NETWORK AID AFRICA
INTERNET POLICY 2026

Protection Against Internet Abuse & Misuse

Abstract
We believe that your success is our success. That's why we've developed this Internet Policy to help outline our policies and procedures and to help guide you throughout your relationship with us.

Tel: +23275525100 Website: www.networkaidafrica.org Email: contact@networkaidafrica.org or nnetaid@gmail.com

Network AID Africa Internet Policy 2026

1. Overview

The internet has changed the way that we all act and interact. At Network AID Africa Africa (the "Organisation"), we recognize that all Employees/Volunteers utilize the Internet in their day-to-day lives. This Internet Policy is created to ensure that those working for or with the Organisation are using the Internet appropriately and responsibly, to ensure the interests of the Organisation and its constituents are protected.

The Internet Policy establish and outlines the rules, practices, and procedures for Employees/Volunteers utilizing the Internet, either on their own time or on Organisation devices. Internet Policy includes information about cell phone and social media usage, as well as rules governing e-correspondence, such as e-mail etc. The Policy, informs Employees/Volunteers about the standards that are expected of them while utilizing the Internet. This Policy is an extremely important document in the life of the Organisation.

Employees/Volunteers are required to read and review the policy and agree to it through their employment/volunteerism and sign.

We believe that your success is our success. That's why we've developed this Internet Policy to help outline our policies and procedures and to help guide you throughout your relationship with us.

2. Purpose

The purpose of this Internet Policy is not only to help you ensure a fruitful working relationship with the Organisation but also to clarify the specific rules regarding usage of the Internet while at work or while you are representing the Organisation. Your personal activity on the internet may be subject to this Policy if it impacts the business of the Organisation, Organisation Employees/Volunteers/volunteers or third party, or your work at the Organisation.

3. Applicable Law

Internet Polic is subject to State law, in that they are not permitted to restrict employee free speech or organizing, even if that activity is done online. State laws will cover the individual elements of the employment relationship.

4. Read and Review

Please take the time to read and review this Internet Policy as thoroughly as possible. If you have any questions, please reach out to your line coordinator. This Policy is to be read in conjunction with any other workplace policies you have received, including those about appropriate conduct. Employees/Volunteers who do not abide by his Policy may be subject to disciplinary action, up to and including termination.

Network AID Africa Internet Policy 2026

5. Definition

The following definition will be used for "social media" in the context of this Internet Policy: mobile and web-based applications for user-generated content, communication, and social interaction. This definition includes, but is not limited to, the following social media platforms: blogs, online communities; discussion forums, review sites, Instagram, Twitter, Facebook, LinkedIn, Snapchat, Youtube, WhatsApp, Reddit, Google+ and any other related or similar websites.

6. Confidentiality

Your work at the Organisation shall generally be considered confidential. This confidentiality extends to any internal and external communications made as a result of your work with the Organisation through the Internet, such as e-mail, text messages, voicemail, or other appropriate means of electronic communication. All communication made as a result of your work with the Organisation should be professional, not personal, communication. The communications you make in this regard may be subject to discovery in litigation.

7. Monitoring

The Organisation reserve the right to monitor your electronic communications and content, including files, folders, and internet usage undertaken while at work or off work or on Organisation devices.

8. Organisation E-Correspondence

A wide selection of communication methods may be used in the Organisation. At minimum, they include SMS/text messaging, email, article, media, voicemail and instant messaging, and are on and through electronic devices such as telephones, computers, Internet and mobile devices (cell phones, tablets, etc.). These, as well as their contents, such as physical and digital files, data, and operating programs, will be further referred to as "e-correspondence." All forms of e-correspondence are strictly for professional use as they are the exclusive property of the Organisation.

The following list and standards regarding e-correspondence are not comprehensive as the Organisation has the right to adjust the rules if necessary. All forms of e-correspondence that: (1) can identify the Organisation; (2) can be accessed on the Organisation's property, and (3) can be accessed by using Organisation funds or on equipment provided by the Organisation will adhere to the following rules:

a) Employees/Volunteers may not, under any circumstances, install personal software on any Organisation-owned computer system. Employees/Volunteers may not use e-correspondence for any activity such as patent, copyright, or trademark infringement, libel, slander, or unauthorized sharing of trade secrets. E- correspondence shall not be used against the Organisation's best interest or be activity that can be considered illegal. E-correspondence shall adhere to Organisation policy and shall not constitute harassment, hate, racist, use of

obscene or discriminatory language. Any activity thereof will be subject to discipline up to and including termination.

b) Employees/Volunteers must make all e-correspondence as accessible as possible within the Organisation. Employees/Volunteers do not own any e-correspondence, be it confidential or password protected. Personal passwords used on Organisation devices are considered Organisation property and may be overridden at any time, if necessary. The Organisation may keep all passwords, codes, etc. on record. The Organisation maintains the rights to all information created by an employee on the property or transmitted to the premises.

c) The Organisation may ensure violations of Organisation policy and applicable law do not occur by monitoring the employee and their activity. The Organisation may view all e-correspondence and digital information, including blogs and other social media, at any time. Any information created or obtained by the employee/volunteer may be disclosed to the Organisation, if necessary.

d) Employees/Volunteers may not encrypt programs or install encryption software with any email communications. Employees/Volunteers may not use any form of anonymous correspondence. Employees/Volunteers shall not have access to any e-correspondence of third parties or other Employees/Volunteers under any circumstances except with authority from the senior coordinator and approval from the Chief Country Coordinator/Country Coordinator.

e) All devices for receiving and recording information such as computers, telephones of any kind and fax machines or scanners may not be used for transmitting sensitive information or sharing Organisation secrets.

f) Use of Organisation-funded communication services, websites and the Internet is permissible for Organisation-related business only. Prior approval must be requested before any information about the Organisation, its products, or services can appear in the electronic media to be accessed by others.

9. Social Media Policy

Please be advised that this Policy asks you to assume that all of your online activities are publicly visible and available at any given time. You may be subject to termination for violating any of the Organisation's internal policies, such as posts which may display unlawful harassment or discrimination or which may include racial slurs, epithets, and/or derogatory remarks, stereotypes, jokes, offensive visuals based on race, national origin, age, disability, marital status or other legally protected classifications.

While you are permitted to use social media at work, the Organisation requires that you remain within the following guidelines:

a) Personal social media use is limited to a few minutes per workday.
b) Representing the Organisation or Organisation activities is not permitted unless you are specifically authorized to represent the Organisation as described elsewhere in this Policy

c) Sharing of Organisation intellectual property like trademarks or copyrights is not permitted
d) All internal Organisation policies apply
e) Ensure that you make clear your personal opinions and statements do not represent the Organisation

While you are permitted to use social media on Organisation electronic devices, the Organisation requires that you remain within the following guidelines:

a) Visiting any obscene, adult, or 18+ websites is not permitted
b) Visiting any unlawful websites is not permitted
c) Participating in any security breach or hacking activity is not permitted
d) Always consider that your activity may be monitored
e) Personal social media use is limited to a few minutes per workday
f) Representing the Organisation or Organisation activities is not permitted unless you are specifically authorized to represent the Organisation as described elsewhere in this Policy
g) Employees/Volunteers who are permitted to access the Organisation's social media accounts to post content online will be specifically notified as such in writing. If you are not one of these Employees/Volunteers, you may not utilize the Organisation's official social media accounts or represent the Organisation online in any way.

If you are permitted to officially represent the Organisation online, the following guidelines apply:

a) Be respectful and polite. Never get into arguments with customers or clients.
b) Avoid making promises. If you are dealing with a person's service issue, always offer to speak to the person or client on the phone, rather than making express promises online.
c) Do not answer questions that are not within your expertise. If you need help from the senior coordinator or line coordinator, ask before you post.
d) Follow all written Organisation guidelines, such as the Organisation's employee handbook, confidentiality policy, and any other written documents.
e) Never share sensitive Organisation information, even if it is not subject to a written policy. Sensitive Organisation information includes person's and client lists, marketing strategies, financial information, protected intellectual property, donor/partner numbers, or any other information which is not generally publicly available.
f) Remain in constant contact with the partnership, fundraising and IEC team regarding the content you post.
g) Avoid deleting a person's or client's comments or questions, even if you disagree with them.
h) Do not post anything which may display unlawful harassment or discrimination or which may include racial slurs, epithets, and/or derogatory remarks, stereotypes, jokes, or offensive visuals based on race, national origin, age, disability, marital status or other legally protected classifications.
i) Correct false information about the Organisation as soon as possible.
j) Never violate the intellectual property rights of any third party. Obtain proper permission to use any content, and always use the correct attribution form.

k) Be mindful of the following rules:
   i. Do not post between the hours of midnight to 4 am except for exceptional cases with approval from the senior or line coordinator

While your activities on your own time and devices are your own business and responsibility, the Organisation requests that you keep the following in mind for your own personal social media activities:

a) Always act according to the terms and conditions of the social media websites you are posting on.
b) Ensure that you make clear your views are not the Organisation's views, through disclaimers.
c) Always act lawfully.
d) Avoid discussing illegal activities, such as drug use, trafficking, money laundering, child pornography, kidnapping, incitement etc.
e) Always ask others for permission before posting about them.

Please keep in mind that you are an at-will employee, and if the Organisation discovers any objectionable content on your personal social media accounts, you may be subject to termination.

While adhering to the Organisation's policies, Employees/Volunteers are encouraged to use their social networking platforms to support the Organisation's activities through their personal social media accounts.

You are legally responsible for anything you post on your personal social media accounts, including failure to disclose relationships in marketing, or posting about any unlawful activity. If you violate any laws while posting on the Organisation's social media accounts, you may be required to indemnify the Organisation for any damages caused.

Please place cell phones on vibrate mode, silent mode or completely powered off during work meetings as a courtesy to others.

10. Signature/Consent

For any questions, please see your line coordinator.

Employee Name:…………………………………………..

Employee Signature:……………………………………

Date:………………………………………………………