Digital Media

and

Data Protection

Policy

for

Advance Afrika

Final Version

Published: Kampala, October 2022

Table of content

1. Administrative statement

Brief description
These policy and guidelines are a set of internal rules and instructions binding for all staff of Advance Africa telling how to handle communication on digital social media platforms and care about data protection privacy. This policy prescribes a framework for the regulation of content by online publishers, current affairs content and audio-visual content.

The scope of these policy is to streamline and harmonize all media and digital media activities like website content, newsletter and social media postings of Advance Afrika for better visibility, branding and marketing reason. It is a guidance about using digital media applications for external and internal communication and create awareness about mandatory ethic rules and considering data protection matters. Private activities on social media of staff members are excluded, so far as they are not concerning the organisations activities and policies.

This policy includes data protection and data security rules and principles binding for all Advance Afrika employees.

Policy effective.: This policy is effective from 1st of November 2022. All staff members, who have a working contract with Advance Afrika have to obey to the rules.

Approved by CEO Sharon Atukunda

Responsible organisation: Advance Afrika Uganda

Policy contact: Vivien Muyama E-Mail> vmuyama@advanceafrika.org; Sheila Innocent E-Mail: sinnocent@advanceafrika.org

Review status: To reflect the adaptive and changing nature of social media, the Digital Media Guide will be updated as appropriate.

Applies to all staff members of Advance Afrika, Uganda

History of involvement in producing the guideline: These guidelines have been developed and edited by Dr. Mark S. Degner, Technical Advisor for Advance Afrika

2. Introduction

Advance Afrika believes in sharing information and professionalism. We are handling personal information from our beneficiaries and partners with utmost sensitivity and follow data protection rules. In our work, we collect data from various sources - for research in our projects (like baseline, feasibility or evaluation data), and for our media and marketing activities (like reports, success stories, events or campaigns). We use this data to provide the best possible results for all our stakeholders and being accountable for our actions. Usage and storage of data requires rules, what to keep and what to share, which makes clear guidelines necessary.

Especially in using social media platforms and digital networks, we share information about our results and experience with the public, to get feedback which supports us to improve. Information sharing is crucial for our organisation, it helps to meet beneficiaries and client needs through quick response systems. We share also information about our provided services and improve access for clients to these services. Like every communication, this requires to accept rules and rights, which we take very seriously.

Most of the young generation in Uganda has access and are using digital media for communication and networking, like Facebook, Youtube, Instagram or WhatsApp. Social media has become a powerful tool to inform and connect with the communities, but engaging on such platforms without a clear strategy in place and a guidelines can end in failure and misunderstanding. This guideline will shape our online engagement through digital media in a way it will contribute to our overall objective to deliver services to the people of Uganda and worldwide audience.

3. Guiding principles for social media use

These guidelines are intended for and apply to anyone involved in creating, contributing or distributing information pertaining to Advance Afrika via digital media communication channels as the word wide web, social media platforms or web blogs.

We strongly encourage the engagement and integration of any digital media platform that can help achieve the objectives of our organization. It is important to remember all staff, that such efforts are part of Advance Afrika’s voice and we ask

them be mindful of the content they post and consider these principles, when they post on our website, on our social media accounts (Facebook, Twitter, LinkedIn, Youtube) or other digital publications like newsletters and Info-Mail.

1. Protect your privacy and that of others

For your own protection you should not share personal information such as phone numbers, complete physical addresses, passwords. When managing a digital media site, review the settings to determine what information is being disclosed and adjust the settings accordingly. Likewise, don't pass along personal information about others.

2. Offer Value to others

Digital media initiatives should be created when there is an opportunity to share information and build relationships. Listen and engage to get to know the others who are there. Your level of participation will determine the level of success of your participation.

3. Respect Others

Treat others as you would like to be treated. Keep in mind everyone is entitled to his or her own opinion and spirited debate can be a good thing. Always maintain a level of respect for others and their viewpoints. When disagreeing with others' opinions, **be polite.**

4. Be transparent

When posting, as an individual, on digital media platforms, honesty is the best policy and other users will tolerate nothing less. Use your real name when posting rather than a pseudonym or posting anonymously. When appropriate, clarify your position with Advance Afrika. If you have a vested personal or professional interest in a topic you are discussing, acknowledge this

5. Adhere to Legal or Regulatory Requirements

Never share proprietary or confidential information or comment on anything related to legal matters without the appropriate approval. Please be familiar with Advance Afrika's policies and procedures and legal data protection rules of Uganda.

As an NGO Advance Afrika cannot take a position on a variety of topics (i.e. political candidates) and employees of the NGO are prohibited from stating any position on behalf of the organisation without prior approval.

6. Decency and integrity

Do not post content or images involving the use Alcohol or Drugs Allowed of these substances.

If you make a mistake, admit it. Be upfront and be quick with your correction. If you're making changes to a blog to correct an earlier post be clear that you have done so.

7. Don’t use social media platforms as your bulletin board

Instead, look at them as a welcome window; an opportunity to meet, greet and interact with your clients, beneficiaries and interested visitors. Over time, your investment in this digital community will reap the same rewards, when you invest time and resources in communities in person: increased relationships, trust and valuable lines of communication.

8. Create some excitement

Give your audience a reason to follow or engage with you. Create excitement with good and transparent content.

9. When in Doubt, Don’t Post

If you are concerned whether posting something is appropriate,take a minute to review these guidelines again and modify your approach accordingly. If you're still unsure, you might want to discuss your concerns with someone in authority. Ultimately, what you publish is yours, as is the responsibility.

10. Be consistent in your conversation

If you post on various social media platforms or digital media channels be consistent in opinion, statement and outlining results. It is very confusing to find contradictive statements from the same source in different platforms.

11. Identify the purpose and have a plan

The information we provide should be unique and specifically support the stated objectives of our organization. Strive to be a valuable resource to our audience by providing important information not easily obtainable elsewhere.

Creating an online presence takes time and dedication. Make sure you have a plan about what you post and follow it for the most effective use of your time and to achieve your objectives.

12. Designate responsibilities

Social platforms open a portal for others to communicate with you. You must be prepared to respond to these posts as well as proactively engage with your audience to maximize the impact of your online efforts. Each social site, page or account for your group should have a designated administrator, as well as a succession plan should that person leave. These responsibilities should be reviewed on an annual basis to ensure adequate coverage.

4. Principles for using Facebook Platform, Twitter or LinkedIn

Advance Afrika reserves the right to moderate any and all comments. Comments will be removed if they meet any of the following criteria:

- Profanity, hate speech, and offensive or inappropriate language.
- Personal attacks on other users or Advance Afrika, staff or partners.
- Posts containing illegal activity, commercial, political or fund raising solicitations, spam, or copyright/trademark infringement.
- Posts containing advertisements or solicitations will be deleted.
- Off-topic posts inappropriate for this forum.

Advance Afrika reserves the right, at its discretion, to remove any post or to revoke a user's privilege to post to its Facebook page.

Comments posted by others do not reflect the opinions of Advance Afrika.
The Facebook rules are subject to change at the discretion of Advance Afrika
.

“Behave online in the same manner you operate in real life ! “

When officers contact residents every day, we expect them to be professional, courteous and able to answer general questions from the public. And in their contacts, we expect our officers to show humanity, compassion and empathy when appropriate as well as

taking control, being authoritative and in command when the situation dictates. It's no different online.

5. Data Protection Rules

5.1 Privacy Rules

We, Advance Afrika Management take the privacy of our project beneficiaries, partners, associates and social media users seriously. Our mission is to deliver services to people in need and building trust is one key principle of our intervention. Privacy Policy explains what information we collect during our project implementation and communication activities about you, why we collect the information, as well as how we collect and use the information so that we can deliver the best that we can.

This Privacy Rules are intended for individuals in Uganda. If you live outside of Uganda and choose to use the Sites connected with this Privacy Policy, you do so at your own risk and understand that your information will be sent to and stored in Uganda.

By using any of our websites and mobile applications that link to this Privacy Rules (collectively, "Sites") or otherwise providing Personal Information to us, you agree to this rules. Note that there may be other websites that reference the Advance Afrika but are subject to a different privacy policy.

5.2 Principles for use and protection of data at Advance Afrika

Data is…..

(a) processed lawfully, fairly and in a transparent manner in relation to individuals (follow the rules of lawfulness, fairness and transparency)

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

5.2 Personal Information on digital media

"Personal Information" generally means any information that can reasonably identify you as an individual, and any other information we associate with it. We collect categories of information, from different sources.

1. Profile information and other content you voluntarily provide us, which may include:

- **User name** and password
- **Contact information** when you register on our Sites or do business with us, such as your name, street address, demographic information (such as your gender), date of birth, phone number, and/or email address.
- **Other people:** You may also provide us information about other people, such as when you direct us to send a gift on your behalf. If you submit any Personal Information relating to other people in connection with the Sites, you represent that you have the authority to do so and to permit us to use the information in accordance with this Privacy Rules.
- **Similar professional contact** information if you interact with us in the scope of your employment, for instance if you book a corporate event. This may include

your employer, job title, work address, phone and/or email, and similar such information.

- **Any content or contributions** you post in a public space on the Sites. This includes comments, videos and photos that you might submit. If you contact us through a social media site, we may collect your social media identifier.

5.3 Children security

We do not knowingly collect or solicit any information on the Site from anyone under the age of 13 or allow minors under the age of 13 to disclose their Personal Information to us through the Sites. The Sites are directed to individuals who are permitted to share their Personal Information without parental consent.

5.4 Careers

The Sites may include a link to our Careers section. Any Personal Information submitted through that portion of the Sites, by upload or via e-mail, will be governed by our Resume/CV Submission Policy at

5.5 Website: Use of cookies

Cookies are small pieces of text. They are provided by most websites and stored by your web browser on the computer, phone, or other device that you are using. Cookies serve many purposes. They can help a website remember your preferences, learn which areas of the website are useful and which areas need improvement, and provide you with targeted advertisements or personalized content. Sometimes, cookies are enabled when pixels are placed on a website. Pixels are also referred to as web beacons, clear gifs, and tags. They enable websites to read and place cookies.

First-party cookies and third-party cookies

Cookies can be first-party or third-party. A first-party cookie is one that you receive directly from Advance Afrika when visiting our Site. A third-party cookie is one that you have received from another party, such as Google or Facebook. We do not control what third parties do on other sites. However, we may work with certain third-party providers such as Google or Facebook to permit their cookies to function through our Site so we can learn more about your web experience on our Site and better personalize our services for you.

5.6 How We May Use Personal Information

We may use Personal Information as permitted by law, for the following business purposes:

- to respond to your inquiries and fulfill your requests
- to communicate with you about and to process services, donations, promotions, campaigns, programs, contests , rewards and accounts
- to inform you about our projects, interventions, events or other promotional purposes
- to re-contact you if we have not heard from you in a while
- to permit you to participate in social sharing, including live social media feeds
- to perform analytics, quality control, market research, and determine the effectiveness of our websites, mobile applications, promotional campaigns, and develop new products and services

We may also use Personal Information as we believe to be necessary or appropriate for certain essential purposes, including:

- to comply with applicable law and legal process
- to respond to requests from public and government authorities, including public and government authorities outside your country of residence
- to detect, prevent, or investigate potential security incidents or fraud
- to facilitate the functionality of our mobile applications and websites
- to provide important product safety information and notice of product recalls

In addition to collecting Personal Information, we may collect information that does not identify you and is not associated with your Personal Information. We may also de-identify information so it no longer identifies you

6. Data SECURITY

Data security in Advance Afrika is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. It encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures.

We use standard physical, technical and administrative measures designed to reduce the risk of loss, misuse, unauthorized access, disclosure or modification of your Personal Information. Unfortunately, no system or network can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of any account you might have with us has been compromised), please immediately.

6.1 General principles

a. Each user shall be identified by a unique user ID so that individuals can be held accountable for their actions.

b. The use of shared identities is permitted only where they are suitable, such as training accounts or service accounts.

d. Records of user access may be used to provide evidence for security incident investigations.

e. Access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.

f. Advance Afrika restrict access to confidential and sensitive data to protect it from being lost or compromised in order to avoid adversely impacting our customers, incurring penalties for non-compliance and suffering damage to our reputation.

g. At the same time, we must ensure users can access data as required for them to work effectively.

6.2 Access Control Authorization

- Access to company IT resources and services will be given through the provision of a unique user account and complex password. Accounts are provided by the IT department based on records in the HR department.
- Passwords are managed by the IT Service Desk. Requirements for password length, complexity and expiration are stated during registration.
- The company shall provide all employees and contracted third parties with access to information they need to carry out their responsibilities as effectively and efficiently as possible.
- Information that is classified as Public is not subject to this policy. Other data can be excluded from the policy by company management based on specific business needs, such as that protecting the data is too costly or too complex.

6.3 Data Back-up Security

Data storage refers to holding data files in a secure location that can readily and easily be accessed. Data backup, in contrast, refers to saving additional copies of your data in separate physical or virtual locations from data files in storage.

Making backups of collected data is critically important in data management. Backups protect against human errors, hardware failure, virus attacks, power failure, and natural disasters. Backups can help save time and money if these failures occur.

Data is the foundation of our work! If we lose data, recovery will be slow, costly, or impossible. It is important that we secure, store, and backup our data on as regular a basis as possible!

Securing our data will help to prevent:

- Accidental or malicious damage/modification to data
- Theft of valuable data
- Breach of confidentiality agreements and privacy laws
- Premature release of data, which can void intellectual property claims
- Release before data have been checked for accuracy and authenticity

Regular backups protect against the risk of damage or loss due to hardware failure, software or media faults, viruses or hacking, power failure, or even human errors.

6.4 Security of Data and Network

Physical security and computer security of data must be considered in good data management. While it is encouraged to make scientific data available to the public, sometimes confidential or sensitive information must be kept secure.

Date security needs to be considered for all copies of our data, including our working data set, backup copies and archived copies.

- Network security
    - Keep confidential data off the Internet
    - Put sensitive materials on computers not connected to the internet
- Physical Security
    - Restrict access to buildings and rooms where computers or media are kept
    - Only let trusted individuals troubleshoot computer problems
- Computer Systems & Files
    - Keep virus protection up to date

- Don’t sent confidential data via e-mail or FTP - use encryption, if you must send data
- Use good passwords on files and computers

6.5 Storage & Backup

One of the most important data management tasks is keeping backups of our data. There is a real risk of losing data through hard drive failure or accidental deletion.

- Remember to use the Backup 3-2-1 Rule
  - 3 copies of your data - 2 copies are not enough!
  - 2 different formats - internal hard drive + tape backup or / flash drive
  - 1 off-site backup - have 2 physical backups and one in the cloud

- Backup options we use
  - Hard drives - personal or work computer
  - Departmental or institution server
  - External hard drives
  - USB Flash backups
  - Cloud storage

Note that for some types of sensitive data and research, we may have restrictions on where we can safely put our data and its copies.

Author of first edition:

The first published version of these Digital Media and Data Protection policy was written and edited by Dr. Mark S. Degner, Technical Advisor seconded by German BfdW Bread for the World organization, advising Advance Afrika in Communication and Digitalisation. Oct 2022.

The policy was developed in collaboration with CEO Sharon Atukunda and Communication Officer Vivien Muyama.