Internet & Electronic Communication: Acceptable Use Policy

IGDP_P9 VERSION 1.00

ALADDIN MIDDLE EAST LTD – TURKEY ANKARA BRANCH OFFICE

Internet & Electronic Communication: Acceptable Use Policy

1. INTRODUCTION

The Aladdin Middle East Limited – Turkey Branch Office("Company"), has a responsibility as a registered private entity to ensure that all corporate resources are utilized correctly and not misused or abused. This includes electronic services such as Email and Internet access. The Company provides its staff members, staffs and authorized visitors (collectively known as 'Users') with access to information and communication technologies to enhance and support their research, administrative and service functions.

All Users should be aware of this policy and associated procedures, responsibilities and legal obligations. All Users are required to comply with this policy and are bound by law to observe applicable legislation. Like all Company assets and services, the information and communication technologies in all their various forms, should be used in an efficient, lawful and ethical manner.

The Company has a legitimate right to capture and inspect any data stored or transmitted on the AME Turkey's facilities (regardless of data ownership) when investigating system problems or potential security violations; and to maintain system security and integrity; and to prevent, detect or minimize unacceptable behavior on that facility. Such data will not be released to persons within or outside of the Company, except in response to the circumstances described in the AME Turkey's Directive on Inspection of Electronic Communications and Data.

2. PURPOSE AND SCOPE

The purpose of this policy is to determine the procedures and principles to be observed by staff members while using Company's electronic communication purposes. This document and the associated procedures apply to all staff members and authorized visitors of the Company. This policy comprises three sections:

- Internet use policy
- Email use policy
- Communication between staff members.

s policy should also be read in conjunction with the following policies:

- Staff code of conduct
- Data Protection and Processing policy

- Information Security Policy

For the purposes of this policy 'email' is taken to include all forms of electronic communication, including, for example, webmail, instant message and web forums. Use of the Company's internet and email facilities, whether onsite, using wireless or via remote desktop acceptance will imply acceptance of the conditions of use laid down in this policy.

3. Internet use policy

3.1. **Purpose of Service and User Responsibilities**:

The Internet Service is provided primarily for Company's business activities. It is acceptable for individuals to utilize this resource for personal use provided that usage is reasonable, sensible and managed by each employee responsibly, especially in respect of the time spent when accessing the Internet for personal business.

3.2.**Monitoring**:

3.2.1. Staff using the internet at Company on the company systems do not have a right to confidentiality or privacy. The AME Turkey has a robust system for monitoring Internet searches and blocking websites and links which are inappropriate for staff and visitors to use while on company premises. The system is managed by the IT department and monitored by the heads of Departments and Board of Directors. To ensure that flaws and gaps in the system do not arise, the firewall is challenged on a termly basis by members of the safeguarding team

3.2.2. The monitoring software tracks the use of the Company's internet and the Head of IT Department and the Chief of Departments monitor and review network logs maintained in order to ensure compliance with corporate policies. This includes the remote scanning of computer monitors, the checking of files and emails and the analysis of internet sites visited. This software records details of every web site visited, along with the relevant user name and date/time details, and produces regular reports for monitoring purposes. Misuse, or visits to sites of a dubious nature, will automatically be reported and dealt with in line with normal disciplinary procedures. In using the AME network, users agree to such monitoring and reviewing of internet access

3.3.Private subscriptions or recreational use:

Users may not make their own provision for accessing the Internet from Company premises using resources other than those which have been provided through the Company. Specifically, employees may not take out private subscriptions to internet service providers and/or online services and use them on Company computer equipment unless this has been agreed in writing with the Head of IT Department. Employees may not use the Internet for inappropriate recreational use, such as games or gambling.

3.4.Prohibited Behaviors that May Bring the Company into Disrepute:

Users may not use the Internet in such a manner which might be prejudicial to the interests of the Company or which may bring it or associated parties, such as Partners or business associates, into disrepute. An example of this might be subscribing to a web site that contains illicit or illegal material or by downloading and using a third party's copyrighted images unless explicitly permitted by the copyright owner.

3.5. Downloading software:

The downloading of software is strictly forbidden, in accordance with Company policy, in order to minimize virus risks and to help ensure the network does not contain unlicensed software. This includes the downloading of games and screen saver software. Where there is an business need to make an exception to this policy please contact IT Department for guidance.

3.6. **Unlawful use:**

An employee may not knowingly use the Internet for any activity which is unlawful under the laws of Turkey. Employees may not use the Internet to locate, download, access or otherwise investigate material of a nature which may cause offence to other employees on grounds of gender, race, religious belief, sexual orientation, disability or otherwise.

3.7.**Shopping online:**

It is permissible to shop on line on occasions where employees are working long hours. It should however be noted that you should avoid downloading the retailer's software. Ame Turkey cannot be held responsible for the security of any financial transactions, although the system is no less secure than a home based PC. Shopping should be restricted to items which do not fall into the categories described in the 'prohibited activities' section, especially items that are "obscene, pornographic or of an intimate nature".

3.8.Security:

It is essential that you do not divulge your user name or password to anyone else, as you alone are responsible for access and security of your Network Area. Computers should be “locked” when unattended (by pressing Ctrl-Alt-L or Ctrl-Alt-Del). Should a personal device, which has been used to access corporate emails or data, be lost or stolen, the loss or theft must be reported to the Head of IT Department. Staff should ensure they are familiar with the Information Security Policy which gives detailed guidance on password protection and security

3.9.Prohibited Activities:

Prohibited uses of the Internet at all times include, but are not limited to, viewing, storing, distributing or otherwise using the facilities for the following:

- Illegal activities (including any violation of copyright laws)

- Threatening, abusive, harassing or discriminatory behavior
- Slanderous or defamatory purposes
- Obscene, suggestive or intimate messages or offensive graphical images or pornographic materials
- Activities that will incur a cost to the Company without prior proper authorization
- Chain letters through Email
- Private, commercial activities for profit making purposes
- Malicious damage
- . Inappropriate political, religious or recreational use

3.10. **Safeguarding**:

Any employee inadvertently exposed to images depicting the abuse of children whilst using the AME Turkey network must report the location of those images to the Company via the Head of IT Department, and must not make copies or disseminate such images.

3.11. Security and Access Considerations:

3.11.1. The Company has in place provision to protect itself and its computer systems, web sites and employees from external or internal security threats, real or potential. Examples of security measures which may be deployed include but are not limited to the following examples: firewalls and proxy servers to block outgoing/incoming Internet traffic; anti-virus software; access control software (typically restricts access to specific web sites); measures to prevent the downloading of software; restriction of potentially harmful software scripting or elements.

3.11.2. The Company currently subscribes to a filtered service from its internet provider. Whilst access to the internet is generally not further restricted by the AME Turkey for staff who are provided with the internet, the Company may block access to known sites which contain or are believed to contain illegal, pornographic or otherwise offensive material (for example sexually explicit; web-based chat; criminal skills & hacking; drugs, alcohol & tobacco; gambling & games; personals & dating; Usenet news; violence & weapons).

3.11.3. Users of the Internet should be aware that many web-sites record details (sometimes surreptitiously) of who visits them, and that access to the internet could leave a record of activity on the PC itself.

3.11.4. The Company reserves the right to withdraw the Internet without notice in the event of a suspected security violation requiring immediate investigation or where it otherwise believes that the AME Turkey Network and/or computer systems are at risk.

4. EMAIL POLICY & GUIDELINES

4.1. The purpose of this policy is to ensure the proper use of the email system. Everyone who has access to email is responsible for adhering to this policy, that email is used responsibly, effectively and for approved purposes only. This policy is intended to provide guidance to staff on communication by email particularly for internal correspondence. For example, excessive personal use of the Company email system is not acceptable.

4.2. Status of email communication:

Staff should always bear in mind when communicating by email that in law, an email is a document that may be disclosed in legal proceedings. All email messages sent or received within the AME email network are the property of the Company and users should not expect personal privacy when using the email system. The Head of IT Department is authorized to monitor email messages and network logs so as to ensure compliance with Company policies. All users agree to such monitoring and reviewing of emails.

4.3. **Personal emails :**

Whilst users of the email system may send and receive personal messages internally and externally, this must not interfere with the user's work or the work of another user or be detrimental to the user's duties and responsibilities. Use of email for personal matters must not be excessive. The email system should not be used for private commercial activities or to disclose, distribute or otherwise disseminate confidential information belonging to the Company or corporation

4.4. Content:

The content of all emails must not contain offence or harassment of a sexual, racial or religious nature, whether explicit or implicit, and must be written using only vocabulary acceptable for professional communication in the workplace.

4.5. Confidentiality:

Confidentiality is not guaranteed. Any message sent or received may be accessed by colleagues other than the individual to whom it is sent, whether by accident (e.g. a computer left logged on) or design (e.g. an email may need to be opened to diagnose connectivity problems). Messages cannot therefore be regarded as private or confidential. Personal messages should be written remembering this possibility for third parties to review the content. In the case of external email, there is no inherent security at all and such messages can potentially be intercepted and read by third parties without our knowledge. Messages of particular confidentiality or sensitivity should be sent by an alternative medium and using the processes set out in the Information Security Policy and Directive on Principles and Code of Conduct for Secure Data Transfers.

4.6. **File Attachments**:

To avoid the possibility of any inappropriate material being copied down onto the Company network, and to reduce the risk of virus infections, file attachments to email messages, (whether they are images, text or spreadsheets), may only ever be downloaded if they come from trusted sources (that is, from a correspondent whom you know) and are not of an inappropriate nature. Under no circumstances may attached executable program files be opened. Instead, such messages should be forwarded to the IT Support Team for advice. Executable files include those which end in the following suffixes: .EXE, .COM, VBS .SCR, game.exe, and screen.scr.

4.7. Chain Letters/Jokes:

Chain letters and jokes are not an appropriate use of Company time and resources and may unwittingly cause offence. If received they should not be forwarded and should be deleted from the network.

4.8. Virus Hoaxes/Warnings:

Messages from external parties, which warn of viruses, must not be distributed or passed on. In practice most of these messages are simple hoaxes. However, in all cases they should be forwarded to IT Support for advice and then deleted from your Inbox.

4.9. Use of external email systems for corporate business:

All email correspondence pertaining to Company business must be sent using the AME email network. It is not permitted to use private email systems and accounts (e.g. AOL, Hotmail, ISPs and others not cited) for corporate business. Staff who need to access the AME network when off site should contact the IT helpdesk for advice on remote working.

4.10. Guidelines for sending email:

4.10.1. Addressing email:

a) Check Carefully: Careful proofreading of addressees before sending will avoid common addressing errors, e.g. the incorrect use of 'Reply All' vs. 'Reply' icons.

b) Principal Addressee: As well as entering the principal addressee into the address box on the email header, the message should have a text heading "Message to xxxx" or be headed, "Dear xxxx" to make it clear who the recipient is and who is expected to respond. CCs would then only be copied for information. The person you put in CC when sending the mail is the person you want to give information about that job, who is not the direct addressee of the mail. If you put someone on CC in the mail, this assignment can be seen by anyone who receives the mail. In other words, when you put someone on CC in your e-mail, you predict that person will have information about this e-mail.

c) CC Lists: As anyone would consider carefully the appropriate addressee and copy list for a memo or letter, so the same care should be given to addressing an email. In particular multiple CCs of an Email should be avoided. Analyze carefully whether there is real and effective purpose to either copying the information or soliciting input from each and every person copied. Do not use CC lists for emails to groups of parents; such communications should be sent through the portal. You must take special care to respect the privacy of recipients such as parents by not using lists of email addresses in the 'To' or 'CC' boxes.

d) BCC lists: Written e-mail is sent to the e-mail addresses written in this field. "To" and "CC" recipients cannot see the e-mail addresses entered in this field. Only the sender and the recipient of the e-mail address written in this field can see this field. However, people entered in the "BCC" field can see who are the recipients in "To" and "CC". Whilst there are appropriate uses of BCC with emails sent to third parties, its use can be a very bad idea for internal messages when knowledge of the sharing of communications between colleagues is withheld from one or more parties, since emails can be forwarded and the secrecy subsequently unmasked. Issues of trust between colleagues can arise when messages assumed by some to be private are shared in this manner, and so blind copying between colleagues is generally to be avoided.

e) Mass emailing: Mass-mailed messages may only be sent for Company purposes and may not be used to broadcast personal messages of any kind. Further, services/goods of third parties may not be advertised or recommended via email.

f) Sending Document/Spreadsheet Attachments: Email may be used to distribute memos or other document attachments. However, large file attachments, defined as greater than 10 MB, may not be distributed (in general most documents and spreadsheets are well within this limit). IT Support can provide advice on the distribution of large files e.g. by using shared areas.

5. Personal Data protection:

Any communication that contains personal data will be governed by current data protection legislation. Make sure you are familiar with the Data Protection and Processing Policy and the Information Security Policy both of which contain detailed guidance on how to keep personal data secure.