA Glossary https://www.qgcio.qld.gov.au/publications/qgea-glossary/professional-use-of-social-media-definition

[4] QGEA Glossary https://www.qgcio.qld.gov.au/publications/qgea-glossary/personal-use-of-social-media-definition

3. Representing the Service on official social media

3.1 Rules

3.1.1 If authorised to use official social media on behalf of the Service, members are to:

- ensure any content they publish is factually accurate;
- obtain relevant approvals for the release of information, including images, as outlined in the Media Guidelines;
- not commit the Service or the Government to any action or initiative unless they have the authority to do so;
- not disclose confidential information or information classified Sensitive or Protected;
- not disclose personal information unless it can be justified on the grounds that the information is being published for legitimate operational and/or law enforcement functions (see the *Information Privacy Act 2009* (IPA));
- refer community members to relevant agencies for advice and support about topics that fall outside their area of responsibility or expertise;
- not make comments or perform an online action (such as sharing or liking) that would bring the Service into disrepute or embarrassment, or would imply commercial endorsement of an organisation, product, service or activity;
- use images that uphold the values and good reputation of the Service, or if used as part of an engagement strategy are in good taste and relevant to official messaging;
- ensure messaging aligns with current Service and Government initiatives and campaigns;
- not criticise the decisions, policies or practices of the Government, the Service or other agencies;
- not influence support for a political party, such as advocating or criticising the statements, policies or promotional activities of political parties or politicians;
- be courteous, impartial, professional and respectful of all individuals and communities online;
- not use insensitive, inflammatory, condescending or other socially unacceptable or offensive language;
- not publish material likely to result in criminal penalty or civil liability;
- not publish any material that is prejudicial, defamatory, bullying, libellous, discriminatory, harassing, obscene or threatening;
- exercise care if referring to pending court proceedings to avoid publishing material that may prejudice those proceedings or breach a court suppression order, or breach an individual's privacy;
- acknowledge copyright and attribute the source of material shared. Do not publish any material that infringes intellectual property, copyright or a trademark;
- obtain the permission of members or community members before posting images of them (see s. 3.2.11 of this policy); and
- not publish images or otherwise identify undercover or surveillance operatives, or other persons with suppressed identities.

3.2 Content

3.2.1 Official Service social media should include the following:

- an introductory statement that clearly specifies the purpose and scope of the Service presence on the site;

- a statement that confirms the page is maintained by the Service;
- for regional/district sites, a disclaimer notice that clearly states the page is not monitored at all times;
- information on how members of the public can contact police for emergency and routine calls for service;
- where the platform allows, a note that states the opinions expressed by visitors of the site do not reflect the opinions of the Service;
- links to official Service websites; and
- explanatory notes outlining terms of use and moderation of public comments.

3.2.2 The Service is bound by the Queensland Government corporate identity system to maintain the Queensland Government visual brand, and build government recognition, trust and transparency. Communication Services, DPC, oversees the administration of the Government's visual brand. The Queensland Government Advertising and Marketing Communication Code of Conduct provides guidance on the expectations and responsibilities of communicating as public sector organisations.

3.2.3 Use of the Service logo on social media must comply with s. 9.5: 'Use of Service logo' Management Support Manual (MSM). External use of the Service logo is to be authorised by the Executive Director, Communications, Culture and Engagement (CCE) Division. Only approved versions of the Service logo are to be used.

3.2.4 Use or sharing of unauthorised content could lead to breach of copyright and removal of content. Only Service owned or authorised images, video and audio are to be published. Refer to s. 7.2: 'Intellectual Property' of this policy.

3.2.5 Content should balance operational need for sharing with public interest or disinterest. The objective is to continually build and maintain a following invested in Service messaging through timely responses and engagement with users. Content should be relevant to Service priorities and be linked to the five social media content pillars outlined in s. 3.2.8 of this policy. Outputs should be accurate, up to date and relevant, with a regular flow of new content to maintain user interest. Content such as an appeal should be updated or removed as soon as it becomes outdated. Regular reviews should be conducted to identify any content that is out of date.

3.2.6 Any information, messages, comments, images or videos posted should serve a clear organisational and/or policing purpose. Every opportunity should be used to promote Service key messages around reassurance and keeping people safe. Official social media should be used to share positive community-minded stories which enhance the Service reputation and reflect the good work members do in their community and to inform the public of upcoming events such as road closures.

3.2.7 Options for posting operational or proactive content include:

- text posts to newsfeed;
- images accompanied with text;
- video posts;
- livestreaming;
- story posts; or
- sharing content from other agencies.

3.2.8 The five social media content pillars are described as:

1. QPS human touch (personal, humanising staff, relatable content, relaxed, funny, 'punny', light-hearted);
2. urgent communications (time crucial, high priority, urgent, important, evacuations, natural disasters, missing persons, Amber Alerts);

3. campaigns and education (affirming presence in community, road safety, proactive, education of laws);
4. news updates (inform of incidents or updates, less time crucial, notifying community, arrests, crime, deaths, traffic alerts/road updates); and
5. citizen engagement (appeals for information).

3.2.9 For regional/district level social media, all content should meet Service standards of professionalism and be subject to regional approvals. When in doubt, approved authors for regional/district Facebook and myPolice News pages should seek advice from MPA for vetting and quality assurance of content.

3.2.10 Service video content, including body worn, Polair, dashcam, portable device or CCTV footage, shall be edited, marked with Service branding and be subject to regional, command or senior executive approvals, as appropriate, before publishing on corporate level social media.

3.2.11 To publish images of members or third parties on official Service social media channels for proactive or extended media or marketing campaigns, written consent must be obtained from the individual/s concerned. Informed consent must be obtained from a parent or guardian for use of images of children. Under no circumstances should identifiable images of children suspected of criminal conduct or at risk of harm, be placed on social media.

3.2.12 For members, vetting should be conducted by Ethical Standards Command with approval granted prior to release. For external parties, a Queensland Government Film/Photo Consent form should be signed and lodged with MPA. Consideration should be given to the future operational impact of posting images of members and appropriate vetting must be undertaken if the image is being used to promote the Service brand or services.

3.3 Principles for effective social media content

3.3.1 In determining appropriate content for official use, the six key principles for effective social media should be considered:

1. *Content is king but context is key* – each social media channel should be exploited differently to appeal to various audiences;
2. *Use channels to engage* – content should provide value to the audience using two-way interaction where possible;
3. *Be concise* – aim to deliver key messaging in as few words as possible to cut through social media noise;
4. *Be consistent* – every post on social media is a representation of the Service. Be consistent in tone, look and feel. Refer to the Media and Public Affairs social media style guide;
5. *Be accountable* – where possible, follow up with or answer public enquiries when posting content that engages the audience; and
6. *Be confident* – in tone and responses as the voice of the Service.

3.3.2 Other general considerations for posting content include:

- keep captions short and provide a link to myPolice News for more information;
- remain professional in communications and avoid being too casual;
- use approved Service writing style for dates, time and locations and correct grammar, spelling and punctuation. See the Web Writing and style guide;
- quality over quantity as social media platforms may use algorithms which penalise too frequent posting;
- establish a consistent persona for posting so users identify a single voice and tone;
- use consistent language and terminology across posts;

- seek approval from partner agencies before posting information involving those agencies;
- content deemed likely to raise criticism of police, be controversial or be received negatively should be escalated to the senior executive for briefing and approval prior to publishing;
- a risk assessment should be conducted prior to publishing such content as to the benefit of the post and potential damage it may cause;
- a nominated spokesperson should be briefed prior to publishing such content to allow time to prepare response/s for follow up media enquiries;
- positive content deemed likely to generate heightened interest should involve chain of command and social media moderator briefings; and
- be aware of sentiment/sensitivities surrounding issues, current events and media climate to assess appropriate timing of release to avoid being taken out of context.

3.4 Corporate level social media

3.4.1 The Service, through MPA, operates corporate level social media platforms. Centralised operation engenders good governance, risk management, resourcing, training, and quality control of social media content and Service messaging.

3.4.2 Service corporate social media platforms include:

- QPS Facebook;
- QPS Instagram;
- QPS Twitter;
- QPS myPolice News;
- QPS Livestream;
- QPS YouTube;
- QPS Pinterest; and
- other platforms as occasionally used.

3.4.3 Content, including videos, comments, text, and photographs shared to corporate level social media should have state-wide significance likely to generate wider community or media interest. Content should be tailored to the respective platform and expectation/s of the users.

3.4.4 Select police-centric community news stories, crime notifications and alerts are published online using myPolice News, a Service owned and managed platform. Suitable content includes:

- major incidents;
- serious offences;
- major events;
- proactive campaigns;
- traffic alerts;
- amber alerts;
- emergency alerts;
- appeals for public assistance;
- missing or wanted persons;
- public safety messaging;
- good police work or outcomes of operations;
- high engagement content with policing related messaging; and

- shared alerts or appeals from partner agencies.

3.4.5 Subscribers, including journalists, may elect to receive individual notifications, or a daily summary of new releases via email. MPA may share myPolice News stories using Service corporate social media platforms to expand reach to larger audiences. Similarly, regional or district Facebook page administrators may also share myPolice News stories and alerts of local interest through their respective regional/district level social media pages.

3.4.6 Applications for new corporate level social media platforms require a business case submission to and approval from the DPC.

3.5 Regional/district level social media

3.5.1 The Service, through local administrators, operates regional/district level social media Facebook pages. These pages do not need to align with established Service boundaries but should reflect broader geographical areas and/or communities.

3.5.2 There are several benefits to this approach including:

- increased opportunities for creating engaging content for a wider audience;
- increased following which enhances community reach for public messaging;
- increased rate of following growth which creates a prominent online presence and legitimacy; and
- reduced impost on individuals with shared responsibility for creating engaging content and monitoring and moderation responsibilities.

3.5.3 Applications for new regional/district level social media platforms require a business case submission to and approval from the DPC.

3.5.4 Regional/district level Facebook pages are created by MPA to ensure compliance with Government and Service requirements regarding branding and appearance. Upon successful completion of MPA delivered training, local administrators are responsible for operation and management of their respective pages including content, monitoring and moderation of public comments, metrics and outcomes reporting.

3.5.5 In line with QGov requirements MPA will apply for blue tick verification on behalf of regional/district pages. Blue tick verification provides public confidence the page is authentic, approved by the Service and meets all required privacy and security factors.

3.5.6 Content from the Service corporate Facebook page may be shared on regional/district Facebook pages where appropriate and relevant to the local community. Messaging on regional/district pages should be generally consistent with corporate level messaging.

3.5.7 Administrators of regional/district Facebook pages should undertake regular environmental scans regarding type and volume of content to ensure it meets the needs and expectations of their community.

3.5.8 The Service may be held legally liable for content and comments posted on social media. Administrators must carefully monitor and moderate comments, hiding or removing offensive material as a matter of priority.

3.6 Advertising and external links

3.6.1 Careful consideration must be given before liking or sharing links to an external site. Sharing information from partner agencies may be appropriate and necessary for example, natural disasters, major incidents or events. However, other sites may carry outdated or conflicting advice which has the potential to cause community confusion and embarrassment to the Service. Links to non-government sites should be avoided, and must avoid any implied endorsement of products, services or sponsorship.

3.6.2 The Service cannot control external advertising on social media platforms. Notwithstanding, commercial advertising is not to be published on Service social media. However, a company, individual or partner agency sponsoring an approved police activity or program may be acknowledged, without endorsing the sponsor, product or service.

3.6.3 Service paid advertising campaigns published on social media must comply with the Government Advertising and Communication Committee (GACC) guidelines to ensure campaigns align with and support government priorities.

4. Governance framework

4.1 Regional/district Facebook page approvals

4.1.1 Proposals for new regional/district Facebook pages should commence with district officer (or delegate) consultation with Inspector, MPA regarding several parameters including:

- proposed geographical area and included stations;
- identification of suitable members from those stations with the necessary skills, knowledge, and personal experience with social media to undertake requisite training and become page administrators;
- a page name that best reflects the community identity;
- verification there is no existing Facebook page which can adequately represent the community, including corporate and/or regional/district pages; and
- an understanding successful administration of social media platform requires sustained effort, which may impact service delivery including core frontline duties.

4.1.2 Upon satisfaction of the above, MPA will prepare a business case submission seeking Commissioner support for the establishment of a new social media presence (see s. 3.4.6 of this policy). DPC approval must be received before any proposed page is to go live. The business case submission must address the following key criteria:

- the objectives of the page and benefits to the local community;
- identifying the target audience;
- type of content relevant to the page;
- risk mitigation strategies including Privacy Impact Assessment;
- capability for monitoring and moderation;
- appropriate resourcing and staffing, supervision and ability to escalate issues within the chain of command;
- proposal for implementation and on-going management; and
- evaluation, metrics and outcomes reporting.

4.1.3 Upon DPC approval, MPA will:

- create the respective regional/district Facebook page;
- create appropriate branding/graphics;
- deliver training to the proposed page administrator/s; and
- handover operation and ongoing responsibility for the new page to the local administrator/s.

4.1.4 A regional or district point of contact (POC) is to be appointed as the senior administrator, and as a primary POC to assist MPA with timely resolution of any identified issues.

4.1.5 The authority to decommission a regional/district Facebook pages rests with the regional assistant commissioner in consultation with the Director, MPA.

4.2 Quarterly reporting

4.2.1 Page administrators are to submit a quarterly report to their respective Assistant Commissioner, with a copy referred to MPA for central collation. The report will address the metrics and outcomes criteria listed in the DPC social media governance checklist.

4.2.2 MPA will coordinate a collated agency response as required by DPC. The primary key performance indicator examines performance metrics embedded within the platform to ensure appropriate growth, reach and engagement levels are maintained. A key component is assessment against peer law enforcement agencies to ensure consistent growth in followers and engagement levels.

4.2.3 Accounts which fail to maintain appropriate growth, reach and engagement levels will be subject to review and potential closure in line with the DPC social media guidelines.

4.3 Monitoring and moderation

4.3.1 Moderation is the method to review and address comments which are irrelevant, misleading, offensive, obscene, illegal, insulting or in breach of platform conditions of use. Moderating is often time intensive, and adequate resourcing must be provided to ensure the Service meets its responsibility to actively monitor, moderate and respond to social media posts. Not all comments critical of police or the government should be hidden or deleted. Seek MPA advice if unsure. Examples of comments that should be hidden or removed include:

- inciting violence or hatred;
- irrelevant comments which detract attention from the intended message;
- ridiculing the appearance or names of people depicted in images or videos;
- victim blaming;
- fake news;
- links to other sites;
- online ‘sparring’ where users become engaged in unconstructive arguments; and
- racism, sexism, homophobia, transphobia etc.

4.3.2 Effective moderation minimises reputational harm. Importantly, it also reduces the risk of organisational liability. In 2019, the New South Wales Supreme Court (*Voller v Nationwide News Pty Ltd; Voller v Fairfax Media Publications Pty Ltd; Voller v Australian News Channel Pty Ltd [2019] NSWSC 766*) ruled that companies may be considered publishers of third-party comments on their respective Facebook pages. The decision has wide-ranging implications for organisations which may now be held responsible for content posted by users on their social media pages. In 2020, the NSW Court of Appeal upheld this decision.

4.3.3 A catalogue of pre-prepared responses may assist with frequently encountered comments and questions, particularly when posting potentially contentious posts likely to generate significant engagement. Examples include:

- advising users not to report crime on social media and providing information as to official reporting methods;
- providing reporting and support information for domestic and family violence and self-harm reports;
- providing website links for police recruiting information; and
- advising users on how to provide feedback on the performance of the Service.

4.3.4 MPA and Policelink jointly moderate Service corporate level Facebook and Twitter accounts, initially focussing on comments requiring an operational response; then secondly a scripted reply; and finally Facebook comments that need to be hidden. Communication should occur between MPA and Policelink when time critical moderation is required for posts such as:

- high risk missing persons;
- Amber Alerts;
- community BOLO announcements; and

- situations likely to generate high levels of calls for service or inappropriate and/or offensive conduct.

4.3.5 Administrators of official Service social media are permitted to ban users who engage in spam, extreme or repetitive inappropriate or offensive conduct. Details of banned users and the reasons why they were banned are to be recorded in line with *Public Records Act 2002* (PRA).

4.3.6 Further government guidance regarding moderation policies and processes are provided in Principle 11: 'Official social media accounts will be monitored and moderated regularly' of the Queensland Government Enterprise Architecture (QGEA) framework's Principles for the use of social media networks and emerging technologies.

5. Information management and security

5.1 Information management principles

5.1.1 Principle 8: 'Correspondence received via official social media accounts are considered official correspondence and shall be treated as such' of the Principles for the use of social media networks and emerging technologies legitimises social media communications as official correspondence. Principle 9: 'Social media activities are subject to relevant recordkeeping policy and procedures' stipulates that social media activities be subject to relevant record keeping policy and procedures. In this regard, records created through the use of social media should be captured and managed in accordance with *the* PRA, IPA, *Right to Information Act 2009* (RTIA) and the Service records governance policy. Administrators are required to implement appropriate record keeping and archiving methods.

5.1.2 Complaints received through official social media channels shall be handled in accordance with s. 6A.1: 'Duty concerning misconduct and other grounds for disciplinary action' of the PSAA.

5.2 Information security

5.2.1 Members are not to use private email accounts or systems and messaging applications for Service-related business. As provided in s. 5.3: 'Use of Service email' of the MSM and Public Service Commission Private Email Use Policy, the use of such accounts poses a security risk and prevents the proper management of records.

5.2.2 In order to minimise the risk of a security breach, recommended measures outlined in Principle 12 of the (QGEA) Principles for the use of social media networks and emerging technologies must be adhered to, including:

- direct access to State Government social media accounts should be restricted to a very limited number of skilled social media officers. All other activity should be conducted through a social media management tool;
- agencies should establish a central register of official social media accounts detailing:
    - social media channel;
    - the account's purpose;
    - area/division that manages the account;
    - officers authorised to access the account; and
    - account holder details sufficient to enable continuity of access by the agency;
- all computers and devices that access social media channels should be updated for:
    - the operating system;
    - software, such as Java and Adobe Flash;
    - browsers, including at least one alternative to Microsoft Internet Explorer; and
    - security suites;
- computers and devices should be password protected to prevent unauthorised access, including personal devices or home computers;
- devices that can be lost or stolen (phones, tablets, laptops) should have remote tracking and wiping software installed where possible;
- social media management systems that are used to manage Queensland Government social media accounts should not be used for personal accounts, even if the service has the capacity to separate personal and work account management;
- email accounts that are associated with social media channels should either be official email accounts controlled by the social media team, or if webmail accounts (e.g. Gmail), they should use two-factor authentication;

- a password manager should be used with unique, complex passwords generated for each social media account and webmail (if necessary). Passwords should never be written down, only managed using the password manager;
- all social media passwords should be changed if there is a change to social media staff as per agency procedures relating to social media passwords;
- two-factor authentication should also be implemented whenever possible as security of social media log in accounts is paramount; and
- social media channels should never be accessed using public kiosks or other untrusted, or shared devices.

5.2.3 The IPA, the PSEA, *the* PRA and the Code of Conduct require that information be managed responsibly. The Queensland Government Information Security Standard IS 18 requires agencies to identify and manage risks to information. Information classified Sensitive or Protected is not to be publicly disclosed, via social media or any other platform or means.

5.2.4 For security reasons, except for an approved social media management system and associated applications, social media users should not give any third-party applications access to their accounts. Location services on social networks should be turned off to protect operational security.

5.2.5 As a minimum standard, all Service official social media accounts must be protected by two-factor authentication with regimens in place to protect and regularly update passwords (see s. 5.2.2 of this policy).

6. Issue and crisis management

6.1 Service social media for public messaging

6.1.1 Social media is recognised as a primary public messaging channel during crisis, emergencies, significant events and natural disasters. The MPA External Digital Media Strategy priorities focus on community safety by building an audience for times of crisis and keeping the community informed using timely and prioritised alerts.

6.1.2 The type of crisis will inform which government agency is the lead agency, responsible for coordinating public information including:

- drafting communication materials;
- monitoring traditional media and digital channels;
- creating whole of government messaging; and
- engaging with stakeholders.

6.1.3 Information provided through Service official social media must be current and accurate. Public messaging may be reinforced by sharing information from official partner agencies.

6.2 Whole of Government Crisis Communication Network

6.2.1 The Queensland Government Crisis Communication Plan, developed by DPC outlines the actions to be taken by the government in response to an issue or crisis that has a high impact to Queensland, impacts a significant portion of the state's population, or has the potential to negatively impact the reputation of the Queensland Government.

7. Legislative requirements

7.1 Privacy

7.1.1 Social media, private and instant messaging tools must not be used to send personal information relating to any caller, victim, witness, suspect or colleague and any other individual's personal details. Direct messages as part of official social media use should be considered public information which may be obtained under Right to Information requests.

7.1.2 For applicable Service policy regarding release of information, see s. 6: 'Release of information' of the Media Guidelines for further guidance.

7.1.3 All members are to comply with the requirements in the IPA and the *Human Rights Act 2019* (HRA) regarding the collection, management, use and disclosure of personal information. Privacy is an important concern for social media users and members must understand privacy requirements when using Service social media.

7.1.4 The Office of the Information Commissioner's Privacy and Social Media Guide provides further guidance regarding information privacy in social media. Similarly, the *QGEA* Principles for the use of social media networks and emerging technologies provides guidance on information technology, information management and risk management practices for government agencies using social media platforms.

7.1.5 It is important to distinguish information appropriate for public release. Confidential information should not be published on social media channels unless it meets the requirements of urgent public messaging.

7.1.6 Where appropriate, steps should be taken to protect an individual's identify through measures such as blurring faces and identifying features and removing audio. The Media Guidelines provide guidance for privacy when considering release of vision and audio. Considerations supporting a decision to not release vision include:

- graphic or violent content;
- potential to re-victimise persons involved;
- identification of victims or witnesses;
- depiction of police use of force actions or methodology;
- interference with the administration of justice; or
- impact on internal investigation procedural fairness.

7.2 Intellectual property

7.2.1 Copyright is a form of intellectual property that protects the original expression of ideas. In Australia, the *Copyright Act 1968* (Cth) grants copyright owners exclusive rights over material they have copyrighted, including text, photos, images, icons, computing programs, video and/or audio. The term covers the various legal rights to protect the original and creative effort. Property subject to intellectual property rights cannot be used on social media channels without explicit consent and acknowledgement.

7.2.2 The Service *myPolice News* publishes under Creative Commons enabling adapting, sharing and publication of our information with appropriate attribution. When publishing on Facebook, permission is by default assigned to enable use of Service intellectual property.

7.3 Human rights

7.3.1 The HRA places an obligation on a decision maker to act and make decisions compatible with human rights and which give proper consideration to human rights.

7.4 Defamation

7.4.1 Defamation is an area of law concerned with a person's damaged reputation. Defamatory publications can include social media posts, emails, internet articles, online business reviews, Google search results, YouTube, blog posts, SMS text messages, newspaper articles, radio shows, television shows etc.

7.4.2 Members must not comment on businesses or individuals that may be defamatory, confidential or based on rumour. Refer ss. 3.1: 'Rules' and 4.3.2 of this policy.

7.5 Accessibility obligations

7.5.1 Despite widespread use of social media, some community members may find accessibility difficult for a variety of factors including:

- disability;
- lack of skills to operate a computer or mobile device;
- lack of access to a computer or mobile device;
- lack of access to a reliable network connection; or
- limited download quotas via mobile devices.

7.5.2 To accommodate differential uptake of communication channels, messages or information should be made available across a range of formats. However, in some instances it may be appropriate to only use social media as a channel, or one specific social media platform, such as for campaigns targeting specific demographic groups or for emergency or disaster-related events.

7.5.3 Members of the community may use social media to interact with the Service, however, this should not be the only avenue available for them. In some cases, the alternative may be represented on the Service corporate website or by referring individuals to telephone or face-to-face channels.

7.5.4 The Web Content Accessibility Guidelines (WCAG) 2.0 is mandated Queensland Government policy which provides guidance on making QGov internet content more accessible to all people.

7.6 Records Management

7.6.1 The PRA obliges all Queensland Government agencies, including the Service, to make and keep full and accurate records of its activities. All agencies must have regard to any relevant policy, standards and guidelines made by Queensland State Archivist (the archivist).

7.6.2 The archivist's Records Governance Policy sets out the six foundational principles of recordkeeping for Queensland Government agencies to meet minimum recordkeeping requirements now and into the future.

7.6.3 The archivist also authorises the retention and disposal of public records via a schedule. The archivist's General Retention and Disposal Schedule (GRDS) covers public records of common activities and functions, transitory, and short-term public records created as part of routine transactional business practices. As the GRDS is frequently amended and updated, readers should use the GRDS website for the current version to ensure that any Service social media content is captured as a record and retained appropriately before it may be lawfully disposed.

7.6.4 Service social media content is a public record in accordance with Principle 9 of the Queensland Government Enterprise Architecture (QGEA)'s Principles for the use of social media networks and emerging technologies.

8. Use of social media

8.1 Use of social media for official purposes

8.1.1 Use of social media for official purposes is permitted for intelligence, investigative, operational, and research purposes, provided members comply with relevant legislation, policies, procedures and guidelines. As is applicable for internet access via Service ICT assets or systems, access to and use of social media platforms is monitored and governed by existing Service ICT Security and Usage policies.

8.1.2 The Service has implemented Workplace an (internal) social media platform for official purposes. Workplace is a dedicated and secure space for members to connect, collaborate, share, innovate and distribute information pertaining to specific interest groups or categories. Any matters relating to Workplace should be referred to the Internal Communications Team, CCE Division. Further information may also be found at s. 4.1.6: 'Workplace' of the MSM.

8.2 Use of social media for personal and non-work related purposes

8.2.1 The Service recognises members may use social media for personal and non-work-related purposes in their own time. Despite the many benefits social media may bring, in certain instances unintended consequences may result. Accordingly, members are to understand:

- despite tight personal privacy settings, in reality there is no such thing as a private social media post, and control of same may be lost very quickly and easily;
- inappropriate posts, especially, may rapidly gather momentum and go 'viral' with far-reaching consequences;
- it is not befitting to be a member of social media groups or pages where others post derogatory or inappropriate comments. Your very presence in the group arguably provides tacit support, endorsement, and authority for same — particularly if you are in a leadership role in the Service.

8.2.2 Improper personal use of social media can result in breaches of various legislative provisions including:

- for officers, Part 7: 'Discipline process for officers' of the PSAA;
- for staff members, Chapter 6: 'Disciplinary action for public service employees and former public service employees' of the *Public Service Act 2008* (PSA);
- PSEA;
- Code of Conduct; and
- Standard of Professional Practice.

8.2.3 The Service supports all members who report conduct that is misconduct or another ground for disciplinary action, including conduct not consistent with the legislation and policies referred in 8.2.2 above. All members are to comply with s. 6A.1: 'Duty concerning misconduct and other grounds for disciplinary action' of the PSAA if they identify any conduct that is reportable as misconduct or disciplinable conduct.

8.2.4 Members may be subject to disciplinary and/or legal action for improper use of social media in a personal and non-work related capacity including, but not limited to, when using their own name, a version of it, a person or persons name/s which is not their own (with or without permission) and/or pseudonym/s. A claim of anonymity may be irrelevant: see Comcare v Banerji [2019] HCA 23. Without limiting the circumstances where improper use of social media may apply, members must not:

- publish or post false information that harms the reputation of another person, group, or organisation (defamation);
- use information obtained through their Service position to publish or post 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; would be offensive to a reasonable person; and/or compromise an investigative or intelligence function;

- post comments that appear to be made on behalf of the Service;
- post criticisms of the government, a member of parliament or their respective party or policies, that raise questions about the member's capacity to work professionally, effectively or impartially as a Service member;
- use someone else's name, likeness, or other personal attributes without that person's permission;
- publish the trademarks, confidential business information or creative work of another without the permission of the owner;
- engage in activities online, posting comments or uploading images that would bring the Service into disrepute, undermine the Service standing as a trusted member of law enforcement and intelligence communities, are inconsistent with Service values, or compromise the effectiveness or security of operations, court proceedings or assets;
- divulge official Service information, including information obtained through their duties, expand on information already available in the public domain, or release protectively marked information;
- compromise the member's capacity to fulfil their duties in an unbiased, professional or impartial manner by posting or publishing derogatory comments about Service policies, procedures, operations, activities or those of partner agencies;
- post comments which compromise public confidence in the Service;
- post comments identifying themself as a member or images in uniform on dating applications or websites;
- post comments, images or videos of a station or establishment; that may compromise the security of any police station or establishment;
- post comments in support of individuals or associations that present an integrity risk as outlined in the Declarable Association Policy framework;
- post personal attacks connected with the member's workplace;
- use or misrepresent Service copyright material, including the Service logo for financial gain or without reasonable justification;
- conduct themselves online in any way that may be seen to harass, intimidate, bully, victimise or discriminate against others.

8.2.5 Members shall take action to protect their personal information and minimise risk of security breaches. Members should:

- not disclose their position as a Service member. The content and links of a personal webpage may also identify the person as a member of the Service, even in the absence of a direct statement of the person's occupation;
- not disclose personal details and images in the public domain. This may compromise the member's vetting status or ability to be deployed on certain types of policing activity (such as surveillance, intelligence, controlled or covert operations). Members should be aware of the consequences of these actions on their ability to remain an effective member of the Service;
- not post photos or videos of themselves undertaking police operations, or confidential and security classified activities inside police premises. These actions can potentially compromise both personal and organisational security;
- not disclose any personal details which may contribute to identity theft or identify a member's home address or other sensitive details about themselves, their family and/or their colleagues. This may include posting of photos and the use of geo-tagging;

- activate the highest level of privacy settings available to restrict who can find their profile and view their content.

8.2.6 Members are accountable for content posted on social media in both a public and private capacity including direct/private messenger services e.g. Messenger, WhatsApp etc. See recent decision Calvin Dunne v Commissioner of Police [2021] NSWIRComm 1020 where a police officer lost an appeal against dismissal for racist, homophobic and sexists texts shared privately with work colleagues.

8.2.7 To protect the reputation of the Service and its members, members must not create or manage unofficial social media police groups, pages or accounts. However, members may create and manage social media for Queensland Police Service clubs, associations or affiliate organisations approved pursuant to s.11.3 of the Management Support Manual.

8.2.8 Personal and corporate social media must not be used to establish or pursue an improper relationship with any current or former victim, offender or witness.

8.2.9 Members are to be aware of the potential actions that may occur when their personal use of social media reflects seriously or adversely on the public service, Service and/or contravenes their obligations under legislation, the Code of Conduct or Service-wide policy.

9 Intelligence and investigative function and procedure

9.1 Exclusion of Intelligence and Investigative function and procedure

9.1.1 Nothing in this policy document is intended to restrict or modify intelligence or investigative functions and procedures as they relate to access and use of social media.

9.2 Online assumed identities

9.2.1 Members shall not use personal social media accounts to access other user accounts, websites or information for intelligence or investigative purposes. Such login credentials shall be via use of an online assumed identity.

9.2.2 An online assumed identity enables greater scope for intelligence and investigative purposes. Covert activity must be conducted in accordance with an authority, in the course of duty and for law enforcement purposes directly related to the functions of the Service. See Chapter 12: Assumed identities' of the PPRA and s. 2.10.6: 'Online intelligence' of the OPM.

9.2.3 Schedule 3: 'Information Privacy Principles' of the IPA is to be adhered to when collecting information from online searches. See s. 5.9: 'Information privacy principles' of the MSM.

9.2.4 The Guide to Open Source Searching, Monitoring and Engagement provides guidance in the sensitive area of online engagement. Not only are specialised skills required to create and maintain an authentic online persona, there are significant legal risks including unlawful procurement of offences and other unlawful acts by members. When using social media, trained and accredited judgement is required when deciding what is appropriate for the purpose of an online assumed identity.