INFORMATION AND TECHNOLOGY POLICY

Kabul, Afghanistan

January 2021

Contents

Summary

The objective of AAEHDA IT Policy is to foster an environment that will secure information within the Youth Health and Development community from threats against privacy, productivity and reputation. This policy creates an effective, professional, legal, ethical and equitable IT usage environment across AEHDA countrywide. Owned by AEHDA Executive Director, this policy will be implemented by the Provincial Coordinators and Project Managers as well as the respective IT Manager.

This policy is binding on all AEHDA offices, including all incoming staff, contractors or consultants who make use of AEHDA IT resources. This policy is a minimum non-negotiable set to be implemented in regional offices.

AEHDA IT Policy will be reviewed annually. AEHDA management and IT Manager will have the authority to enforce these policies through appropriate technology.

1. Introduction

AEHDA regional and central offices are linked by a common vision, common mission and values, common strategies and policies, common themes and campaigns and a single brand. In this scenario, the vital element that keeps us linked is information. It is the role of the IT Manager of AEHDA to ensure that we have the right infrastructure and systems to keep this information flowing.

Through this policy, we seek to create an effective, professional, legal, ethical and equitable IT usage environment across AEHDA in Afghanistan.

1.2 Scope of the policy

This policy is binding on all AEHDA offices, including all incoming affiliates. They are also binding on all staff, contractors or consultants and others (including others NGO employees, partners and board members) who make use of AEHDA IT resources located off AEHDA premises. e.g. laptops used by staff at home or when travelling. Appropriate policies are also binding on the usage of AEHDA information and systems on non-AEHDA resources.

This policy should be regarded as a minimum non-negotiable set to be implemented in all AEHDA offices. It should be noted that any local legal or regulatory requirements that are stricter than this policy will supersede the policy.

1.3. About this document

This document includes general user policies and is aimed at users and IT technical staff. All employees will be provided with the IT policy upon joining the organization.

1.4 Review of the policy

The policy will be reviewed annually. Revised versions will be issued if there are any significant changes in technologies or environment that warrant change in the way we work.

2. Compliance to this policy

2.1 Compliance and monitoring of this policy

AEHDA Executive Director and IT Manager will have the authority to enforce these policies through appropriate technology, and to audit and check compliance (manually or through technology) of all AEHDA IT resources. Compliance to policy will also be monitored in the usual way through audits.

2.2 Action in the event of a breach of this policy

Where there is assessed to be a serious breach of this policy, AEHDA will act promptly to prevent the breach being continued or repeated. e.g. immediately removing any unacceptable materials. This action will be taken according to normal line management arrangements, and will typically involve the appropriate member(s) of senior management.

Actions that will be taken in such situations will be as follows:

- Any indication of non-compliance with this policy will be investigated in line with normal Disciplinary Procedures.
- Non-compliance with this Policy will lead to appropriate disciplinary action, which could include dismissal on the grounds of gross misconduct. If non-compliance is considered to be a criminal offence, it will be reported to the legal authorities for them to take appropriate action.
- Access to Internet, email and other facilities may be withdrawn at any time as a result of, or pending the outcome of, investigations into suspected misuse.
- Users might be personally liable to prosecution, and open to claims for damages if their actions are found to be in breach of the law in the country in which the member of staff is working. If a user is accused of harassment, claiming they did not intend to harass or cause offence will not constitute an acceptable defense.

3. General user policy

3.1 User account and e-mail id creation and deletion

All AEHDA staff, long-term contractors, and long-term and full-time consultants are provided with a user account within the “AEHDA” domain, as well as an e-mail ID [of the form <first-name>. <last-name>@AEHDA.org. The display name will be of the form <firstname> <last-name> e.g. Email ID: marco.deponte@AEHDA.org; Display name: Marco DePonte. Any exception to this needs to be approved by AEHDA Executive Director.

Email IDs of any other format are in the process of being discontinued.

Process: The IT staff do not have the authority or responsibility to set up or delete user or email IDs. This authority/responsibility belongs to HR department.

3.2 Responsibility for assigned resources

AEHDA employees will be held responsible for AEHDA information resources assigned to them and should ensure the security of their passwords and other resources.

Unauthorized access of AEHDA information resources including other people's email and other accounts will invite disciplinary action.

3.3 Ownership of AEHDA Information

All information contained in the AEHDA network (including servers, desktops, laptops, mobile phones etc.) is deemed to be property of the organization.

It is an offence that attracts disciplinary action for anybody (including the IT people) to access anyone else's information without authorization from the owner of the information or from the Executive Director.

It required that anybody leaving the organization should properly handover all project information (incl. files, e-mails, reports, documents etc.) and resources (incl. laptop, mobiles etc.) that was in his/her care to the next person who takes on the role (or equivalent) or to an authority designated by his/her manager or to the local HR person.

Portable storage devices cannot be used to store critical or sensitive data. However, if necessary in order to provide a required business function an exception must be approved by the manager. Ensure that critical data on portable storage device is password protected and if possible required appropriate encryption processes must be implemented.

3.4 AEHDA standard

AEHDA employees will be provided with the resources to access organizational information. Where staff are given individual machines for use, they will be given only one of a desktop or a laptop. The local logistic team will keep a pool of laptops to provide for any needs of employees who have only a desktop. All desktops/laptops will be built with standard software's.

Laptops, desktops, mobile phones etc. should be replaced (if so assessed by IT) only after three years of use or if they become dysfunctional and cannot be repaired.

3.5 Virus protection policy

The virus protection software must not be disabled, bypassed or have its settings altered.

All viruses that are not automatically cleaned by the virus protection software must be reported to the IT Manager.

Users must not intentionally write, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any organization's computer systems.

Attachments to electronic mail and externally supplied, computer-readable files, software programs, databases, word processing documents, and spreadsheets must not be executed or opened unless they have been checked for viruses.

Users should consult IT before plugging in any portable devices like USB drives, SD cards, CDs, DVDs etc. They can carry viruses and can cause damage to our systems. You will be held responsible if you do not check with IT on this.

3.6 Network access policy

Access to the AEHDA information network is permitted only with devices authorized. Any access to the network bypassing the official gateways, firewall etc. is forbidden. Users are not allowed to change device ids, configurations or other details on any of their devices. Users should not divulge their access details to outsiders nor allow outsiders to access AEHDA resources in any way except on permission from Executive Director.

Users should not download, install or run unauthorized programs on their desktops, laptops or other devices.

Users should not use AEHDA resources for any illegal or unethical activity including accessing unauthorized resources within or outside AEHDA.

3.7 Backup policy

All business critical data will be backed up on a monthly basis. The local IT responsible will enter into an agreement with users for this purpose. The Executive Director is responsible to keep the backed up data in his possession. In regional offices, the provincial coordinators are responsible to do so.

Any data not covered by this agreement will need to be backed by the user individually.

3.8 E-mail policy

All e-mails that are created, received and stored, or transmitted through AEHDA corporate e-mail system are solely AEHDA property.

Users must not create rules or scripts to automatically forward e-mail located on internal AEHDA system to external e-mail services like yahoo or gmail.

The external e-mail addresses should be included in our distribution groups with approval by the Executive Director.

Users must be careful to address e-mail messages correctly to ensure messages are sent only to the intended e-mail recipients.

Users must not use e-mail to represent, give opinions, or otherwise make statements to external parties on behalf of AEHDA unless appropriately authorized to do so.

Users must not knowingly open e-mail or e-mail attachments from unknown external sources or that are suspected of containing viruses or malicious code.

The following activities are prohibited and may result in disciplinary action:

- Intercepting, eavesdropping, recording or altering another person s e-mail message
- Adopting the identity of another person in any e-mail message
- Misrepresenting your affiliation on any e-mail message
- Composing e-mail that does not conform to the AEHDA values and or integrity policy, including but not limited to sending racially or sexually explicit or harassing messages and/or files or use of profanities.
- Using e-mail for any non-AEHDA business purpose (personal mails are allowed to a limited extent)
- Sending or receiving software or any other material in violation of copyright law or other legal requirements.
- Sending chain letters though e-mail
- Sending unsolicited messages to large groups (SPAM) except as required to conduct AEHDA business.
- Sending messages that may be construed as a threat or related to acts or instruments of violence
- Attempting to access e-mail without proper authorization
- Using e-mail for purposes of political lobbying or campaigning unless explicitly approved by AEHDA Executive Director

3.9 Personal use

AEHDA permits the use of its computing resources like email, internet, DVD/CD drives etc. by staff and other authorized users for a reasonable level of personal use (like viewing Bank account/ use for booking train / airline tickets / News website / financial information / watching movies etc.). An absolute definition of abuse is difficult to achieve (the use should not add to our costs) but certainly includes (but is not necessarily limited to):

- A level of use that is not detrimental to the main purpose for which the facilities are provided. Priority must be given to use of resources for the main purpose for which they are provided.
- Not being of a commercial or profit-making nature, or for any other form of personal financial gain.
- Not be of a nature that competes with AEHDA business.

- Not be connected with any use or application that conflicts with an employee's obligations to AEHDA as their employer.
- Not be against AEHDA rules, regulations, policies and procedures and in particular these set of policies.

It is not permitted to use AEHDA IT systems to store or pass on pornography, or any other material that could cause offence or injury.

It is not permitted use resource-heavy facilities for personal use like downloading music, using Skype, msn etc. for talking to friends on VoIP etc. These will choke up our limited bandwidth and will slow down legitimate business accesses.

3.10 Quotas and limits

All e-mail boxes have quota limits placed on them. Users receive email notification when approaching their quota limit and are encouraged to follow guidance in this email and guidance from their IT officer to manage their account. Once over quota, no further email can be delivered to an individual's inbox until they have reduced their storage below their limit.

Some types of attachments to e-mails (like .bat, dll and many such others) that are considered harmful will be blocked by our spam control system and will not be delivered.

3.11 Legal Consequences of Misuse of Email Facilities

In a growing number of cases involving civil or criminal law, email messages are produced as legal evidence. There are a number of areas of law which apply to the use of email and which could involve liability of users or AEHDA. These will usually include intellectual property, obscenity, defamation and data protection, discrimination and harassment.

3.12 Internet (browsing) policy

All internet access should be through the configuration set up by AEHDA IT team. All internet access will be scanned for viruses and monitored and recorded and filtered for inappropriate access.

The following categories should not be accessed or used.

Adult/Sexually Explicit sites, Intolerance & Hate sites, Criminal Activity sites, Tasteless & Offensive sites, sites promoting Violence and/or Weapons, Illegal sites catering to Drugs, Hacking, Spyware, Religion, Sex Education, Phishing & Fraud, sites providing Ringtones/Mobile Phone Downloads, Spam URLs, Proxy and Translators, unlicensed software, music and video streaming and material that violate international, national or local laws and regulations. [This is not an exhaustive list. Please keep away from sites that are suspicious in any nature]

Access to blocked sites will be allowed to individual users on authorization from the Executive Director.

All users must ensure that they do not knowingly or unknowingly enter into any agreement with third parties on behalf of AEHDA without explicit approval from appropriate authority.

The AEHDA network should not be used to conduct personal businesses (including blogging).

No software (freeware, shareware or paid) should be downloaded or installed on AEHDA systems except those permitted by the IT department and under IT supervision. These include various types of anti-spyware software, toolbars and nifty utilities. Plug-ins or active contents like ActiveX, Applets from un-trusted sources should not be installed or run. If there is a business need to download/install some software please check with AEHDA IT Manager and logistic department.

Please refrain from clicking the "Agree" or "OK" buttons that you may find in suspicious pop-up windows. These buttons can masquerade as innocent features that inadvertently start an unwanted download of Spyware/adware program. Instead, close the window.

Any suspicious activity that may happen as part of your browsing should be reported to the IT Manager.

In addition to reporting problems with systems you are also required to report directly to IT the following types of incidents:

- Disruption of AEHDA services
- Loss of sensitive information
- Violation of AEHDA Security / Integrity policies
- Unauthorized access to information
- Unauthorized modification of information / data
- Identity thefts
- Loss of AEHDA assets
- Misuse of information & Computing resources
- Unusual behavior of system
- Incidents related to physical security such as but not limited to, laptop lost, unauthorized entry into premises, assault etc.

3.13 Responsible/Green IT use

- Switch off all desktops and monitors in the evening
- Enable automatic shutdown of desktops if they are not used for 15 minutes.
- Do not take print-outs unless it is absolutely necessary and use double-sided printing where possible.
- Re-use printed paper for notes etc.
- Unplug mobile phone charger when not in use.

3.14 Policy on use of Voice over IP (VoIP)

Where technologically possible, it is AEHDA policy that we use VoIP phones such as Skype, MSN etc. to make official calls so that we can bring down our communication costs. Some of these products also allow videoconferencing and these can be used to reduce travel costs. Ids of Skype, MSN etc. should be made available to our personal information file and email signature, so that contact through these becomes easy.

3.15 Security of Information Technology Resources

Every information technology (IT) device connected to AEHDA network must have at least one individual who is responsible for the security of that device. The organization must preserve its information technology resources, comply with applicable laws and regulations, and protect / preserve its data. Toward these ends, staff must share in the responsibility for the security of information technology devices.

3.16 Administrative Rights of IT Officer/Manager

IT Officer/Manager of AEHDA are not allowed to access content information (e-mails, documents, etc.) on user machines except on authority from the user of this information or from the Executive Director and after complying with local laws.

However, the IT Officer/Manager of AEHDA will have the following administrative rights:

- IT Unit is permitted access to a network user's computer when that user has given explicit consent for such access, as during installation, upgrade, troubleshooting and repair operations.
- IT Unit has access to information about the current configuration of any user's networked computer, subject to the limitation that no user-input information is to be collected by the administrator.
- IT Unit is authorized to use utilities to help identify peripheral/device specification, system resources, and operating system specifications and isolate system faults.
- IT Unit has special authorization to use network administrative rights from the client machines for installation and configuration purposes.
- IT Unit is permitted to make use of network management software for optimum network services. This includes file and bandwidth identification and allocation areas. This is to protect the maximum amount of network bandwidth for professional purposes of the organization.
- To optimize system resources, identify errors and trend analysis, IT Management may comprehensively log email and/or Internet traffic at any time without prior notification.

4. Technical policies

4. 1 Data Security

All AEHDA/partners critical or sensitive data must be stored on a secure server with appropriate access control rights. All data retention or storage should be in accordance with any local legal requirements.

Access to computing resources and information must be limited to those individuals who require such access due to the nature of their role and responsibilities within the organization.

An owner must be assigned to any shared document folder or intranet workgroup that is set up. The owner has complete ownership on the folder or workgroup and owner can add / remove users based on the project requirements.

4.2 Resources Management and License policy

All AEHDA laptops, desktops, servers, mobile phones etc. must operate with legal, licensed software. All offices should follow this strictly. The Executive Director and/or the head of the office will be held responsible for this. It is considered an offence that can attract disciplinary proceedings for anyone to download or install illegal or unlicensed software on AEHDA resources.

IT Officer should keep an inventory of all IT systems under their care and ensure (with the help of HR and logistic department) that laptops, mobile phones and other equipment given to staff are returned when staff leave the organization.

4.3 Virus protection policy

All workstations and other IT resources (servers, gateways, etc.) whether connected to the AEHDA network or standalone, must use the most current approved standard virus protection software and configuration. The virus protection software must not be disabled, bypassed or have its settings altered.