Acceptable IT & Computer Use Policy Manual

February 2014

1. **PURPOSE OF THE POLICY GUIDE**

As an employee of EAS, you are required to comply with EAS' Data Protection Policy and IT Security Policy.

These policies ensure best-practice in the management, storage and use of EAS IT systems, assets and electronic data.

The IT & Computer Use Policy Guide provides employees with strict instruction on the use of various IT services to ensure their employer- EAS – can continue to adhere to these policies.

All employees with EAS must agree to abide by the rules and procedures outlined in this document before they will be allowed access to the Academy IT systems, databases, or issued an Academy email address. Compliance with its principles is also mandatory for any authorized third party users accessing any computer system owned or operated by EAS.

Any actual suspected breaches of the rules and procedures contained in this document within or affecting the Academy's systems will be thoroughly investigated in accordance with EAS disciplinary procedures and may lead to disciplinary action being taken. Serious breaches may amount to gross misconduct resulting in summary dismissal.

Any action taken internally does not preclude prosecution through a court of law.

We reserve the right to amend this policy Guide when deemed appropriate by the Academy.

2. ASSET AND DATA SECURITY

The rules and guidelines described here apply to all computer users accessing/operating any IT services owned and/or operated by EAS. Their application extends to the use of all such equipment, or access to any EAS database/IT system in the secretariat, at home and/or overseas.

These guidelines have been written to help employees guard against the risk of theft of hardware and software, the unauthorized access of data, the maintenance of system security and protection of the Academy's intellectual property.

Asset Security

The rules should not disclose information relating to the Academy IT facilities to anyone outside the Academy without the Academy's expressed permission. Any telephone or email approaches canvassing for information should be passed directly to the IT officer of EAS under EAS' IT Security Policy.

Laptop computers or other portable data-storage devices should not be left unattended in any location, and never left in plain sight in cars, public transport or hotels. Laptops should not be kept on desks overnight and must be stored in locked cupboards, drawers or taken home. If left unattended in a car, these must be locked in the boot or glove compartment at all times.

Only nominated IT personnel or contracted third party personnel at the direction of the Executive Director are permitted to move any IT equipment with the exception of portable equipment such as laptop computers.

It is prohibited to deliberately attempt to access a system to which you have no authority. EAS regularly monitors all systems through its third party contractors and all unauthorized attempts to access systems are investigated.

Data Security

All computer and IT system users are given a Username and Password; these are unique and must not be shared with any other employee. No user is permitted to log onto any other users account without good cause. Failure to comply with this will lead to disciplinary action being taken.

Passwords to EAS IT systems or email accounts should not be written down, or kept where others might find them. All passwords should be hard to guess and it is recommended they contain at least eight characters, including upper and lower case letters, numbers and special characters such as ! # £ $ ( ) ^. Passwords should also ideally be changed at regular intervals.

Computers logged onto EAS' internal network or an EAS email account, should never be left unattended and unlocked, especially when in-use outside the office. The user logged in at a computer will be considered to be the legal author and progenitor of any messages sent from that computer, and will be liable for any network activity logged through their user account.

Data should always be saved on a shared network drive managed by EAS. The copying of EAS data on to personal computers, external hard drives or any other portable device is strictly prohibited. Any and all data held on EAS computers and servers is the property of EAS and its clients, and must be returned or deleted on request.

3. SOFTWARE

Installation or copying of any software onto EAS computers is strictly prohibited without prior consent of the EAS IT officer as this may: (a) cause unforeseen software conflicts leading to data and/or system integrity loss; (b) reduce the efficiency, or otherwise compromise the operation of EAS IT systems/computers; or (c) unknowingly constitute a breach of copyright law.

Legitimate copies of software will be purchased and provided, if and when required.

The following additional guidelines are designed to protect EAS and its employees from a reduction in, or critical loss of IT system services. At all times, employees:

- must protect their computer against the threat of invasive viruses and other malicious intrusions by ensuring their anti-virus protection software is active and up-to-date, and that all email content controls are active and not purposefully circumvented;
- Must not, under any circumstances, download software from the Internet other than with the express permission and guidance of EAS IT officer. This also applies to the downloading of copyrighted music files and non-work related video footage, third-party applications, games and screen-savers; and
- Must not bring software from home and load it on to any EAS computer, or copy any EAS licensed software and load it onto home computers or any other personal device.

All software, information and programs developed for and/or on behalf of the EAS by employees or contracted third-parties during the course of their employment remain the property of EAS. Duplication, use or sale of such software without the prior consent of EAS will be an infringement of the Academy's copyright and will be dealt with as a disciplinary matter. This may become a prosecution under law if employment has already terminated when the copyright is infringed upon.

4. ACCEPTABLE EMAIL AND INTERNET USAGE

EAS provides its employees with access to the internet and its email system to assist them in the performance of their duties. Their use should primarily be for official Academy's business; however, minimal personal use of the internet and EAS email is permitted, provided the user complies with the provisions contained in this Policy, as follows:-

- personal use of the email system or surfing of the internet should never impact the normal flow of business related email and network traffic. EAS reserves the right to ask its mailbox hosts to purge identifiable personal email to preserve the integrity of the email systems, and to restrict the access of specific individuals to the internet should their use be judged excessive.
- The viewing, creation or transmission by any employee, consultant or contractor of any offensive, obscene or indecent images, data or other restricted material by email or on the internet is prohibited. Examples of prohibited material include, but are not limited to:
    - Sexually explicit messages, images, cartoons, or jokes;
    - Unwelcome propositions, requests for dates, or love letters;

- Profanity, obscenity, slander, or libel;
- Ethnic, religious, or racial slurs;
- Political beliefs or commentary;
- Terrorism, terrorist activities, inciting or condoning violence or vandalism; and
- Any other activity considered illegal in the country of origin/receipt.

It is recognized that websites which display material of a pornographic or offensive nature, or which contain malware designed to infect and harm your computer, may be accidentally accessed from time to time. Should this happen and you become concerned for the integrity of your computer and/or network access, inform the IT officer immediately and discontinue use of your system, closing down all shared drives. Remedial action will be taken as necessary to protect your computer and EAS' IT systems from further infection.

The forwarding of chain-letters is strictly forbidden – this includes those purporting to be for Charity or other good causes as well as those promising wealth or other personal gain. Likewise, no non-business related messages of any kind should be sent to multiple external destinations as this is considered 'spamming', an illegal activity in many countries.

Email should not be used to send large attached files, and a strict limit of 25Mb has been applied by the mailbox host. In addition, many email systems will not accept large files which may be returned and result in the overloading of the EAS email system. The Academy has active email security protocols to screen for malicious content; even so, employees are recommended to exercise caution when opening all attachments, particularly if the file extension is not recognized.

The Ethiopian Academy of Sciences reserves the right to monitor employees' email and internet usage, including intercepting emails before they are read, and accessing personal internet browser history for the purpose of investigating unauthorized use of the EAS' telecommunication system, preventing or detecting crime, or ascertaining compliance with this Policy. This will include personal emails where appropriate.

All monitoring will be authorized by the Executive Director of EAS. Any information obtained during the course of monitoring will be kept strictly confidential and will be used only for the purpose for which the monitoring has taken place.

5. CONFIDENTIALITY AND INTELLECTUAL PROPERTY

EAS employees are strictly forbidden to make any copy, abstract, summary or précis of the whole or part of any document constituting the intellectual property of the company, sub-contractor, partners, or its clients – except where expressly authorized so to do or in the proper performance of their duties.

Employees are required to promptly disclose to the Academy, and keep confidential, all inventions, copyright work, designs or technical know-how conceived or made by them alone or with others in the course of their employment. They must hold all such intellectual property in trust for the Academy, sub-contractor, partners and clients as necessary, and will vest intellectual property fully in EAS and/or secure patent or other appropriate forms of protection of the same.

Employees at all times – both during their employment with EAS and after its termination – must keep confidential, and shall not at any time turn to their own account, make personal use of, divulge, make known to anyone or enable anyone to become aware of (other than those who are employed by EAS and authorized to receive the same) any information relating in any way to:-

- Suppliers, potential suppliers, customers and potential customers;
- Techniques, engineering and procedural documentation of the Academy;
- The details of any business, financial or other arrangements transacted with persons, firms or statutory bodies by EAS on behalf of itself or any of its clients; and
- Policy documents or any other internal restricted document, including personal information relating to EAS employees or its partner/clients.

6. DATA PROTECTION

EAS will protect all data in its care and can only do this with the assistance of staff and partners. All staff and partners are required to keep EAS informed of all material changes in your circumstances.

This policy makes available to you full details of your entitlements and responsibilities to make this happen.

As an employee you must acknowledge and consent to the following:

- That EAS maintains and holds electronic records relating to you and all our employees principally to enable us to effectively record and administer our HR function and processes such as pay and benefits;
- That it may be necessary from time to time, to pass personal data to other organizations, partners and clients for the following purposes:
    - Sharing knowledge, information, products and ideas;
    - Marketing initiatives and Business Development activities;
    - Administrative purposes; and
    - If required to do so, by a government body.

You may make a written request to the Executive Director if you wish to see records held by EAS about you. Where we are able to provide such details to you, it will be given.

7. DISCIPLINARY PROCEDURES

Failure to comply with the provisions outlined in the above sections will lead to appropriate reprimand. Any action judged to constitute gross misconduct may lead to summary dismissal at the discretion of the Executive Director.