Information Technology (IT) Policy

Aiming Change for Tomorrow

Table of Contents

1. Information Technology (IT) Policy

In fulfilling needs of the Information Communication Technologies (ICTs), ACT International uses a wide variety of Information Technologies (IT) to assist ACT International's employees in serving the public. The Information Technology Policy provides employees with guidelines for the proper use of the Department's computer hardware and software, e-mail, and Internet service.

These guidelines are designed to alert ACT International staff of their responsibilities. It is the responsibility of each ACT International staff member to:

- Use the ACT International computer systems properly.
- Understand and follow the IT policies in this document.
- Protect the integrity of the systems by treating equipment with care and respecting IT security measures.
- Contact IT department when a problem occurs.

It is the obligation of ACT International's Information Technology staff to:

- Educate staff about any IT questions or concerns.
- Follow a process that addresses IT needs in a timely manner.
- Provide staff with working equipment that helps to meet their needs.
- Respect staff's privacy for all information they store in the IT systems.
- Respond to IT related employee's queries in a timely manner.

2. User Responsibilities

2.1 Requesting service for computer problems

- **Emergencies** – Contact IT Department, explain your problem. The IT Department shall respond to the queries immediately. The IT Help Desk working hours are Monday through Friday, 9:00 AM to 5:00 PM.

- **Non-emergencies** – Submit a written IT Service Requisition (ITSR) form. This form should have the appropriate supervisor and/or CEO approval prior to submission to the IT Department. Upon receipt of the form, IT staff will notify requestor within 24 hours of receipt of their ITSR.

2.2 Hardware (Including hardware issued and used offsite)

- **Moving Computers** – ACT International staff are NOT allowed to relocate, move, slide, or reposition any computer equipment.

- **Installing and Removing Hardware** - Users are not authorized to attach/detach or install/uninstall any computer components without authorization from their Managers and involvement of IT staff. This includes keyboard, mouse, printer, modem, monitor, internal boards, or other components. The IT Department is responsible for assigning computer components to specific computers.

- **Storing Data** – All data must be stored on designated servers, not on local hard drives when that option exists. Data on the servers are backed-up weekly, thus

protecting the user from loss of data should a computer malfunction. Data storage space on the servers is limited. Therefore, users with the need for an extraordinary amount of data storage should notify their Managers who will then work with the IT staff to meet the user's needs. If portable media containing electronic protected health information is generated, the user must take the responsibility to store the media in a secured, locked location and dispose of the media per the media disposal guidelines when no longer needed.

- **Acquiring and Disposing of Computer Hardware** – The purchase of any computer hardware or the disposal of old computer hardware is done only with the approval of the CEO and involvement of IT staff. Please check with IT staff on proper disposal of removable media (CDs or floppy disks…) containing confidential information.

2.3 Software

- **Installing Software** – ACT International staff are NOT authorized to install any software, programs or batch files on ACT International computer equipment. It is the responsibility of the IT Department to complete these tasks. Users must submit an ITSR to have any programs installed on any ACT International equipment by the IT staff.

- **Unauthorized Downloadable Software** – The use of unauthorized downloadable software is prohibited. Downloadable software such as freeware, shareware, program demos, surveys, advertising, training, Internet browsers, copyrighted data, fonts, personal digital images, graphics and personal photos should not be downloaded without prior approval by the concern Managers and the involvement of the IT staff

- **ACT International Developed Software** – Any software or data developed at ACT International is the sole and exclusive property of ACT International.

- **Software Licensing Compliance** –Violation of any software licensing agreement, copyright, or other intellectual property rights of third parties is strictly prohibited. This includes, but is not limited to, computer software/data or related manuals and materials. Contact the IT Department for more information about software licensing agreements.

2.4 Internet and Email

- **Internet and E-mail Usage** – The ACT International computer system, Internet and E-mail system are to be used for ACT International purposes only; however, the Organization realizes that occasionally it is necessary for employees to use the Internet for important personal issues, but such usage must be kept to a minimum and all computer use rules must be followed. Supervisors are responsible for monitoring employee use of the Internet. The progressive discipline process applies to misuse of the Internet. Some examples of limited personal use may be to access other email accounts, bank accounts, and to verify travel plans.

- **Viruses** – The IT network or any ACT International computer resource shall not be used to download or distribute pirated software or data, or to propagate any virus or variant thereof.

- **Chat Rooms /News Groups/Instant Messaging** – Only those employees who are authorized to speak to the media, to analysts, or at public gatherings on behalf of ACT International may speak (write) in the name of ACT International at any Internet chat room / news group or on Instant Messaging. This can occur only after going through the normal concern Managers review and approval process within the Department. Instant messaging/Chat rooms and the like are expressly prohibited to all employees unless specifically authorized by the employee's Managers.

- **Privacy** – Management has the right to inspect and disclose to appropriate people any and all files and /or messages stored on any ACT International computer, including e-mail files.

2.5 System Security

- **Passwords** – ACT International staff are expressly PROHIBITED from sharing or displaying their User ID or password. Some computer system capabilities are restricted to certain User ID's for job related reasons. If a user's job requires such access and the user does not have it, the user should notify their supervisor.

- **Access** – Staff access to internet, various directories, files and/or data is determined by their supervisor. Computers are normally accessible on non-holiday workdays between the hours of 9:00 AM and 05:00 PM.

- **Support** – Computer support is available from ACT International IT staff from 9:00 AM to 5:00 PM on weekdays. When users need access to a computer outside of the normal hours or need authorization to access different files, they should contact their Supervisor who will notify the IT staff in writing. ACT International e-mail access is available 24 hours per day via the Internet.

- **Shutting Off Computers** – Users have the responsibility to sign off from the computer after they are done using the computer or whenever they need to leave the computer for an extended period of time. All personal computers must be shut down and powered off after use at the end of each workday. When leaving a computer unattended, **lock/log off** the computer.

- **Virus Scan** – All disks, removable media, and drives from any outside source MUST be scanned for viruses prior to opening the contents on the disk/removable media/drives.

- **Privacy** – No ACT International computer user should have the expectation of privacy on ACT International computerized systems. No computer user should expect that e-mail messages, either sent or received, are private nor that Internet usage is private.

- **Working From Home** – Processing ACT International work on a home computer (owned by someone other than ACT International) is permissible as long as copyright, confidentiality, or public information laws are not violated. Staff working from home must have updated virus protection software on their computer. ACT International will supply virus protection software and other standardized software to staff working from home upon authorization from their managers. Electronic protected health information should not be accessed from home except under compelling circumstances for timely compliance. Procedures should still be maintained to protect others from viewing protected health information.

- **Moving ACT International Hardware Off Location** – No users are permitted to remove any ACT International computer equipment, components or software from ACT International premises without prior authorization from their Supervisor and involvement of the IT staff, excluding properly checked out laptops and LCD projectors.

- **Laptops** – Laptops need to have virus software updated every 3 months. The IT Department will provide users with practical avenues to accommodate anti-virus software updates. DO NOT have protected health information on laptops unless needed to capture data or transport data in a manner not available by other means. Protected health information should be removed from laptops as soon as possible. If the information needs to be stored, this should be done on one of the internal network drives with assistance from IT if needed.

2.6 Prohibited Uses of ACT International Computers

- **Offensive or Inappropriate Information** – Preparing, displaying, or transmitting messages, pictures, or information considered offensive or inappropriate including, but not limited to, content pertaining to race, ethnicity, religion, age, gender, sexual contents etc.,

- **Copyright** – Copying, replicating, or transmitting documents, software, or other information in violation of copyright laws.

- **Network** – Disabling or overloading any computer network or circumventing any system designed to protect the privacy or security of another user.

- **Unauthorized Persons** – Providing IT systems access to unauthorized persons.

- **Unauthorized Access** – Gaining unauthorized access to electronic information and communication systems.

- **Personal/Financial Gain** – ACT International computer equipment cannot be used for personal or financial gain. This includes, but is not limited, to employees operated ventures/businesses.

- **Inappropriate Websites** – Accessing websites including but not limited to pornography, gambling, gaming, dating, shopping, music file downloading, job searching, chain letters, etc.

2.7 Other Inappropriate use of ACT International Computers

- Do not access radio stations or music files via the PC.
- Do not download personal pictures that friends send as attachments to e-mail. Please tell your friends to send these types of e-mails to your personal e-mail.
- Do not use the video feature on your PC unless you are using it for web cast based training/teleconferencing that is relevant to your work. In other words, do not play movie clips, TV channel news or other video media.
- Confine Internet browsing to work-related use.
- Do not save files, folders, or databases on your Windows Desktop. Each one of these has to pass across the ACT International computer network every time you login and every time you logout. Save them to your Share Drive, instead.
- Do not send "attachments" to internal e-mail. Store your "attachment" – file on the PUBLIC – folder or the division specific folder, and tell other employees in the text of your e-mail where to find it. Attachments should be limited to <20mb in size.

Your signed acknowledgement of the Information Technology Policy will serve as a tool to enforce terms and conditions of employment with ACT International. If you have questions or queries please contact Manager Information Technology.

3. Data Management Policy

3.1 Guiding principles for data and information sharing and management

The following principles have been adapted from the UN Privacy Policy Group Principles, as well as the Humanitarian Principles, Sphere and the Core Humanitarian Standards and serve as a benchmark for the processing of non-personal data.

3.2 FAIR AND LEGITIMATE PROCESSING OF DATA:

Humanitarian data should be processed in a fair manner, in accordance with humanitarian mandates and governing instruments, including Humanitarian Principles, and on the basis of:

(i) the clear, freely given and informed consent of a data subject has been obtained;
(ii) in the public interest, understood in this context as consistent with the organization's humanitarian mandate
(iii) in the vital interests or best interest of a data subject who is not able to make a determination about data management him/herself, or;
(iv) any other legal basis specifically identified by the organization's regulatory framework or applicable laws, so long as these do not conflict with (i) through (iii)

PURPOSE SPECIFICATION: Humanitarian data should be processed for specified purposes that are narrowly-defined, consistent with organizational mandates and take into account the balancing of relevant rights, freedoms and interests. Personal data or non-personal sensitive data should not be shared with third parties without an express purpose and without data safety policies being in place.

NECESSITY, RELEVANCE AND ADEQUACY OF DATA PROCESSING: The processing of humanitarian data should be relevant, limited and adequate to what is necessary for data processing.

RETENTION: Humanitarian data should only be retained as long as necessary to fulfill the purpose for which it was collected. Personal data and other sensitive data should only be retained for as long as it is necessary for the specified purpose for which it is being managed or as required by applicable law or regulations.

ACCURACY: Humanitarian data should be accurate and, when necessary, up to date to meet the specified purposes. There should be capacity to have specific data on crisis-affected individuals removed from databases at the individual's request or when it is no longer accurate.

CONFIDENTIALITY: Humanitarian data should be processed with due regard to confidentiality and not shared with third parties without consent.

SECURITY: Appropriate organizational, administrative, physical and technical safeguards and procedures should be implemented to protect the security of humanitarian data, including against or from unauthorized or accidental access, purposeful misuse, damage, loss or other risks presented by data processing. Training should be provided to staff who manage such information so that they are aware of their obligations.

TRANSPARENCY: Processing of personal data should be carried out with transparency to data subjects, as appropriate and whenever possible. This should include, for example, provision of information about the processing of humanitarian data, as well as information on how to request access, verification, rectification, and/or deletion of that humanitarian data, insofar as the specified purpose for which humanitarian data is processed is not undermined.

ACCOUNTABILITY: Humanitarian organizations should have adequate policies and mechanisms in place to adhere to these Principles.

DATA OWNERSHIP: Crisis-affected individuals are the primary owners of their data. Organizations should have policies requiring staff to inform crisis-affected people of that fact, and of their right to keep their personal data private.

GLOBAL OBLIGATIONS: Processing of humanitarian data must comply with relevant global data standards and protocols.

3.3 Informed consent

Humanitarian organizations should manage personal and non-personal sensitive data in accordance with mandates, the context of the response, governing instruments and global norms and standards including the Humanitarian Principles. Data should only be processed on the basis of one of the following legal bases, in order of priority:

a. the explicit, freely given and informed consent of a data subject has been obtained;
b. in the public interest, understood in this context as consistent with the organization's humanitarian mandate
c. in the vital interests or best interest of a data subject who is not able to make a determination about data management him/herself, or;
d. any other legal basis specifically identified by the organization's regulatory framework or applicable laws, so long as these do not conflict with (a through (c).

When requested, consent is to be given unambiguously through accessible and appropriate methods, enabling a freely given, specific and informed indication of the data subject's wishes, either by a written, oral or other statement, or by a clear affirmative action by the

data subject signifying their agreement to have their personal data processed. The data controller is obliged to keep record of when and how the data subject provided explicit consent for any collection and subsequent use of their data. Informed consent should always be obtained in ways that are culturally and linguistically appropriate and relevant (verbal or written), and the collection of information should not take place until field staff have been trained to ensure that principles of informed consent are understood and respected. Where consent has not been requested, or has not been recorded, the information must not be transmitted to a third party. In such circumstances, it would be necessary to revisit the participant, in order to request and obtain consent before transmitting the information.

Consent covers all data processing activities carried out for the same purpose. The data subject should receive explanations in clear terms and in the language she/he prefers (verbal or written), as to the following:

- the identity and contact details of the data controller;
- the specific purpose for processing of his/her personal data and an explanation of the potential risks and benefits;
- the fact that the data controller may process his/her personal data for purposes other than those initially specified at the time of collection, if compatible with a specific purpose mentioned above; circumstances in which it might not be possible to treat his/her personal data confidentially;
- the data subject's rights and limitations on his/her rights to access, correct and delete her/his personal data and object to processing, either at the time of collection or later;
- an indication of the security measures implemented by the data controller regarding data processing;
- a process and a communication channel for the subject to inform the data controller that he/she wants personal information kept private;
- that the data controller may need to transfer data to another country; and
- an indication of the data controller's policy on record retention (how long records are kept and any steps taken to ensure that records are accurate and kept up to date), whether a data subject's personal data can be shared with other organizations, with the Government in the country of data collection or another country, or be publicly disclosed and to approve that their personal data be used as explained.

3.4 Sensitive and non-sensitive referrals

A referral is the process of directing a data subject (beneficiary) to another service provider because s/he requires help that is beyond the expertise or scope of work of the current service provider. A referral can be made to a variety of services, for example health, psychosocial support, protection services, nutrition, education, shelter, material or financial assistance, physical rehabilitation, community center and/or a social service agency. Similarly, with the consent of the beneficiary, referrals can be made to humanitarian, development or government entities.

Whether the case being referred between service providers is sensitive or non-sensitive, all referrals should include basic steps:

- Identification of org/orgs who are able to meet this need
- Engagement with identified service provider to confirm that the intended beneficiary meets the eligibility criteria of the identified services provider
- A detailed explanation of the referral process to the intended beneficiary. Information provided should include details regarding which services are available, where the service provider is located, and how the service provider can be accessed. A clear option for the beneficiary to decline referral should also be provided
- If the beneficiary consents to the referral, documented consent of the beneficiary should be obtained
- A referral form should be filled in. Electronic copies of the referral form should be provided to the referring agency, the beneficiary, and the receiving agency

- All referral forms and case files should be stored in secure locations to ensure safe data processing

4. Employee Policy Acknowledgment Information Technology (IT) Policy for Employees

I acknowledge that I have read and understood ACT International's Information Technology (IT) Policy. I understand that the information contained in this policy supersedes any written or verbal policies I may have received in the past.

My signature below indicates that I have familiarized myself with the information contained in the policy and that I will seek verification or clarification where necessary.

I understand that the information contained in the policy is subject to change as situations warrant. Further, I understand that changes in policy may be communicated in writing, or in an automated form. I accept full responsibility for keeping myself informed of the policy and practices in place at a given point in time, as well as for any changes thereto.

I understand that, as an employee of ACT International, if I fail to meet these standards, I will be subject to appropriate disciplinary action up to and including dismissal. If I have questions regarding this policy, I should discuss them with my supervisor/manager or Information Technology Manager.

I understand that this policy, and the related practices and procedures contained in the policy do not constitute any form of contractual or legal employment agreement between the ACT International and me. My employment with the ACT International is "at will" and is by mutual consent of the ACT International as the employer and me as the employee as per contact.

_____ _____

Employee's Name (Printed) Employee's Signature

Date _____

NOTE: This form becomes a permanent part of an employee's personnel file.