Common Market for Eastern
and Southern Africa

Social Media Policy

TABLE OF CONTENTS

Background

The Common Market for Eastern and Southern Africa (COMESA) is an intergovernmental regional integration organization comprising of 21 Member States. COMESA's current strategy can be summed up in the phrase "economic prosperity through regional integration". With a combined population of over 583 million, a majority being youth and a Gross Domestic Product of US$ 805 billion, COMESA forms a major marketplace for both internal and external trading and a huge opportunity for youth employment.

The COMESA Social Media Policy

The COMESA Social Media policy outlines the standards, approach to the use and management of social media for both the internal and external stakeholders of COMESA. It supplements COMESA's Information and Communication Technology Policy document, the COMESA Code of Conduct Policy, Staff Rules and Regulations and any other relevant policy.

The rationale for having the COMESA Social Media Policy COMESA is to deepen its usage of social media such as social networking sites (Facebook, Twitter, Instagram, WhatsApp LinkedIn, and YouTube) blogs, wikis, podcasts, to promote the organization with both internal and external stakeholders.

This policy serves as a guide to all employees including fixed terms consultants working at all levels and grades at the Secretariat, and COMESA institutions.

Article 1

Definitions

"Social Media" -means facilities used for online publication and commentary including without limitation to platforms such as blogs, microblogs, wikis, LinkedIn, Facebook, Instagram, Twitter, WhatsApp, Telegram and YouTube;

Web pages - Corporate Website and Intranet

"Copyrights" – means the rights of an author to control reproduction and use of any creative expression that has been fixed in tangible form, such as graphical works, photographic works, audio-visual works, electronic works, and musical works. It is illegal to reproduce and use copyrighted material through social media channels without the permission of the copyright owner;

"Official Use" – means use by an authorized staff member of social media as a representative of COMESA through a social media account that is labelled as an official "COMESA" account, i.e., not a distinct individual person;

"Personal Use" – means use by a staff member of social media in their personal capacity on any social media account, not officially representing COMESA, but identifying themselves as affiliated with COMESA in their online biographies, profiles, or posts, or through other social platforms;

YouTube Terminologies - Embed Codes, Comments, Likes, Dislikes & Shares

"Embed codes" means unique codes that are provided to entice others to share online content without requiring the sharer to host the content. (For example, it is possible to display a YouTube

user's video in someone else's social media account/channel without requiring that person to host the source video file);

"Comments": means written responses on videos, channels, and playlists or in response to other comments;

"Like": means a user action that shows appreciation for a video;

"Dislikes": means a way to show disapproval of the content published;

"Share": means the ability to distributed videos via social media, e-mail or direct links;

Twitter Terminologies: Tweets, Retweets & DM (Direct Message)

"Tweet": means a 280-character social media disclosure distributed on the Twitter micro-blogging service;

"Retweets": means tweets from one twitter user that are redistributed by another twitter user;

"Direct Message": means a private message from one Twitter user to another and can only be sent to users following each other;

Facebook Terminologies - Timeline, Newsfeed, Like, Dislikes & Shares

"TimeLine" means updates and activities by fans/friends on a Facebook home page in reverse chronological order;

"Newsfeed" means an ongoing list of updates on a homepage that shows what is new with friends and pages liked;

"Like" means a way to give positive feedback and connect with content an individual care about;

"Dislike" means a way to show disapproval of the content published; and

"Share" means when an individual replicates content from another friend/user/brand on their own newsfeed/timeline.

Article 2

Scope Of the Policy

All internal and external stakeholders shall comply with this Policy to protect the privacy, confidentiality, and interests of COMESA, its products/services, employees, partners, customers, fans/followers/subscribers, and competitors.

Article 3

Implementation of the Policy

1. The COMESA Secretariat Management has the overall responsibility for the effective operation of this Policy. The Corporate Communications Unit and the Information and Networking Division shall be responsible for monitoring and reviewing the content and application of this Policy and making recommendations for changes to minimize risk to the organization's operations on social platforms.

2. All staff shall comply with this Policy and ensure that it is consistently applied. All staff shall take time to read and understand it. Questions or clarifications regarding the content and application of this Policy should be directed to the Corporate Communications Unit.

Article 4

Authorized Members of Staff

The following are authorized to post material on any of the organization's social sites in COMESA's name and on behalf of COMESA:

(a) The Head of the Corporate Communications Unit or a nominee;

(b) The Director of the Information and Networking Division or a nominee;

(c) The Webmaster

Article 5

COMESA Requirements

1. COMESA has laid down policies regarding its promotional activities that would include promotion on social platforms. All communications should be in strict compliance with the Corporate Communication Policy.

2. All official initiated (Promotions/Marketing/Corporate Social Responsibility etc.) communications made using social platforms shall be identified or suggested by the relevant Unit or Division, reviewed by the Head of the Corporate Communications Unit and approved by Management.

3. Unauthorized staff shall not communicate in the organization's official social platforms, pages, profiles, timelines.

Article 6

General Guidelines

The profile on social media sites must be consistent with COMESA's profile on the COMESA website or other COMESA publications and be in line with COMESA brand guidelines. All official users of social media must follow the ethical standards always expected of COMESA employees such as:

(a) Refraining from criticizing clients (fans/ followers), colleagues or institutions;

(b) Responding to others' opinion respectfully and professionally;

(c) Avoiding anything that breaches my terms of employment;

(d) Refraining from harassing, flirting, bullying or intimidating fellow colleagues;

(e) Acknowledging and correcting mistakes promptly;

(f) Disclosure of conflicts of interest;

(g) Refraining from knowingly posting inaccurate information;

(h) Linking to online reference and original source materials directly to avoid infringement of copyright and trademark rights;

(i) Displaying polite, considerate, kind and fair behaviour;

(j) Ensuring that one's activities do not cause harm to the organization or any fellow employee; and

(k) Championing COMESA and its mandate.

Article 7

General Account Management

Facebook, Twitter, LinkedIn, YouTube, Instagram

1. An administrator will manage the social media accounts (including but not limited to Facebook page, Twitter, LinkedIn, Instagram, YouTube), possibly chosen from (or closely liaising with) the team who provide content for the website. The administrator may appoint other users, whether authorized employees or external providers, as co-administrators.

2. An administrator can edit the page from their personal Facebook or LinkedIn account and can manage all the editing options on the page. However, care must be taken to respond corporately, on behalf of the page and not from the administrator's profile.

3. An email address or cloud storage should be set up for all social media content and correspondence (e.g., socialmedia@comesa.int). This will help to domicile past and upcoming content and grant access to authorized staff.

4. The Social Media Policy requires that any passwords and logins associated with social media sites must be registered by the Corporate Communications Unit and made accessible only to staff with the appropriate authority.

Article 7.1

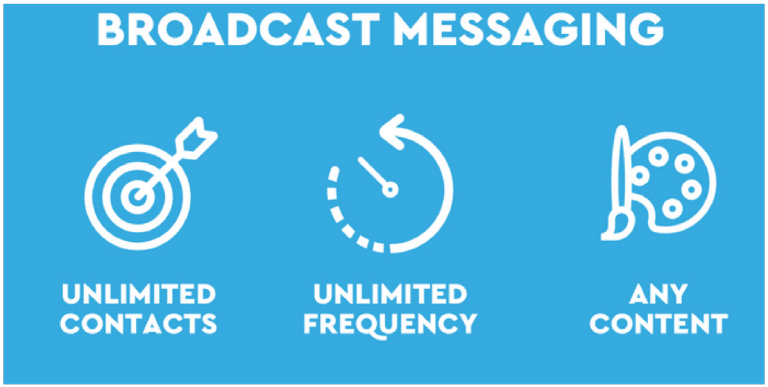
Telegram for Business

1. Telegram is a free messaging app focused on speed and security. The interface is simple and clutter-free. You can download Telegram on several devices and messages will sync smoothly across them all. It has one central interface, the messages panel. A pull-out menu on the left gives access to Contacts as well as the ability to create new groups, secret chats, and channels.

2. Telegram Groups are ideal for community building and can have as many as 200,000 members. You can add members individually or post a group link publicly. Groups can even be made public and searchable on Telegram. Only administrators can send messages.

3. Telegram channels have no user limits making it easy to broadcast information. Users subscribe to channels by searching in-app or by using channel links listed on the website and other places. Channels with more than 1000 subscribers show channel and post analytics.

4. There are two ways to use Telegram for business. You can create groups and channels, but the best is to create a Telegram Bot for business. The Telegram Bot API or Telegram Business API is free and can be used to create bots for social, productivity, and e-commerce services. Telegram Bots may use for human support by connecting them to a Customer Relationship Management (CRM) or messaging platform. To get your customers as Telegram Contacts, such customers will have to initiate contact.



Telegram Broadcast

5. This is a limitation used by Telegram and other messaging app business accounts to reduce spam.

6. Chat Links and Quick Response (QR) Codes can be sent to existing customers to link to a brand on Telegram. Frequent Telegram users will likely find it through In-App Search.

7. Chat Links work well on websites, social media profiles, or even in emails sent to customers. On mobile, users will be directed to download the Telegram app if they press the link. If they press the link on desktop, users will be taken to a page where they can open Telegram Web, however this only works when users have visited the page previously.

8. You can send rich media like pictures, videos, files, and text to an unlimited number of Contacts. But remember, you will need to get them to message you first to become Contacts. The administrator will need to connect your bot to a business messaging platform to send a broadcast.

Article 7.2

WhatsApp for Business

1. This version of WhatsApp helps firms to separate their personal and work messages. Businesses can easily reply to messages on the go. Outside of operating hours, businesses can also set automated greeting messages and away messages.

2. To create an account, download the App onto a phone with a SIM card. Keep in mind, you will need a separate SIM card or number for Business WhatsApp; if you have a dual SIM phone, you can buy an additional SIM card to insert and assign that number to the Business App. You cannot use the same SIM card as your personal WhatsApp account. At the moment, only one user to one device is allowed.

3. There are no messaging limitations as long as your business abides by WhatsApp Business Policy and WhatsApp Commerce Policy. Once your inbox gets busy, there is a Quick Reply and Automated Greeting & Away Messages feature to help with managing your chats. The platform allows the user to send Contacts the first message if the user has their number.

4. Businesses are free to broadcast any form of content to 256 people per Broadcast List at a time. But only contacts who have saved your number can receive your broadcast. Using the labels provided in the Business App, the administrator will be able to organize people into groups and send targeted WhatsApp messages en masse.

Article 7.3

Content Management

1. An internal process will be established to funnel information about milestones, initiatives and events to the administrator for use in social media. All relevant staff should be aware of the objectives of the social media site and invited to contribute relevant information.

2. Content owned by a third party (photos, documents, videos, etc.) must not be uploaded unless written permission has been obtained. These permissions and releases must be saved on a folder or email accessible by authorized staff.

3. Staff of the Secretariat can create WhatsApp and Telegram Groups for the purposes of rapid communication and coordination amongst them.

4. The groups could be based on Divisions, Units, projects etc and should have specific objectives to ensure they remain focused and relevant. They may also be based on task teams to facilitate coordination. The Heads of Division/ Units/Projects etc should be the principal administrator of the platforms and any other staff identified as substitute.

5. Like any other medium, the groups should be strictly used for the intended objective which should be outlined under the group's description.

6. Content that is irrelevant to the objective of the group should not be allowed.

7. The group's members and administrators should ensure the guidelines on Copyrights, Official Use and Personal Use of such platforms are upheld.

8. The administrator will have the authority to suspend any group member violating the guidelines and demand deletion of inappropriate content.

Article 7.4

Site setup and branding

1. The COMESA logo must be prominently placed on the respective social media sites that are used for dissemination of content especially i.e., Facebook and Twitter, Flicker and other

2. Ad-hoc content will be posted whenever appropriate, and there will be a focus on responding to any comments or posts on the Page. The chance for real and meaningful engagement on a range of topics is one of the biggest benefits and distinctions of social media.

3. Ad-hoc content could include:

   (a) links to positive stories about COMESA in the media;

   (b) links to the website when media releases are issued, or when any new documents/ forms become available online;

   (c) relevant awards/industry recognition for COMESA or its stakeholders;

   (d) new key staff or job openings at COMESA;

   (e) advice about trade facilitation;

   (f) promotion of competitions/events being run by or endorsed by COMESA;

   (g) links to helpful resources such as funding and training opportunities;

(h) local business success stories assisted by COMESA economic development projects;

(i) promotion of youth events;

(j) updates on policy and advocacy work; and

(k) links to digital platforms of COMESA institutions, programmes and projects.

Article 7.5

Response times

1. The social media site should be actively monitored by the authorized staff throughout and all comments responded to within 24 hours.

2. Authorized personnel should post relevant content regularly while avoiding overwhelming the audience.

Article 7.6

Style

It is important to adopt a conversational and friendly tone when using social media, as a less formal approach 'humanizes' COMESA and develops a rapport with readers.

Article 7.7

Content Removal

1. COMESA reserves the right to take down and remove inappropriate content and block the user from the social media site.

2. The following content is not permitted and will be removed from COMESA social media sites:

   (a) profane language or content;

   (b) sexual content or links to sexual content excluding material relating to sexual health;

   (c) content that promotes, fosters or perpetuates discrimination on the basis of race, creed; colour, age, religion, gender, marital status, national origin, physical or mental disability or sexual orientation;

   (d) copyright or ownership protected materials;

   (e) content not relating to the subject matter of the social media site;

   (f) material designed to encourage or conduct illegal activities;

   (g) material which could compromise the safety of COMESA, its employees or its technical systems;

   (h) spam (the distribution of unsolicited bulk electronic messages); and

   (i) non-official language.

3. The staff member responsible for the social media site must monitor the posts and comments posted on the social media sites and remove anything which breaches this policy. If content is removed the following details about the post must be recorded and stored in COMESA's record management system:

   (a) post content;

   (b) author's name;

   (c) date and time;

   (d) name of the social media site;

   (e) web address of the social media page; and

   (f) screen print of the comment.

4. External organizations and other tools (Google Alerts, Social Mention Tracker) can be used to continually monitor third party social media sites, which reduces the time by staff for this task.

Article 7.8

Internal Policy

1. The authorized staff shall act in a respectful manner when posting or tweeting anything related to COMESA's official profiles.

2. The following policies apply to all employees within the organization who participate on social media (official or personal) sites such as Facebook, LinkedIn, Twitter, YouTube, blogs, wikis, podcasts, and forums.

Article 7.9

Prohibited Conduct

COMESA Secretariat prohibits the use of social sites (official & personal) to:

(a) Evaluate the performance of staff, co-workers, customers, business partners or vendors, etc.;

(b) Publicly criticize or complain about the behaviour or actions of COMESA's customers, co-workers (staff), business partners, vendors or competitors. The criticism or complain should be fair and must be channeled through the Corporate Communications Unit;

(c) If the comment is inappropriate or irrelevant, respond in a polite fashion, linking information or redirecting the user to other websites which may provide an adequate response, if necessary;

(d) A standard template response would be prepared to respond to users making inappropriate comments;

(e) Comments must be addressed as soon as possible, including thanking the user for participating and any additional content that may be needed;

(f) All posts and comments by COMESA should link back to its website, where relevant, for accurate and more detailed information;

(g) Discuss confidential information, legal matters, litigation or the organization's financial performance. In case where one is compelled to respond, employees will relay the following: "The Common Market for Eastern and Southern Africa

(COMESA Social Media policy only allows authorized employees to discuss these types of matters, but I can refer you to someone from contact person at the relevant Division or Unit;

(h) Post material in breach of copyright or other intellectual property rights, or which invades the privacy of any person;

(i) Use language that is defamatory, degrading, disparaging or violates COMESA's Code of Conduct;

(j) Conduct private business on COMESA's social media presence;

(k) Stalk, bully, troll or ignore any individual or group;

(l) Access or upload pornographic, gambling or illegal content, including extreme images of any illegal activities;

(m) Involvement, comments, discussion, analysis relating to politics/race/ethnicity/ tribe, etc;

(n) Hack or attempting to infiltrate the systems of COMESA or another organization;

(o) Upload information of a confidential nature, especially in regard to COMESA's services/products or any other organization;

(p) Name call or engage in behaviour that may bring COMESA into disrepute;

(q) Express political or religious views;

(r) Discriminatory language on gender, ethnicity, religion or nationality;

Article 7.10

Transparency

All authorized staff are required to:

(a) Always identify themselves when engaging publicly on any social media platform related to COMESA, competitors, or any products in the marketplace;

(b) Indicate their (staff) affiliation with COMESA where appropriate. All staff must comply with all laws and regulations regarding disclosure of self-identity;

(c) Never represent themselves to be other than who they really are, so long as they can do so without forfeiting their legal rights to engage in protected activities of COMESA;

(d) Ensure transparency and consistency across all profile pages of COMESA's social media accounts. Conflicting information can damage the organization's credibility and could adversely affect its reputation; and

(e) Use simple and grammatically correct language that makes it easy for the average user to understand their position when commenting on COMESA or COMESA-related topics through the various social media channels.

Article 8

Integrity and Honesty

All authorized staff of COMESA shall not:

(a) Blog, comment, post, tweet anonymously or use false screen names. Only real name initials ("PA" for Peter Adams) should be used and affiliation with COMESA clearly indicated;

(b) Say anything dishonest, untrue or misleading. Authorized staff must stick to the area of their expertise and always get assistance from the relevant personnel to respond to a query which they do not have accurate information on; and

(c) Engage in conversation before understanding the context. Authorized staff must explore the topic being discussed, read about it and contribute only when input adds or advances the discussion. The goal is to ensure COMESA's voice is part of the larger conversation relating to the communities that COMESA serves.

Article 9

Disclaimer

COMESA recognizes the importance of staff joining in and helping shape industry conversations and direction through interaction on social media guided by the following:

(a) When COMESA staff use their personal accounts on social media, they should remember that their behaviour is still bound by COMESA's values and code of conduct. However, in order to protect the COMESA brand, all staff (including those authorized) who have disclosed their affiliation with COMESA on their personal social sites must use the disclaimer as below.

> *The postings/comment/tweet on this site are my own views and don't necessarily represent the Common Market for Eastern and Southern Africa (COMESA)'s positions, strategies or opinions."*

(b) When a COMESA staff/employee participates in a discussion not directly related to their work but that draws on their expertise in a field, such as IT, communications, this would be considered personal use. However, the staff should not reveal information about the division they are in that is not publicly available.

Article 10

Protecting the COMESA Brand

1. All employees using social media channels (for personal use) are prohibited from using COMESA's brand, logo, copyrights, trademarks etc.

2. When an employee wishes to use creative images on the organization's official social media channels, approval shall be sought from the Head of Corporate Communications before posting online.

3. Employees of COMESA and its Institutions shall respect the laws governing copyright and fair use of copyrighted materials owned by others as well as the COMESA.

4. Employees shall not quote more than a short extract of someone else's work and must always attribute such work to the original author/source and provide link to where the extract is publicly available on the internet as this is unethical and may directly create a negative impression of the COMESA brand. This applies to the official use of social media.

5. Only authorized staff of this Policy can share links to copyrighted works hosted by copyrighted owners or their resellers without obtaining the permission of the copyright owner only if done so without any modification of content and must also include an original description of the link they are sharing.

6. Only authorized staff of this Policy may embed and share copyrighted content (such as YouTube videos) in the organization's official social media channels so long as the embedded code has been provided by the rightful copyright owner or reseller.

7. In special circumstances, like disasters or emergencies (such as COVID 19), where the public's right to know outweighs the financial objectives of a copyright owner, employees may share copyrighted material/content without the permission of the copyrighted owner. This could be photographs uploaded to social media channels of a disaster to help others stay out of harm's way (applicable to personal use only).

8. COMESA will exercise the right to delete posts, and on rare occasions ban users. Content that may be removed includes, but is not limited to:

   (a) Spam (for instance, promotions, sales, self-promotion, repeated posts with the same messages and so on);

   (b) Racist, sexist, religious intolerance, xenophobic or other content that members of our social communities may find offensive; and

   (c) Libelous, misleading or inaccurate accusations.

Article 11

Application of Existing COMESA Policies and Procedures

1. All activities on social media are subject to the policies and procedures of COMESA.

2. Any breach through social media is subject to the organization's rules and regulations, code of conduct and individual contracts with COMESA.

3. Staff are legally liable for anything they write or present online, whether for official or personal use. All employees shall not take an active part in any political activity/discussion on the organization's official social media channels regardless of any circumstance, as this will adversely affect the image of the organization.

4. Gender sensitivity as per the COMESA Gender Policy shall guide content to promote gender equality.

Article 11.1

Confidentiality

(a) All staff shall maintain the confidentiality of the organization data, information, records, clients, suppliers, vendors 'details pursuant to the Staff Rules and Regulations.

(b) If staff are not sure of the appropriateness of content to share, they shall consult the Corporate Communications Unit. This includes information that has not been publicly released by the organization (Applicable to both Personal and Official use of social media).

(c) Staff shall not post any information on social media, whether in personal or official use, which is not public information and which has come by them by virtue of their official position in the organization and hence can be construed as "insider information."

(d) Where staff is unsure, they shall consult the Corporate Communications Unit which shall seek authorization from the Secretary General.

(e) Staff must not release any information that could potentially harm the organization, current and future products/services, employees, partners, and customers.

Article 11.2

Professionalism

(a) Authorized staff must always watch for typing errors, grammatical errors and misspellings. Proper e-mail etiquette shall apply to the use of social media (no defamatory /discriminatory, degrading language or provocative words).

(b) The organization encourages all authorized staff to write knowledgeably, accurately, and using appropriate professionalism.

(c) Any user may make complaints or negative comments regarding COMESA through social media channels. Authorized staff must ensure that they do not argue, refute complaints, or respond in anger to negative feedback on the organization's official social media channels. This behaviour can antagonize or fuel further attacks on COMESA brand and/or reputation.

(d) Staff should endeavour to offer clarity and seek to address (and resolve) the issue(s) raised in a professional way.

Article 11.3

Security

(a) All authorized users must maintain the confidentiality and security of passwords used on official social media sites, in compliance with COMESA's ICT policy.

(b) The authorized staff will use the available social media administration tools or the various social media platforms to communicate with fans/followers on various social sites. Access to use the tools or social media platforms will be granted to authorized staff with specific rights to each.

(c) To safeguard against unauthorized access to the organization's social media sites, web pages, all authorized members/users MUST follow the below guidelines:

(i) Passwords should conform to the required guidelines in the ICT password security policy;

(ii) The passwords for social media access should be changed according to ICT password policy guidelines or as and when it is felt that the password is being compromised;

(iii) Sharing of passwords for any software/tool/platform is strictly prohibited unless instructed/authorized by Director of ICT;

(iv) All authorized members may request a password reset for themselves by e-mail to the Director of ICT by providing the requisite details. Credentials will be given before processing the reset and record them in a spreadsheet which will provide an audit trail for all password resets;

(v) ICT division will conduct periodic password changes as per existing policies to ensure accounts such as Twitter and Instagram remain secure and are only accessed by authorised users; and

(vi) For platforms which do not require password access for users such as Facebook, LinkedIn and YouTube channel, ICT will periodically review account administrators to ensure only appointed users have access.

Article 11.4

Monitoring

(a) Staff should be aware that all official use of social media sites may be monitored.

(b) The organization reserves the right to restrict or prevent access to certain social media sites if the organization notices personal use on them.

(c) Uploading, posting, forwarding or posting a link of materials such as mentioned below to any of COMESA's social media sites, whether in a professional or personal capacity, will amount to gross misconduct:

(i) Indecent content (written, pictures, films and video clips of sexually explicit nature)

(ii) A false, discriminatory, degrading and defamatory statement about any person or organization;

(iii) Material, which is offensive, culturally or gender-insensitive, obscene, discriminatory, degrading, derogatory, or one that may cause embarrassment to our Member States, partners, our staff and other stakeholders;

(iv) Confidential information about the organization or any of the organization's staff or stakeholders (which you do not have express authority to disseminate):

(v) Material in breach of copyright or other intellectual property rights, or which invades the privacy of any person;

(vi) Any such action will be addressed under the organization's HR Policy Manual; and

(vii) If any staff notices any use of social media by other members of staff, in breach of this Policy, they should inform to Head of Corporate Communications/ Director ICT.

Article 11.5

Advice

1. Any member of staff should not offer any legal, financial, medical, or psychological analyses or advice in an official capacity on the organization's social media channels.

2. Advice shall be limited to the Division or Unit and position they serve in. If in doubt, ensure that any content is approved.

Article 11.6

Organization's Time

1. The organization does not permit use of social media sites for personal use.

2. Only authorized members of staff are allowed to access and use social media from the organization's equipment and using the organization's network.

Article 11.7

Be a Watchdog

1. If any staff finds any negative disparaging comment or tweet, or otherwise concerning posts about the organization, its products and services, staff or clients, they shall alert the Head of Corporate Communications and the Director of Information and Networking.

2. Authorized staff shall clear the responses with their respective Directors or Heads of Unit and Divisions or the Head of Corporate Communications Unit.

Article 11.8

Response to Mistakes

1. If an authorized member of staff makes an error, they must be quick to correct it as soon as it is detected or notified.

2. If they choose to modify an earlier post, they must make it clear that they have done so.

3. Where a member of staff is accused of posting something improper (such as copyrighted material or a defamatory comment), authorized staff responsible for it must remove it immediately.

Article 11.9

Record Keeping Standards

1. The organization shall keep records of all social media communications relating to the organization's business activities.

2. The record keeping standards apply to all records in all formats (image/text/video) and media on all the organization's official social media channels.

3. Keeping a record of message or conversation history will allow the organization to analyze comments on social media and get insight into customer behaviour, preference and interests. This will allow the organization to keep evidence in case of a social media crisis/conflict.

4. Further, keeping and reviewing records will allow the organization to spot trends in customer issues and give a better understanding of where negative sentiment is coming from which will allow the organization to respond before an issue is blown up as crisis.

5. In cases where any staff notices or identifies a possible damaging comment or posts made on the organization's image/brand on any of the organization's social media channels they must immediately notify an authorized member of staff or the Head of the Corporate Communications Unit through e-mail followed up by call in the format below:

   (a) Who sent the message (user pseudonyms are acceptable);

   (b) The date and time it was sent;

   (c) Name of staff reporting;

   (d) A screen capture of the comment/tweet; and

   (e) Name of social media it was created on.

6. The comment/tweet will be recorded for purposes of evidence and the matter dealt with appropriately by an authorized member of staff from the Corporate Communications Unit.

Article 12

How to Archive

1. Create specific folders for each of the content type (this could be categorised as captions, photos, videos, screenshots or based on social media platform) you want to archive. The content can be captured as screenshots and saved in PPT, Word or PDF versions.

2. Each version shall be stored based on its date on a hard drive dedicated to archiving.

3. Data may also be saved in Google Drive (create a common folder using a Gmail account and assign access to relevant personnel who will periodically update the folder with content).

4. Data shall be saved to a network drive that should also be backed up to another data source.

5. Where one has access to Dropbox or a similar storage provider, one must sync the digital archive there too. This ensures 24/7 connectivity to all data.

6. For enterprise solutions, tools such as Pagefreezer, Smarsh, ArchiveSocial have custom made solutions for public institutions with various pricing options.

Article 13

Review of this Policy

This policy will be reviewed by the Corporate Communication Unit bi-annually to ensure it meets legal requirements and reflects best practice.

Any reviews will come into effect after approval by the Secretary General.

COMESA SECRETARIAT
COMESA Center
Ben Bella Road
P.O. Box 30051

+260 211 229 725

www.comesa.int

info@comesa.int

facebook.com/COMESA/

@twitter.com/comesa_lusaka