JAMAICA PRODUCERS GROUP

SOCIAL MEDIA POLICY

1. Introduction

Jamaica Producers Group ('JP) is a diverse, global group of businesses operating in different industries in various jurisdictions around the world. This Policy is meant to provide general guidelines to our team throughout the Group for their professional and personal use of social media. Business Units are expected to put in place more specific guidelines, tailored to their specific products and markets, and in particular, detailed guidelines for their Social Media Managers.

Note that violations of this policy will be enforced under current employee personnel policies.

2. Definition

'Social Media' as interpreted by this policy includes, but is not limited to, all forms of online publishing and discussion, including but not limited to blogs, wikis, file sharing, social networks and other social networking applications.

3. Guidelines for Personal Use of Social Media

Whether you are an official Social Media Manager or not, when you are talking about any company, business or brand in the JP Group using your personal social media account, keep in mind that:

1. The JP Code of Ethics and Business Conduct, the Securities Trading Policy and other relevant policies still apply.
2. You are responsible for your actions. We respect your right to express yourself and we encourage you to get online and have fun but be responsible, use sound judgement and common sense.
3. Your personal social media content should be consistent with how you wish to present yourself with clients and colleagues.
4. As a JP Team Member, you are an important ambassador for your company's brands. We encourage you to promote them, but you should make it clear that the content of your post is personal to you and that you are not acting as an agent of the company.
5. You should never disclose commercially sensitive, anti-competitive, private or confidential information on personal and work-time social

media sites. In cases where you are unsure whether the information you wish to share falls within one of these categories, you should discuss this with the company's General Counsel.

6. You should not post negative comments or opinions in relation to the Group or any of our brands or products on your personal or company social media accounts.
7. If you are not a Social Media Manager or otherwise authorized to comment on social media on behalf of the company, or to use company social media accounts, you should refrain from answering questions related to the company, its brands or products. Instead, you should direct all questions and concerns to the appropriate Social Media Manger.
8. Be responsible when mixing your business and personal lives; be aware of your Business Unit's policy regarding the use of social media during work hours, or on the company's devices.

4. Guidelines for Social Media Managers

Social Media Managers for the purpose of this policy are those authorized to access and manage the group's social media accounts as well as to communicate with the general public via the group's social media accounts. When acting as an official spokesperson for your Business Unit, take into consideration the following:

1. While engaging in work-time social media sites, be transparent. Identify yourself as a Team Member of the company or your affiliation to the company when making posts to the company's social media.
2. Follow all applicable Company policies.
3. Proper judgement and rational thinking should be utilised when publishing content on personal and work time social media sites. As such all material posted on social media shall not be inappropriate or harmful to the company, its employees or customers. For example, content that includes commentary or images that are defamatory, prejudicial, pornographic, harassing, libellous, or that can create a hostile work environment is prohibited.
4. Do not conduct discussions or comment on legal matters relating to the company unless you have been given explicit authorization to do so.
5. Permission must be granted from clients, partners or suppliers when referring or linking them to the company on social media. Similar permission is also needed to use the company's and third-party copyrights, trademarks or other intellectual property on social media.
6. Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against you and the company. As such, the policy shall be read with all applicable and relevant law.
7. Social Media Managers should ensure company's social media usernames, emails and passwords are secure. This information should

not be shared with or made accessible to unauthorized team members or the general public.

8. Keep in mind that your local posts can have global significance. Keep this 'world view' in mind when participating in online conversations.
9. When in doubt, do not post.
10. Remember, anything you post is permanent.

5. Social Media Crisis Management Policy

Definition: 'A Social Media Crisis' is defined as an event that can have a negative effect on a brand, individual or company which originates on a single or multiple social media channel(s).

Application: The objective of this document is to ensure the social media teams are adequately prepared to deal with a crisis that may arise within the Social Media environment. Crises range from small-scale incidents to larger widespread Public Relation incidents. Team Members who are not Social Media Managers should bring any matter falling under this policy to the attention of the relevant Social Media Manager. Only Social Media Managers should respond to Social Media Crises. Social Media Managers should never act alone in responding to a crisis, rather they should act in consultation with the contact teams set out below depending on the level of the threat (collectively referred to as the Crisis Response Team).

Step 1: Identify Threat Level

- Level 1: Minor incident, normally limited to one Social Media platform (e.g. Consumer post dissatisfaction with a service or good).
- Level 2: Incident that spreads across several Social Media platforms (e.g. Video of an employee being unprofessional or rude with a customer).
- Level 3: Incident immediately goes viral across various media and could have a material negative effect on the company's brand. (e.g. Proof of criminal activity by an employee)

Step 2: Acknowledge the Crisis within an hour and re-assure Social Media users that the crisis is being resolved or further investigations will be conducted to aid in solving the issue at hand. In addition to this **pause all other Social Media communication** until the crisis has been averted. This includes, but is not limited to promotions, notices, ongoing conversations, posting, commenting and liking.

Step 3: **Determine the Communication Team** – based on the level of the crisis, the Social Media Manager should contact the appropriate level of administration to address the crisis as soon as possible (customer service, management, executives, human resources). A list of the individuals to contact at each crisis threat level can be found below in the appendix. Key stakeholders should also be contacted within 3-6 hours of the crisis to communicate that the crisis has been acknowledged and is currently being investigated and resolved in a timely manner.

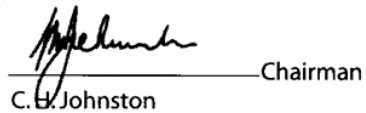
Step 4: Release an Official Statement – Given the fast pace nature of social media an official response within real time will be required in most situations. If the Crisis Response Team decides to give an official response, the official response should be formulated and circulated within 24 hours of the crisis. The response should be positive, rational, politically correct and explicit. The response should reiterate the crisis, include an apology, and provide a solution/compensation for the affected parties as well as the general public. **Inaction is never an acceptable response**. Be reminded that inaction can allow the public to take over the narrative, fuel the negativity and add to the misinformation.

Step 5: Post-Statement Monitoring and Communications – Monitor the crisis continually after the official response to determine the reactions of the general public. as Also, address any questions or concerns that arise post-response, which may or may not have been spoken to in the official statement. The Crisis Response Team should develop and circulate details and FAQs pertaining to the crisis throughout the organization. This is to ensure awareness and consistency in the company's understanding of the crisis, as well as the message that employees should give the general public after the statement.

6. Contact List for Various Crisis Threat Levels

	Contact Name	Title	Phone Number(s)	Email
Level 1				
Level 2				
Level 3				

BY ORDER OF THE BOARD.



Chairman

C. H. Johnston

Date: 5th November 2019

Version #	Board Approval Date	Date of Next Review
1	November 5, 2019	November 5, 2021