Controlled institutional document

Social Media Policy

DOCUMENT REFERENCE

MYC-DOC-2026-C4E20075BF2B

ISSUED / SECURED

2026-08-07T16:40:15 UTC

SOURCE SHA-256

1A693F4CABC633307B99114A143BB6F495723A1EEFEC489C1BBD83EFBE6FA6DA

SIGNATURE ID

GS-D2B585C5CD06B521

Scan to verify this controlled document against the MYCDIC integrity register.

DIGITAL VALIDATION SIGNATURE (HMAC-SHA256)

D2B585C5CD06B52135AEAB72F7E3406F
AB287364772F5A78F94B97707599EE02

How to validate this file

The SHA-256 shown on this page identifies the original uploaded evidence before this security page was attached. The MYCDIC register also stores the SHA-256 of the final secured PDF. A file is authentic only when the live verification service confirms the final hash and signature record.

CONTROL NOTICE

Do not rely on screenshots, extracted pages or renamed copies as proof of authenticity. Verify the complete PDF through the official MYCDIC register.

General Secretariat of MYCDIC · Institutional digital validation

MOROCCAN YOUTH COUNCIL FOR DIPLOMATIC AND INTERNATIONAL COOPERATION

GENERAL SECRETARIAT / CONTROLLED PUBLIC POLICY

Social Media Policy

INSTITUTIONAL POLICY AND GOVERNANCE DOCUMENT

Effective date	27 April 2025
Document status	In force / controlled public edition
Institutional owner	General Secretariat of MYCDIC
Reference note	Official 2025 institutional edition - controlled maintenance

Institutional effect. This document governs conduct and internal institutional practice within its scope. It does not create diplomatic status, public authority, employment, contractual rights, or authority to bind MYCDIC unless a separate approved instrument expressly provides otherwise.

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-SOCIAL-MEDIA-POLICY-CBEA2C22 | SIG RSA-E20099F64CAF19EBB0
SHA-256 FINGERPRINT EDDDC5EA5014EB148C462C6833FA2FB49E9B1C22184F4ADF48B5609EBF2E64EB

SCAN TO VERIFY

1. Purpose and institutional scope

This Social Media Policy sets the minimum standards applicable to MYCDIC members, Youth Ambassadors, office-holders, staff, volunteers, delegates, authorized account users and other persons acting under the Council's name within the scope described in this document.

The policy protects both the Council and the individuals who serve it by clarifying authority, expected conduct, decision controls, evidence standards and the separation between institutional roles and personal activity.

2. Existing policy framework

1 Introduction

The Moroccan Youth Council for Diplomatic and International Cooperation (MYCDIC) leverages social media to engage with global audiences, promote its mission of empowering Moroccan youth in diplomacy, and foster international cooperation. Social media platforms are powerful tools for sharing MYCDIC’s initiatives, events, and values, but their use must be responsible, professional, and aligned with the organization’s standards. This Social Media Policy provides guidelines to ensure that all MYCDIC members, MYCDIC Youth Ambassadors, staff, volunteers, and affiliates (collectively referred to as “Representatives”) use social media in a manner that upholds MYCDIC’s reputation and mission.

This policy complements the MYCDIC Code of Conduct, Diplomatic Protocols, and Event Protocols, ensuring consistency across all interactions, both online and offline.

2 Scope and Application

This Social Media Policy applies to:

All MYCDIC Representatives using social media in an official capacity (e.g., posting on MYCDIC’s accounts or representing the organization).

Personal social media use by Representatives when referencing MYCDIC, its activities, or its members.

The policy covers platforms including, but not limited to, Twitter, Facebook, Instagram, LinkedIn, YouTube, and TikTok, as well as emerging platforms. It applies to posts, comments, stories, videos, and other content shared publicly or privately that could be associated with MYCDIC.

Non-compliance may result in disciplinary action, as outlined in the MYCDIC Code of Conduct.

3 Objectives

The Social Media Policy aims to:

Promote MYCDIC’s mission, events, and achievements through consistent and professional online communication.

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-SOCIAL-MEDIA-POLICY-CBEA2C22 | SIG RSA-E20099F64CAF19EBB0
SHA-256 FINGERPRINT EDDDC5EA5014EB148C462C6833FA2FB49E9B1C22184F4ADF48B5609EBF2E64EB

SCAN TO VERIFY

Protect MYCDIC's reputation and prevent misuse of its name, logo, or resources.

Foster respectful, inclusive, and culturally sensitive online interactions.

Ensure compliance with legal, ethical, and organizational standards.

4 General Principles

All Representatives using social media in connection with MYCDIC shall adhere to the following principles:

Professionalism: Maintain a respectful and polished online presence that reflects MYCDIC's values.

Accuracy: Share verified, accurate information and avoid spreading misinformation.

Neutrality: Refrain from endorsing political, religious, or controversial causes unless authorized by MYCDIC leadership.

Respect: Engage with others courteously, avoiding offensive or discriminatory content.

Transparency: Clearly distinguish between official MYCDIC posts and personal opinions.

5 Guidelines for Official Social Media Use

5.1 Authorized Accounts

Official Accounts: Only designated MYCDIC social media accounts (e.g., @MYCDIC on Twitter, Instagram, etc.) may represent the organization. These are managed by the MYCDIC Communications Team.

Access: Only authorized Representatives with training may post on official accounts. Requests for access must be submitted to media@mycdic.org.

Content Approval: All posts, including text, images, and videos, must be approved by the Communications Team before sharing.

5.2 Content Guidelines

Alignment: Content must promote MYCDIC's mission, events, or initiatives (e.g., conferences, youth programs).

Branding: Use MYCDIC's logo, colors (red/green/gold), and approved templates. Include official hashtags (e.g., #MYCDIC, #YouthDiplomacy).

Cultural Sensitivity: Ensure content respects Moroccan values and the cultural norms of global audiences. Avoid controversial or divisive topics.

Engagement: Respond to comments or messages professionally, escalating sensitive issues to media.presidency@mycdic.org.

5.3 Event Coverage

Pre-Approval: Obtain permission from event organizers before posting about MYCDIC events, especially sensitive or closed sessions.

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-SOCIAL-MEDIA-POLICY-CBEA2C22 | SIG RSA-E20099F64CAF19EBB0
SHA-256 FINGERPRINT EDDDC5EA5014EB148C462C6833FA2FB49E9B1C22184F4ADF48B5609EBF2E64EB

SCAN TO VERIFY

Live Posting: Use discretion when sharing real-time updates. Avoid disclosing confidential details or unverified information.

Tagging: Tag MYCDIC's official accounts and relevant partners, ensuring accuracy in captions and credits.

6 Guidelines for Personal Social Media Use

When referencing MYCDIC on personal accounts, Representatives must:

Disclaimers: Clarify that personal posts do not represent MYCDIC's official stance (e.g., "Views are my own").

Professional Conduct: Avoid content that could harm MYCDIC's reputation, such as offensive remarks, political endorsements, or inappropriate images.

Tagging MYCDIC: Seek approval from media.presidency@mycdic.org before tagging MYCDIC in posts about events or initiatives.

Confidentiality: Do not share internal MYCDIC information (e.g., meeting details, member data) without permission.

7 Prohibited Activities

Representatives are strictly prohibited from:

Posting discriminatory, harassing, or defamatory content.

Sharing misinformation or unverified claims.

Using MYCDIC's name, logo, or resources for personal gain or unauthorized purposes.

Engaging in online arguments or disputes that could reflect poorly on MYCDIC.

Posting about MYCDIC activities without approval, especially during sensitive diplomatic engagements.

8 Monitoring and Enforcement

Monitoring: The MYCDIC Communications Team monitors official accounts and may review public posts referencing MYCDIC.

Reporting Violations: Report concerns about social media misuse to compliance@mycdic.org or via the confidential form at https://www.mycdic.org/contact.html. Include screenshots or links to problematic content.

Disciplinary Actions: Violations may result in:

Removal of posts or account access.

Mandatory retraining.

Suspension or termination of membership, as per the MYCDIC Code of Conduct.

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-SOCIAL-MEDIA-POLICY-CBEA2C22 | SIG RSA-E20099F64CAF19EBB0
SHA-256 FINGERPRINT EDDDC5EA5014EB148C462C6833FA2FB49E9B1C22184F4ADF48B5609EBF2E64EB

SCAN TO VERIFY

Appeals: Representatives may appeal disciplinary decisions by contacting compliance@mycdic.org within 14 days.

9 Training and Support

Mandatory Training: Representatives managing official accounts or posting about MYCDIC must complete social media training, offered through workshops or online modules.

Resources: Access MYCDIC's social media toolkit (available via https://www.mycdic.org/documents.html) for approved templates, hashtags, and guidelines.

Support: Contact media.presidency@mycdic.org for guidance on content creation or crisis management.

10 Crisis Management

In case of a social media crisis (e.g., negative publicity, misinformation):

Immediate Action: Notify the Communications Team at media.presidency@mycdic.org. Do not respond publicly without approval.

Response Strategy: The Communications Team will issue approved statements and coordinate with leadership.

Transparency: Correct misinformation promptly with verified facts, maintaining MYCDIC's credibility.

11 Amendments

This Social Media Policy may be updated to reflect changes in social media trends, legal requirements, or MYCDIC's mission. Representatives will be notified via email and the MYCDIC website. The latest version is available at https://mycdic.org/documents/social-media-policy.pdf.

12 Acknowledgment

By participating in MYCDIC activities or using social media in connection with the organization, Representatives acknowledge their responsibility to adhere to this policy. Non-compliance may result in disciplinary measures, as outlined in the MYCDIC Code of Conduct.

Contact Information

For inquiries about this policy, contact:
Moroccan Youth Council for Diplomatic and International Cooperation (MYCDIC)

Email: contact@mycdic.org

Phone: +34 6 14 14 48 14

Website: https://mycdic.org

Headquarters: Madrid, Spain | National Coordinating Office: Rabat, Morocco | International Office: Brussels, Belgium | Spanish NIF: G75872663

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-SOCIAL-MEDIA-POLICY-CBEA2C22 | SIG RSA-E20099F64CAF19EBB0
SHA-256 FINGERPRINT EDDDC5EA5014EB148C462C6833FA2FB49E9B1C22184F4ADF48B5609EBF2E64EB

SCAN TO VERIFY

Approved by the MYCDIC Leadership Council on April 27, 2025.

Enhanced institutional safeguards

The following provisions strengthen the operational reading of this policy and apply together with the preceding rules.

Authority and representation controls

No member, ambassador, office-holder, volunteer, partner or contractor may bind MYCDIC, make commitments in its name, issue credentials, promise funding, accept legal obligations, or present personal views as an institutional position unless the authority is documented and current.

Titles, badges, cards, email addresses and public profiles evidence only the status shown in the live MYCDIC record. They must not be used to imply diplomatic immunity, governmental authority, consular powers, state accreditation or any status not expressly granted by the competent authority.

Conflict of interest, gifts and improper advantage

Covered persons must disclose actual, potential and perceived conflicts before participating in a decision, procurement, selection, partnership, evaluation, disciplinary matter or financial transaction.

Bribes, facilitation payments, secret commissions, kickbacks and any improper advantage are prohibited. Gifts or hospitality that could reasonably influence judgment must be declined or declared under the applicable approval process.

Information security and institutional records

Confidential, personal, financial, security, credential, investigation and unpublished strategic information must be handled only through approved systems and shared on a need-to-know basis.

Official records must not be altered, fabricated, backdated, selectively deleted or moved to personal accounts to evade oversight. Where a controlled register exists, the live register prevails over screenshots, forwarded files or private copies.

Safeguarding and non-retaliation

Harassment, intimidation, exploitation, coercion, discrimination, sexual misconduct, abuse of authority and retaliation against a person who raises a concern in good faith are prohibited.

Where safety, safeguarding, evidence preservation or institutional integrity requires it, MYCDIC may apply proportionate interim measures without treating those measures as a final finding.

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-SOCIAL-MEDIA-POLICY-CBEA2C22 | SIG RSA-E20099F64CAF19EBB0
SHA-256 FINGERPRINT EDDDC5EA5014EB148C462C6833FA2FB49E9B1C22184F4ADF48B5609EBF2E64EB

SCAN TO VERIFY

Interpretation and hierarchy

This policy must be read with the statutes, internal regulations, approved decisions, privacy rules, safeguarding controls and other applicable MYCDIC instruments. Applicable law always prevails where it imposes a higher or mandatory standard.

If two internal rules conflict, the competent governance body determines the controlling rule, taking account of legal hierarchy, date, scope and the specific decision involved.

Account security and access control

Official accounts must use MFA where supported, unique credentials, approved recovery methods and role-based access. Credentials must not be shared through personal chat threads or stored in public documents. Access must be removed promptly when responsibilities change.

Verification, AI and manipulated content

Representatives must verify material claims before publication. AI-generated, synthetic or materially altered content must not be used to fabricate events, quotations, endorsements, documents or identities. Where synthetic media could mislead a reasonable audience, appropriate disclosure is required.

Crisis and impersonation response

Suspected account compromise, impersonation, coordinated harassment, disinformation or accidental disclosure of confidential data must be escalated immediately. Authorized teams may preserve evidence, revoke sessions, issue corrections and coordinate with platforms or competent authorities.

Archiving and corrections

Important institutional posts, corrections and approvals should be retained in an auditable record. Deleting a public post does not remove the duty to preserve relevant evidence or disclose a material correction where necessary.

Accountability, records and continuing obligations

A person who leaves a role remains responsible for confidentiality, return of Council property, non-misuse of credentials and cooperation with legitimate record-preservation or investigation requirements concerning activity during their mandate.

MYCDIC may amend procedures, forms and technical controls without changing the underlying effective date of this institutional edition, provided that substantive policy amendments are approved through the competent governance process.

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-SOCIAL-MEDIA-POLICY-CBEA2C22 | SIG RSA-E20099F64CAF19EBB0
SHA-256 FINGERPRINT EDDDC5EA5014EB148C462C6833FA2FB49E9B1C22184F4ADF48B5609EBF2E64EB

SCAN TO VERIFY

Acknowledgement

Participation in MYCDIC activities constitutes a duty to read and comply with the instruments applicable to the relevant role. Where acknowledgement is required, electronic acceptance, signed forms, onboarding records or controlled administrative logs may be used as evidence of receipt.

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-SOCIAL-MEDIA-POLICY-CBEA2C22 | SIG RSA-E20099F64CAF19EBB0
SHA-256 FINGERPRINT EDDDC5EA5014EB148C462C6833FA2FB49E9B1C22184F4ADF48B5609EBF2E64EB

SCAN TO VERIFY

Institutional Application Annex

DOCUMENT

Social Media Policy

INSTITUTIONAL USE NOTE

This annex expands how the existing controlled document should be applied within MYCDIC. It does not silently replace the core text. Where the underlying document contains legal, statutory, registration, appointment or other authoritative wording, that original wording remains controlling unless a separately approved instrument expressly amends it.

Operational principles

Authority & scope

Use the document only within the mandate, office, programme or activity to which it actually applies. No publication or title may be read as conferring diplomatic, governmental or legal authority that MYCDIC does not possess.

Decision records

Material approvals, delegations, exceptions and risk decisions should be traceable to an authorized office, a dated record and an identifiable institutional reference.

Integrity & safeguarding

Apply conflict-of-interest, confidentiality, dignity, anti-harassment, data minimization and safeguarding standards proportionately to the activity and the people involved.

Public communication

External statements, branding, media activity and partner references should be accurate, reviewable and consistent with approved institutional positions and published records.

Category-specific implementation expectations

- Official accounts require named custodians, least-privilege access, multi-factor authentication where available and a documented recovery path.
- Separate personal opinion from institutional statements. Sensitive geopolitical or diplomatic content should receive appropriate authorization before publication.
- Archive material institutional announcements and corrections so the Council can demonstrate what was published and when.
- Do not publish private member, applicant, partner or event data unless there is a clear lawful and institutional basis to do so.
- Use a correction and crisis protocol for misinformation, compromised accounts, impersonation or harmful content.
- Respect copyright, image permissions, platform rules, accessibility and the Council's approved visual identity.

Control, Review & Digital Validation

Governance lifecycle

1

Apply

Use the document in the approved institutional context and identify the responsible office or role.

2

Record

Keep proportionate evidence of significant approvals, decisions, incidents, exceptions and outcomes.

3

Review

Reassess the document when law, institutional structure, risk, technology, mandate or operating practice materially changes.

4

Publish

Where publication is appropriate, expose only the public version and keep sensitive operational records separated.

Evidence and institutional recordkeeping

A controlled MYCDIC record should identify the applicable document version, decision owner where relevant, date, affected programme or office, and any evidence necessary to demonstrate responsible implementation. Public records must not disclose confidential personal data, private applicant material, security credentials, or information whose publication would create unnecessary risk.

DIGITAL VALIDATION RECORD

REFERENCE	**MYC-PDF-SOCIAL-MEDIA-POLICY-CBEA2C22**
SIGNATURE ID	**RSA-E20099F64CAF19EBB0**
PUBLIC KEY	MYCDIC-RSA-E8A93889B01EEB70
SOURCE SHA-256	CBEA2C22A38BA00A0DBB0C6D106EC8A8 AC26E4391CD1675C7704E6420AACEFE5
TEXT FINGERPRINT	289F3A8CE8A972DCCCC1F122D32CCDBB 0F094DB2AF29477DB9A2B69CA7973612
RSA SIGNATURE	mSH/FsGF79wXAYAOBzBKuQlGYYLjSXvk80eT5Vi06w0VQWZx8sZFi1hiZHR3zxPCFQyQen E4AexR48h1iOelJtK8eZn0oCx2J3Q5x73J5W76xW5poOx2tISiWh9lNbM1eIXCYHnS5z9L H9+YU9l/CzTco7wmLVvCX5bsRN4LY1DwiOx/CiEfK3hCx3vtIBZlGE52At48DIVvuAVkm/ sSFM1y0SS+F94FbuS2bGwSqpYaW3cNHVbyAnILeQatXTYlFXU7rNayKudP4wZgHS+JT8j8

SCAN TO VERIFY LIVE