actionaid

GLOBAL IT POLICIES AND STANDARDS

September 2009

Table of Contents

0. Summary

The objective of the IT Policies and Guidelines and Standards is to foster an environment that will secure information within the ActionAid community from threats against privacy, productivity and reputation. In designing the policies, care has been taken to ensure that they are consistent with ActionAid guidelines articulated in the Open Information Policy, in particular:

"ActionAid International believes that timely free flow of information in accessible language, form and format is essential for ensuring accountability, learning, trust and good performance."

These policies and standards create an effective, professional, legal, ethical and equitable IT usage environment across ActionAid world-wide.

Owned by the International Director, O&GD and the International Head of IT, these policies will be implemented by the Country Directors and office managers and the respective IT Coordinator/Manager.

These policies are binding on all ActionAid offices, including all incoming affiliates and all staff, contractors or consultants who make use of ActionAid IT resources.

These policies and standards are a minimum non-negotiable set to be implemented in all countries, regional offices and international offices.

These policies and standards will be reviewed annually.

ActionAid International and local IT teams will have the authority to enforce these policies through appropriate technology, and with our audit teams to audit and check compliance (manually or through technology) of all ActionAid's IT resources.

1. Introduction

1.1 What is this?

Our structure, where independently governed country organizations come together across 45 or more countries in Africa, Asia, Americas and Europe to form a single functioning organization is unique in the NGO world. Our countries are linked by a common vision, common mission and values, common strategies and policies, common themes and campaigns and a single brand.

In governance, though, we are not a unitary organization.

In this scenario, the vital element that keeps us linked is information. It is the role of the IT/IS departments of ActionAid to ensure that we have the right infrastructure and systems to keep this information flowing. The functioning of IT/IS activities, like our other functions and themes, are split among the countries and international. This being so, it is important that we have a common set of policies for IT usage across the organisation.

Our Open Information Policy states that “ActionAid International believes that timely free flow of information in accessible language, form and format is essential for ensuring accountability, learning, trust and good performance.”

Through these policies and standards we seek to create an effective, professional, legal, ethical and equitable IT usage environment across ActionAid world-wide.

These policies draw from existing good IT policy practices from within the organisation and from organisations outside ActionAid such as Nethope members and our vendors. We have also consulted other worthy external guidelines and industry standards.

These policies and standards are owned by the International Director, O&GD and the International Head of IT and are to be approved by the International Directors of ActionAid International. These policies will be implemented by the Country Directors and office managers and the respective IT Coordinator/Manager.

1.2 Scope of these policies

These policies are binding on all ActionAid 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 ActionAid IT resources located off ActionAid premises. e.g. laptops used by staff at home or when travelling. Appropriate policies are also binding on the usage of ActionAid information and systems on non-ActionAid resources.

These policies and standards should be regarded as a minimum non-negotiable set to be implemented in all countries, regional offices and international offices. CPs and units are free to adopt local policies and standards in areas where the Global IT Policy does not prescribe anything or does not prescribe policies that are rigorous enough to meet that country’s requirements. It should be noted that any local legal or regulatory requirements that are stricter than these policies will supersede these policies.

Countries running NK and other applications should follow any special guidelines and standards set for these applications.

1.3. About this document

This document is in two sections. The first includes general user policies and is aimed at users and IT technical staff. The second is technical and is aimed at IT technical staff. The appendices contain guidelines to prevent social engineering attacks, our standards, details of devices that can be connected to our network and special requirements for countries running our sponsorship management system, NK.

1.4 Review of these policies

These policies and standards will be reviewed annually and a new version of the document will be issued. Revised versions will also be issued if there are any significant changes in technologies or environment that warrant immediate change in the way we work.

1.5 Abbreviations used

Cat	Category
CDs	Compact Disks
DAT	Digital Audio Tape
DLT	Digital Linear Tape
DMZ	DeMilitarized Zone
DVD	Digital Video Disk
fpt	Fighting Poverty Together
GB	Gigabyte
HP	Hewlett Packard
HRMIS	Human Resource Management Information System
ID	Identity
IS	Information Systems
ISA	Microsoft Internet Security and Acceleration Server
IT	Information Technology
LAN	Local Area Network
MB	Megabyte
MSDE	Microsoft SQL Server Desktop Engine
MSN	Microsoft Network
NIC	Network Interface Card
NK	Nkonsonkonson - Sponsorship Management System
PIX	Private Internet eXchange
PSTN	Public Switch Telephone Network
RAID	Redundant Array of Inexpensive Disks
S/W	Software
SD	Secure Digital
SQL	Structured Query Language
USB	Universal Serial Bus
VM	Virtual Machine
VoIP	Voice over Internet Protocol

2. Compliance to these policies

2.1 Compliance and monitoring of these policies

ActionAid International and local IT teams will have the authority to enforce these policies through appropriate technology, and to audit and check compliance (manually or through technology) of all ActionAid's IT resources. Compliance to policies will also be monitored in the usual way through audits (IT and financial audits).

2.2 Action in the event of a breach of these policies

Where there is assessed to be a serious breach of these policies, ActionAid 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 and ActionAid's IT functions.

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. Staff using ActionAid's IT systems to store or pass on child pornography, or any other material that could cause offence or injury, will face serious disciplinary action and possible dismissal - whether or not they are prosecuted or convicted.
- 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 defence.

3. General (User) policies

3.1 The ActionAid Domain

All ActionAid IT resources operate within a single “fpt” domain. When a user signs into this domain, he/she gains access to all ActionAid IT systems (including e-mail, intranet, NK etc.) according to their user privileges. [This single sign-on process is still being rolled out in many CPs. Until it is implemented globally, the local IT coordinator will implement the required access. Single sign-on access to systems such as NK will be implemented in due course].

3.2 User account and e-mail id creation and deletion

All ActionAid staff, long-term contractors, and long-term and full-time consultants are provided with a user account within the “fpt” domain, as well as an e-mail ID [of the form <first-name>. <last-name>@actionaid.org. The display name will be of the form <first-name> <last-name> e.g. Email ID: marco.deponte@actionaid.org; Display name: Marco DePonte. Any exception to this needs to be approved by the O&GD ID and/or by the Head of IT/IS.

Email IDs of any other format are in the process of being discontinued and all servers will be restricted from receiving emails any other form directly.

Process:

- The local HR member of staff creates an entry for all staff, contractors and consultants in the global HRMIS (Human Resources Management Information System) which automatically creates the user IDs and e-mail IDs in the domain.

- A user who is indicated in the HRMIS system to have left ActionAid is automatically prevented from accessing the domain or e-mails. Any account that is inactive for more than a month is reported to HR/IT and reviewed for action.

IT staff do not have the authority or responsibility to set up or delete user or email IDs. This authority/responsibility is vested with HR.

Other user rights like adding users to appropriate distribution list, assigning home directories etc. will be done by IT units in consultation with line managers and HR managers.

3.3 Responsibility for assigned resources

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

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

3.4 Ownership of ActionAid Information

All information contained in the ActionAid 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 ID, O&GD.

It required that anybody leaving the organization should properly handover all AA 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.

In some countries internal email is considered a form of public communication and can be subpoenaed, for instance as evidence of libel in a defamation lawsuit.

3.5 ActionAid standard Desktop/laptop build

All ActionAid 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 IT centre 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. For these standards see appendix on standards.

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 can't be repaired.

3.6 Resources Management and License policy

All purchase of hardware or software should be done as per the local purchase policy with approval from International or CP IT. The IT department will be best placed to ensure the best rates and to ensure compliance with our policies and legal requirements. Any transfer of resources from one person to another should be with the approval of IT; otherwise there may be license infringement.

3.7 Systems development and procurement policy

Any system development or procurement of systems like websites, databases and other applications must be approved by local or international IT as part of the planning process.

3.8 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 local IT unit.

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.

3.9 Network access policy

Access to the ActionAid information network is permitted only with devices authorized and set up by International or CP IT. 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 ActionAid resources in any way except on permission from the ID, O&GD.

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

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

3.10 Backup policy

All business critical data will be backed up on a regular basis as per the ActionAid backup procedure. The local IT group will enter into an agreement with users for this purpose.

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

3.11 E-mail policy

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

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

No external e-mail addresses should be included in our distribution groups unless approved by the ID, O&GD.

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 ActionAid 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 ActionAid 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-ActionAid 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 ActionAid 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 ActionAid management

3.12 Personal use

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

It is not permitted to use ActionAid's 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. [Buying/downloading music and such other are permitted where there is a management request to do as part of ActionAid promotions where ActionAid gets revenue. This is permitted only where the bandwidths are good and normal office work is not affected.]

3.13 Quotas and limits

All e-mail boxes have quota limits (500 MB) 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 officers 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.

There are limits on the size of an email that can be received and transmitted. No email greater that 2 Mbytes can be accepted for delivery to an AA account. Please use the Hive for exchanging of information over this limit. No email greater than 10 Mbytes can be accepted for transmission by the email servers to an outside account.

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.

3.14 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 ActionAid. These vary significantly by country, thus all users are urged to seek the advice of their line manager. These will usually include:

Intellectual property
Obscenity
Defamation
Data protection

Discrimination
Harassment

3.15 External Website Hosting

All external pointing websites should be hosted at our central data centre. This will ensure disaster recovery and security and also save us money in terms of hosting fees.

3.16 Internet (browsing) policy

All internet access should be through the configuration set up by the local 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 ID, O&GD.

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

The ActionAid network should not be used to conduct personal businesses (including blogging) [except as mentioned in section 3.12]

No software (freeware, shareware or paid) should be downloaded or installed on ActionAid 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 [except for those required by our applications]. If there is a business need to download/install some software please check with your IT department first.

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 team.

3.17 Home internet connection policy

ActionAid will not provide a home internet connection except for those people who have been allowed to work from home for some reasons. Any internet connection at home will require authorization from proper authorities.

3.18 Incident Reporting and Management policy

All incidents and problems with user systems should be reported through our standard incident reporting system - Footprints. Your local IT person will only take cognizance of problems reported through Footprints.

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

Disruption of ActionAid services
Loss of sensitive information
Violation of ActionAid Security / Integrity policies
Unauthorized access to information
Unauthorized modification of information / data
Identity thefts
Loss of ActionAid 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.

3.19 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.

3.20 Policy on use of Voice over IP (VoIP)

Where technologically possible, and where legally permitted, it is ActionAid's policy that we use VoIP phones (like Teleworker), Skype, MSN etc. to make official calls so that we can bring down our communication costs. Some of these products also allow video-conferencing and these can be used to reduce travel costs. Ids of Skype, MSN etc. should be made available to our Global Address List/Hive Personal Profiles so that contact through these becomes easy.

3.21 Policy on teleconferences

Where possible, teleconferences should use the free ActionAid conference bridge rather than more expensive commercial services.

3.22 Security of Information Technology Resources

Every information technology (IT) device connected to the ActionAid network must have at least one individual who is responsible for the security of that device. The organisation 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.

Violations of this policy include

- intentionally maintaining insecure passwords on IT devices attached to the network
- intentionally attaching misconfigured IT devices to the network
- intentionally compromising an IT device attached to the network or using an application or computing system with a known compromise.
- Intentionally transmitting any computer virus or other form of malicious software
- Intentionally accessing or exploiting resources for which you do not have authorization
- Intentionally leaving a computer unattended for a significant period of time thereby increasing the risk of theft.
- Laptops and desktops must be password protected so that data (especially on HR, Finance etc systems) cannot be accessed when the staff member is away from their desks, even if for a short period of time.
- Intentionally destroying or damaging (or allowing others to destroy or damage) ActionAid property

3.23 Administrative Rights of IT Officers/Managers

IT Officers/Managers of CPs and units and locations are not allowed to access content information (e-mails, documents, workgroups etc.) on user machines except on authority from the user of this information or from the CD (for all CP users) or ID, O&GD (for all international users) and after complying with local laws.

However, the IT Officer/Manager of a location or CP 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, trouble-shooting 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 ActionAid / 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 organisation.

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 ActionAid laptops, desktops, servers, mobile phones etc. must operate with legal, licensed software. All offices and countries should follow this strictly. The Country 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 ActionAid resources.

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

Most of the standard software licenses should be procured centrally and distributed to the countries. (See standards for details)

4.3 Virus protection policy

All workstations and other IT resources (servers, gateways etc.) whether connected to the ActionAid network or standalone, must use the most current approved standard virus protection software and configuration [see appendix on standards for the approved version]. The virus protection software must not be disabled, bypassed or have its settings altered.

4.4 Network access policy

Access to the ActionAid information network is permitted only with devices authorized by these policies. Any access to the network bypassing the official gateways, firewall, DMZ, tunnels etc. are forbidden.

CP IT should ensure the following:

- All remote access/vpn access should be setup in consultation with International IT to ensure proper configuration and security settings. All remote access to applications (like SUN) other than web-based applications or client-server based applications should be through Citrix.
- IP addresses (both external and internal) should be setup only in consultation with International IT so that addressing standards can be followed.
- Firewall ports are opened only in consultation with International IT. Opening up of firewall ports not sanctioned by International IT will compromise the security of all our IT systems. This will be treated as a breach of discipline.

4.5 Internet policy

All internet access by users should be configured to be through “fpt” domain through the proxy set up as per our policy and standard.

Ensure web browser security settings are high or set to disallow unsigned ActiveX and components.

All web browsers should be set up to block pop-ups. Exceptions can be made for ActionAid sites.

4.6 System Setup/Standards Policy

All ActionAid systems will be procured, setup, maintained and upgraded as per the standards mentioned in the appendices.

These systems include (but are not limited to) desktops, laptops, mobile phones, communication links, software, accessories, servers and backups.

Appendix 1 (Guidelines to prevent social engineering attacks)

Social engineering activities could be carried out by people and through the use of computers. A skilled Social Engineer can exploit “human willingness to help” by circumventing protection mechanisms.

Please follow the following guidelines

- Never disclose “sensitive” business and personal information to strangers or suspicious people.
- Question the identity of the people whom you do not recognize before revealing any personal/official information.
- Be cautious with what kind of information you hand out.
- Exercise extreme caution while providing personal information on any portals/websites on the internet including your name, contact numbers, dates of birth addresses, email addresses etc.
- Exercise due diligence related to the reputation of the business portal in general.
- Never write down your passwords, credit card details and other sensitive information.
- Never disclose passwords and other sensitive information over phone.
- Always think twice before disclosing any “sensitive information” in stressed situations so that you don t make any hasty decisions.
- Do not act in a certain way only just because you are told that somebody else has done it that way.
- Do not trust people only because they seem or sound nice over phone, especially while disclosing information.
- Always verify the authenticity of the content received in emails from outside domains before taking action, especially for emails received from free email domains.(e.g: Spam emails, Phishing attacks).
- Do not open/ forward any suspicious email with attachments (e.g: virus infected) to anybody.
- Keep your computers updated with the latest antivirus software and updates and anti spy ware.
- Destroy your expired credit cards, financial statements, ATM cards, and documents containing critical information and then dispose carefully in trash.
- Keep your postal mailing address updated with all financial agencies – Banks, Credit card companies, Insurance companies etc
- Never reveal banking PIN numbers, credit card numbers (with expiry dates and CVV numbers), Social Security numbers to strangers for convenience, during normal or even disaster situations.
- Do not fall victim to “phishing” attacks through email. Typical “ phishing ” attack would entice you to open an email and click an embedded URL in that email that pretends to seek personal banking information redirecting you to a fraudulent/malicious website, without your realization.
- No reputed banks seek personal banking information like account numbers,

PIN numbers, ATM transaction details, credit card numbers etc through email. (ActionAid IT will never seek password and such sensitive information through mail)

- Do not openly discuss ActionAid sensitive information in public places. Be careful about eavesdropping and shoulder surfing especially while you are traveling with your laptop.

Appendix 2 (Standards)

No.	Type	Remark	Standard
1	Servers	All servers should conform to Generation 5 (minimum G5) servers with Dual Xeon processors. This allows for full Virtualization platforms to be fully utilized. Domain Controller (VM) File Server (VM) Application Server (VM) Accelera (VM)	Xeon Generation 5 (minimum G5) Dual Xeon min 3ghz 8GB RAM (min for ESXi) 300GBx3 (SAS 10K) DVD ROM RAID X64 compatible h/w Tape Unit (DAT,DLT,Utrium)
2	Workstations	Desktops will be branded systems and not cloned or locally assembled computers. The brands recommended will be HP, DELL and IBM Computers	Intel Duo core - 3.0 GHZ Processor - 1GB RAM - 160GB Hard Disk - 10/100 NIC CARD - DVD /CD writer (Combo) - 17”TFT Screen - Windows XP Prof or Windows vista pre-loaded Mouse Headset (NOT Speakers) Filter (Screen) Power Backup for all PC
3	Laptops	Toshiba laptops are highly recommended for the staff who do frequent travels but other branded models (DELL, HP and IBM) could be purchased for staff who do not have heavy travel schedule	Intel Core 2 Duo - 2.2 GHZ Processor - 2GB RAM - 160GB Hard Disk - 10/100 NIC CARD - DVD /CD writer (Combo) - 14" high resolution vga Screen, - Windows XP Prof or Windows vista pre-loaded. Office 2007/2003 and macfee anti-virus installed from AAI licensing Mouse Headset (NOT Speakers) Filter (Screen) Power Backup for all PC Webcam enabled

4	Printers	Recommended printers will be HP printers and these will range from low range HP P1100 to heavy duty network printers, Panasonic printers could be used where faxing and e-mail network printing is required at the time	HP printers from low range HP P1100 to HP P4500 series. Heavy duty fax/e-mail printers for Panasonic can also be used where this is necessary
5	Scanners	HP is the recommended brand of Scanners	Low range HP scanners to Heavy duty HP scanners with automatic feed scanner facilities
6	Digital cameras	Canon, Sony and other high pixel branded systems are recommended	Above 3 m pixel resolution
7	Instant Messaging and Communications		MSN Messenger VOIP, Skype
8	Telephony Equipment	All CP's should promote use of IP telephone (Teleworkers, Skype phones forms part of these equipments)	Should allow integration with VOIP and PSTN in a box
9	VoIP telephones		Teleworker
10	Mobile phones		Nokia phones for voice and Windows mobile/Blackberry for email. All international travelers should use Blackberry phones for email under the UK O2 blackberry deal.
11	Multimedia Kits	Consult International IT	
12	Cabling	Cat5E or Cat6 cable is the recommended cabling for all offices	Full Structured Cabling or wireless
13	Connectivity Related hardware		LAN cards or in-built dial-up modems as part of Workstation specs
14	Link	Countries should ensure minimum connectivity is attained for smooth operations of NK, E-mail flow , intranent and webiste access.	1 MB (no contention)
15	Connectivity Kits (Emergencies etc.)		Edge card, GPRS card, RBGan, NRK , satellite phones
16	Operating Systems		Windows Vista, XP business edition and SP2 for desktops and laptops and windows 2003 server

17	Backup hardware and Software		Internal 36/72GB tape drives and symantec Backup software is the recommended minimum standards for all servers
18	Networking Systems		Switches, Cisco Pix firewall
19	Standard Office Productivity Tools (Word processor, Spreadsheet, Presentations, email clients)		Office 2003/2007 suites are the recommended applications for all desktops and laptops
20	Email Software		Exchange 2003/2007 is the recommended e-mail systems across the board
21	Security s/w		ISA Server,
22	Database Management s/w		SQL, My SQL, MSDE
23	Development Environments	Consult International IT	
24	Other Application S/w	Consult International IT	VMware, A-Celera