Information Communications Technology (ICT) Policy for Users

Functional Area:	Information and Communications Technology		
Owner:	Global Chief Information Officer		
Approved by:	IH Executive - April 2012, POLT – May 2012		
Date of approval:	May 9, 2012		
Version:	Final		
Date of next review:	May 2013		
Language:	English, Spanish, French		
Applicable to:		**Plan International, Inc, branch offices and subsidiaries**	
		National Organisations	**NO Guideline**
Contact:	Global Chief Information Officer – Mark Banbury		

Introduction

This document outlines the policy on the use of Plan's Information and Communications Technology (ICT) systems and includes the following policies:

- Plan's Electronic Systems Usage & Access Policy Computer Systems, Email, Internet Usage Policy
- Password Policy
- Policy on the use of e-mails
- ICT Policy regarding staff who leave Plan; and
- System Access Policy for Non-Payroll Staff.

It is the responsibility of all managers across Plan Inc. to implement these policies and of each individual staff member to adhere to them.

These policies will be reviewed annually by People and Culture and the ICT Department jointly, and updated in accordance with best practice and Plan business needs. These policies are not intended to be unduly restrictive, but are designed to ensure that Plan's IT systems are secured against unauthorised access.

1.1 PLAN'S ELECTRONIC SYSTEMS USAGE & ACCESS GUIDELINES COMPUTER SYSTEMS, EMAIL, INTERNET USAGE

1.1.1 Purpose

Plan has made significant investments in installing and maintaining its computer systems and networks with access to e-mail and the Internet for its organisational use in order to improve efficiency, effectiveness and productivity.

To ensure that Plan's computer systems and networks are used to Plan's strategic advantage globally and that risks whether legal or from other liabilities due to their inappropriate use are mitigated, these global policies have been introduced for all users of Plan's computer systems and networks.

1.1.2 Coverage

These policies apply to all users of Plan's computer systems and networks and anyone who has a Plan E-mail address wherever they are based within Plan Inc., including in Country Offices, Regional Offices, and International Headquarters, any of their branch offices or while working from remote access. These policies are a guideline for National Organisations and are recommended for adoption of modification for local policy inclusion.

These policies cover the use of all hardware which connects to Plan Inc. owned systems, including but not limited to desktops, laptops, netbooks, mobiles, and iPads (and other tablet devices) whether owned by Plan or not.

Subject to compliance with the Statement of Responsibilities, the Standard Policy below can be adapted or extended locally in accordance with local law.

1.1.3 Overall Guideline

Plan Inc. will provide employees, and may provide consultants, contractors, partners, and volunteers, (referred to as 'users') with full or limited electronic access, depending on their roles, to Plan Inc.'s computer systems and networks including E-mail, Internet, Intranet, Extranet and other related technologies. Plan will provide relevant training and education as necessary.

Plan promotes the use of its computer systems and networks to facilitate rapid organisational communications, continuous learning, reduction of paper work, and effective job performance.

Plan prohibits any use of its computer systems and networks in violation of any applicable law or Plan policy, including those covering child protection, equal opportunities, racial and sexual harassment, discrimination, confidentiality, copyright and proprietary rights, publications, bullying, data protection and privacy; and/or any use that may potentially cause any damage, PR risk, legal or other liabilities to Plan or its people.

Violation of any of the policies by any user may result in disciplinary action including termination of employment or contractual/other relationships or even criminal prosecution.

All users must be aware that Plan may block spam to prevent network overload and that all materials (including E-mails) generated on Plan computer systems are the property of Plan.

Subject to applicable law, Plan reserves the right to monitor, inspect, copy, review, and store at any time, without prior notice, any and all of the following, as reasonably required to ensure compliance with these policies: usage (including private use as permitted in the policies) of Plan's computer systems and networks, including access to E-mail and the Internet, as well as any and all materials, files, information, software, communications, and other content transmitted, received, stored, or printed in connection with this usage. (Referred to as Monitoring of Systems Usage).

1.1.4 Statement of Responsibilities

Each Plan office is responsible, (through the relevant CD, RD or, in the case of IH, the Global CIO, referred to as Responsible Director) in its jurisdiction, for:

- Implementing and interpreting the policies at their respective locations (at IH, this is a joint responsibility of the Global CIO and Director of People and Culture).

- Maintaining the computer systems and networks with proper security in accordance with the convention determined by IH Information and Communications (ICT) team, and providing relevant training to the users.

- Maintaining e-mail address lists, in accordance with the convention determined by IH ICT.

- Ensuring that an appropriate disclaimer is included on all external E-mails sent by users, in accordance with the convention determined by IH ICT. For legal / language etc reasons, the actual disclaimer used by each Plan office / entity should be tailored to give its legal name / registered number/other details as required by local law.

- Ensuring immediate discontinuation of a user's access to Plan's computer systems and networks when the user ceases to have a contractual relationship with Plan.

- Dealing with disciplinary procedures at the respective units (for example, at IH this is the responsibility of the Director of People and Culture, not the Global

CIO).

- Ensuring compliance with E-mail deletion/retention rules as determined by local ICT.

- Ensuring training and education is provided to the users on the policies in consultation with People and Culture.

- Providing any approval or authorisation required under this policy.

- Monitoring of Systems Usage within that jurisdiction, as determined by the Responsible Director, provided that all users in that jurisdiction are treated equally.

> ***Note:*** *Confidentiality should be observed when an alleged violation occurs, e.g. apparent visit to a pornographic website. Sometimes this can be accidental, or material can enter someone's computer as unsolicited E-mail. Proper care should be taken to protect innocent colleagues. Training, education and awareness building should receive top priority*

.

- Discouraging users from sending any message of a size larger than 4 MB or sending any compressible file larger than 200KB without zipping.

- Ensuring that the users keep their passwords secure and change them as required in accordance with Plan's password policies.

- Ensuring receipt of a signed acknowledgement of Plan's Electronic Systems Access Policy from each user as presented below subject to applicable law.

1.1.5 **Standard Policy:** subject to compliance with the Statement of Responsibilities.

Standard Policy		**What this means for staff**
Users are free to:		
1.	Access Plan’s e-mail, computer systems and networks, visit Internet sites and use Internet tools e.g. Instant Messenger at any time for work-related purposes. Personal use is permitted during non-working hours/lunch hours provided this is not excessive and does not interfere with job performance. **Local Directors may limit non-work related access to systems due to local conditions (bandwidth availability, power consumption, etc).**	In order to protect users from tools that may compromise Plan’s security (for instance, virus infections) or may cause computer failures due to non-compatibility with our existing technology, no tool should be downloaded or installed without prior consultation and approval by the IT department. Requests should be submitted to local ICT support.
2.	Download/upload files/software for work-related convenience.	To ensure that any software Plan uses is properly licensed, and in order to protect users from software that may compromise Plan’s security (for instance virus infections) or which may cause computer failures due to non-compatibility with our existing technology; no software should be downloaded or installed without prior consultation and approval by the ICT department. Requests should be submitted to the local ICT support team. Downloading work-related documents from trusted sites is permitted
Users are prohibited to:		
1.	Send personal or confidential information about sponsors, sponsored children, any third	Staff must ensure that the information is encrypted using a password protected zip file.

	party, Plan or any other user to anyone, except as necessary in relation to Plan's work. (If such information is sent outside Plan's e-mail networks, proper encryption should be ensured and written consent should be obtained from the individuals / organisation concerned as necessary)	
2.	Browse or view websites that contain pornographic, offensive or harmful material, and/or download, display, store, print, distribute, or re- distribute any such material.	Self explanatory
3.	Send any message that hides the identity of the sender. Send or forward chain messages.	A chain email can be defined as either of the following: Any non-work related email that asks you to forward the message to any number of people. An unsolicited e-mail sent to large numbers of people, who would consider it to be a junk email. These messages can crash email systems as users forward copies to more and more people.
4.	Install, without proper authorisation, in a Plan computer, any software which is not owned by Plan or licensed to Plan; or use software owned by or licensed to Plan in any non- Plan computer without proper authorisation.	No software should be loaded without prior consultation and approval by the ICT department. Requests should be submitted to the local ICT support team. The downloading and installation of screensaver and webshots software is prohibited because they contain a high risk of virus infection and may lead to general computer problems. Software which can be used to download illegal software is prohibited. Installing software owned by or licensed to

		Plan in any non-Plan computer invalidates the license and is therefore prohibited.
5.	Use external e-mail accounts for Plan work, unless approved by the local Plan office and processed by the Global Helpdesk.	Use of external e-mail accounts for Plan work will only be approved in the event of an emergency such as: • Plan’s e-mail system failing; or • Inability to access Plan’s email system whilst travelling. External e-mail accounts must not be used for sending confidential or child- sensitive information under any circumstances. Plan’s e-mail system should be accessible from any computer with an Internet connection. Any access problems should be reported to the local ICT support team.
6.	Divert E-mail received at their Plan address automatically to a personal e-mail account without authorisation, unless the arrangement is set up by Global Helpdesk.	External e-mail accounts are not secure and e-mails sent externally can be read by unauthorised sources. Other Plan users would be unaware that a Plan e-mail account has been diverted to an external account and may inadvertently send confidential information to an external account. To protect you and Plan, diverting e-mails sent to a Plan account onto an external e-mail account is prohibited.
Users must:		
1.	Keep their password secure and change it at least as often as required by the individual Plan office. (The system may prompt this whenever possible.)	Passwords must meet the minimum requirements specified in the IH Password Policy.

1.1.6 Security of Systems

In general:

- All computer hardware and software must be ordered through local ICT support.

- As a starting point in any investigation, Plan will assume that you have generated all material stored in the cache of your computer. You should therefore lock your computer if you are away from your desk for more than a short period of time.

1.2 PASSWORD POLICY

The continued availability, integrity, and confidentiality of the services and information provided by Plan information communications technology facilities are essential for the successful operation of Plan's business. The potential threat to the security of these facilities requires Plan to ensure it has an appropriate password policy. Recommendations made by our external auditors and current industry standards are used as a basis for best practice within these policies.

1.2.1 Scope of the Password Policy

These policies apply to:

- All Plan employees, volunteers, trustees and agents;

- The employees, volunteers and agents of other organisations who may have access to and/or use Plan's ICT resources or data.

1.2.2 Policy Objectives

The objectives of the policies are:

- To protect Plan's data and information; Plan data and information will be protected against loss, damage, and abuse from unauthorised use.

- To ensure staff and volunteer compliance with password procedures; Plan requires all staff to be aware of, and comply with password Procedures.

1.2.3 Responsibility for Password Security

Staff
Individual members of staff are responsible for keeping passwords secure and not divulging them to other users.

Passwords are individual for a reason; it is good practice and in your best interests to keep your password confidential. If an incident were to happen and were traced back to your password, the assumption would be that you were responsible for any associated misuse of the computer system.

Under exceptional circumstances such as staff illness, the local ICT support team can give access to another person’s account by resetting the password. Requests of this nature will first be approved by the line manager or department director, and signed off by the relevant director (such as the RD, CD or Global CIO).

Staff are also responsible for ensuring that passwords meet the following minimum requirements:

- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z),
  - English lowercase characters (a through z),
  - Base 10 digits (0 through 9),
  - Non-alphanumeric characters (e.g., !, $, #, %) and,
- Be at least eight characters in length;
- Be changed at least every 90 days;
- Not re-use old passwords.

To further improve security passwords must not:

- Contain all or part of the user's account name;
- Use easily identifiable (simple) words such as ‘hello’ and ‘welcome’;
- Use a password that is personal, such as names, places, colours or birth dates;
- Use similar passwords (that is, must not include amendments to previously used passwords).

The Global ICT team has put in place software mechanisms to ensure that password complexity follows the above rules and that passwords are refreshed every 90 days.

Local ICT support Team

The local ICT support team are responsible for establishing effective controls and procedures for ensuring that individuals comply with the minimum password security requirements.

Employees responsible for establishing agreements with external users for use of Plan’s information processing resources must obtain written agreement that the staff of the external organisation will comply with Plan’s policies when using its facilities.

1.3 POLICY ON THE USE OF EMAIL AND INTERNET

1.3.1 General use of e-mail

Compared to formal letter writing, e-mail is an immediate form of communication and can be perceived as more informal. However, you should take as much (if not more) care in the preparation of e-mails as you do when writing letters or faxes. Improper statements sent in e-mails may give rise to personal or Plan liability, even if only sent internally. Always work on the assumption that e-mail messages may be read by people other than the intended recipient, and that once written your e-mail can be considered to be part of the permanent record.

Do not send trivial or inappropriate e-mails (such as chain letters) and only copy messages to people who need to read them. Otherwise you will compromise the purpose of having the system, namely the fast and efficient transfer of information. You should zip any attachments you send outside IH; alternatively, consider making large attachments available on the Intranet and pointing users to their location via a hyperlink.

If you are sending e-mail to a large group of individuals, use the “BCC” function to input the recipients addresses, and put your own user name in the to field. Start the first line of the e-mail with a disclaimer showing who has received the mass e-mail, such as:

> *(The following message has been sent to National Directors, Regional Directors, Country Directors, NO and RO ICT Managers, IH Department Directors and IH ICT Staff)*

This will eliminate the possibility of someone replying to you and inadvertently copying the whole group. If you want others to receive the replies, put them in the “CC” field.

You must immediately report to the local ICT support team any actual, suspected or threatened occasions that you encounter of e-mails being intercepted or tampered with, or being sent or received contrary to the policies contained herein.

1.3.2 Prohibited Use

Never send e-mails that are abusive, sexist, racist, discriminatory, defamatory, obscene or otherwise likely to cause offence.

- Abusive e-mails are likely to amount to harassment, as are repeated and unwanted e-mails requesting a date, containing sexual innuendo or remarks, or simply pestering the recipient on non-work related matters. It is the effect on the recipient which is important, not whether you intend to cause offence.

- The same considerations apply to issues concerning racial harassment.

- Defamatory statements sent by e-mail either externally or internally could cause legal liability to both you and Plan, and a claimant may be able to bring legal action in any country where the message is read.

Plan acknowledges that it may not be possible to control receipt by you of offensive material from external sources; you are however accountable for passing to others any material you receive. If you receive any offensive material, you should inform your supervisor or the local manager responsible for people and culture.

Please refer to the Standard Policy section for further details.

1.3.3 Personal Use

You are permitted to attend to personal matters by e-mail during working hours, but this personal use must not be excessive and must not interfere with your job performance, nor interfere with the performance of Plan's systems. Access to personal use of e-mail may be limited due to local ICT constraints. You should not use the system for inappropriate purposes, for example to send jokes, cartoons or chain letters, or for any of the “Prohibited uses” outlined above.

Please refer to the Standard Policy section for further details.

1.3.4 Employee's responsibility to protect Plan's system from viruses

Computer viruses pose a significant threat to the stability of Plan's ICT systems and it is the responsibility of every user to minimise the risk of their introduction.

Any e-mail received with a non-text file attachment (which may be contained within a zipped file attachment) must be deleted unless it is clearly identified as being work related. If you have any suspicions about a file attachment, in particular a non-text attachment, you should refer it to the local ICT support team before opening it.

Any e-mail you receive warning of potential viruses should be forwarded to the local ICT support team, not circulated to "everyone".

1.3.5 Legal Liability

Always remember that, when you create an e-mail, you are creating a document; it may be required to be disclosed in any Court proceedings, or as a result of investigations carried out by authorities. E-mail messages are not automatically destroyed even after they have been ‘deleted’ and it can be illegal to attempt to do so.

You must take care to avoid entering into legal relations or contractual commitments with third parties by e-mail. It is important that you do not make statements by e-mail in pre-contract negotiations that are incorrect which could give rise to claims for misrepresentation, and that you do not attempt to conclude contracts by e-mail.

Never alter someone else's e-mail and forward it without highlighting your alterations, as this could amount to misrepresentation.

1.3.6 Guidance on use of the Internet

Employees have been given access to the Internet as a tool to support their work. Occasional personal use of the Internet during working hours is permitted, provided it does not interfere with your job performance, and it is agreed that it does not interfere with Plan's network and systems (see the Standard Policy section). However, it is expected that employees will generally restrict any personal use of the Internet to non-working hours. At no time may you use Plan equipment to access illegal, immoral or otherwise inappropriate sites, in particular sites with pornographic or on-line betting / gambling content or on-line chat rooms which are not related to Plan's business. If you enter any of these sites by accident, leave the site immediately and inform your manager.

Please refer to the Standard Policy section for further details.

1.3.7 Monitoring of e-mail and Internet use

Plan requires you to comply with the guidance given in these policies and, in order to ensure compliance with it and consider whether there have been any breaches of it:

- Plan retains the right to monitor each employee's individual use of e-mail including the volume of e-mails sent and received, the addresses e-mails are sent from and to, and the "subject" description in the message header. Where there are reasonable grounds to believe that you have breached these policies, Plan retains the right to monitor the content of e-mails, whether sent or received in connection with your work or for personal reasons and whether sent or received during or outside of normal office hours.

- Plan retains the right to monitor each employee's individual use of the Internet including the volume and time of Internet usage by each employee. Plan retains the right to monitor websites that have been visited from a session in which your username is logged in; this may include reviewing any material downloaded from websites using Plan equipment (whether accessed and/or downloaded during or outside normal office hours). You should be aware that Plan is able to trace the entire history of Internet sites accessed by employees.

With the acceptance of this policy as a condition of your employment, you authorise Plan to monitor your use of e-mail and the Internet in this way.

1.3.8 Disciplinary warning

Plan will carry out an investigation if there is a complaint of misuse of ICT systems (including misuse of e-mail and/or the Internet), or if Plan suspects an employee has been misusing the system. Plan expressly reserves the right to access the employee's device supplied by Plan (computer, laptop, netbook, mobile, tablet) to investigate such a complaint or to make available the employee's device supplied by Plan to an external IT adviser to carry out the necessary investigations.   Plan reserves the right to suspend you from your employment to allow the necessary investigations to be carried out.

Any misuse of the system will result in disciplinary action (up to and including summary dismissal) being taken against you, in accordance with Plan's disciplinary procedure.

1.4 ICT GUIDELINES REGARDING STAFF WHO LEAVE PLAN

1.4.1 Introduction

It is in the interests of Plan to ensure that only current staff may be registered to use Plan's computer systems and equipment, to avoid creating potential security loopholes which may be used to allow access to unauthorised users, and to protect Plan’s intellectual property.

It follows from this that a procedure has been established to ensure the return of all Plan supplied equipment and to delete the computer accounts and e-mail addresses of staff when they leave the organisation.

The term "staff" in this context comprises staff on the payroll, consultants, agency staff and volunteers. Staff are defined as leavers when leaving data is entered into the payroll system. For all others a leaving date will have been set when their computer accounts were created.

1.4.2 Payroll Staff accounts

- Before a member of staff leaves Plan, any files in his/her filestore which need to be kept should be transferred to the filestore of another member of staff who is to take over the leaver's responsibilities. This is the joint responsibility of the leaver and the office/department administrator. Equally, it is the responsibility of the leaver to delete before he/she leaves any private and confidential files which he/she does not wish to be accessed by others. Leavers are also responsible for removing their names from any electronic mailing lists that they have subscribed to.
- Staff leaving the employment of Plan are reminded that any computer software installed under a Plan License on a non-Plan owned computer (e.g. IPASS, Microsoft Office products, etc., licensed under a Plan Agreement) MUST be deleted. Failure to take action will deem the software to be unlicensed and hence illegal.
- Leavers’ accounts and filestore will be deleted one month after their date of departure. The leaver’s line manager/head of department is responsible for invoking the exception procedures for any staff whose registration and filestore need to be retained.
- These procedures are designed to accommodate staff continuing to collaborate with Plan in a part time capacity after they have left. They must not be misused to obviate the security process.
- In the event of a member of staff leaving without notice (for example due to death in service), the office/departmental administrator will be responsible for initiating the transfer of files to an alternative account before the original account is deleted.

- The exception procedure for leavers with a valid reason to retain their accounts will be instigated only on receipt of a formal authorisation from their line manager/head of department and approved by relevant director (RD, CD, Global CIO). This must be submitted to the Helpdesk in the one month period following the leaving date; it must specify the retention period (maximum 12 months) for which their registration is to be extended. At the end of the specified extended period, the leaver's registration and file-store will be deleted automatically unless a further authorisation has been received in the interim. Non-payroll staff will be treated in the same way as leavers, that is to say they will be allowed to retain their accounts only upon the express request of their line manager/departmental head. This request will need to be renewed annually.

- One month after the staff member leaves, if exception procedures are not invoked, local ICT will delete the leaver's registration on the central computers and delete all data files and electronic mail messages in the leaver's file-store on those computers. All offices/Departments should note that requests to recover files must be received within 2 weeks of the deletion date.

- The office/departmental administrator is responsible for setting reply and forward rules on the leaver’s e-mail account on their date of departure. The reply rule should explain that the recipient has left the organisation and the e-mail is being forwarded onto a nominated contact. The forward rule should forward email onto the departmental administrator or nominated contact. Mail must not be forwarded onto a leaver’s external email address.

- Each office/department administrator is responsible for notifying their local ICT when an employee is due to leave. This can be done via the Global Helpdesk by completing the leavers form on the **pla**net.

- Local ICT are responsible for removing a leavers access to Plan’s systems on the date of departure and deleting all data files and electronic mail messages in the leaver's file-store either one month after departure or on the date specified by the person invoking the exception procedures.

1.4.3 All other accounts

- Before any non-payroll staff member leaves Plan, files in his/her file-store, which need to be kept for ongoing research or administrative purposes, will be transferred to a suitable account. Equally, it is the responsibility of the non-payroll staff to delete before he/she leaves any private and confidential files which he/she does not wish to be accessed by others. Leavers are also responsible for removing their names from any electronic mailing lists that they have subscribed to.

- These staff will be given no notice of the deletion of their accounts and file-store.

1.4.4 Equipment of leavers and equipment not in regular use.

- Before a member of staff leaves Plan, the leaver’s line manager/department administrator must ensure that any equipment supplied by Plan has either been transferred to another member of staff who is to take over the leaver's responsibilities, or returned, as below.

- Return to ICT all computer equipment that may have Company data thereon, or may be connected to the network by any means that is not both in regular use and assigned to a Plan employee.
- This equipment is to be data cleaned and made Loan stock, or securely disposed of, and is thereafter no **longer a security risk for lack of secure storage or automatic antivirus updates**. This applies especially to laptop computers.

All spare or loan computer equipment must be returned to ICT when not in use. Only the ICT Department is permitted to hold spare or loan computer equipment.

1.5 SYSTEM ACCESS FOR NON-PAYROLL STAFF

1.5.1 Introduction

Any member of staff, temporary staff, contractor, consultant, volunteer or other representative of Plan who uses Plan's ICT systems, must comply with these policies.

Throughout these policies the term "non-payroll staff" applies to temporary staff, volunteers, consultants & contractors that are not on Plan's payroll system.

1.5.2 Policy

Plan regularly employs non-payroll staff in the course of its business. It is important that Plan's ICT systems are secured against unauthorised access whilst ensuring that non-payroll staff have sufficient access to perform their role during the term of their contract.

Non-payroll staff must adhere to all Plan policies and policies including the Usage & Access to Plan's Internet, and Email & Computer System's policies.

Adhering to these policies will enable non-payroll staff to perform their role effectively without compromising Plan's ICT systems and will reduce the risk of unauthorised access.

1.5.3 Access to Plan's Systems

Access to Plan's ICT systems will only be granted to non-payroll staff that require access to Plan systems in order to perform their role. All requests for access to Plan's systems must be submitted to local ICT support, who will create an account that gives the non-payroll staff member the level of access appropriate for their role.

The non-payroll member's line manager is responsible for submitting requests to local ICT support. Requests must include:

- The person's full name, company name (if applicable) and position

- A list of systems they require access to (including e-mail if required)
- Level of access required for each system; and
- Contract start and end dates (account expiry date)

Local ICT support is responsible for creating and deleting accounts. Accounts will be disabled on the expiry date specified on the request, and deleted as per Plan's policies on deleting computer accounts.

Temporary staff, contractors, and volunteers are permitted to use a Plan e-mail account in order to perform their role. Consultants are not permitted to use a Plan e-mail account.

This policy has been viewed and is approved by:

Nigel Chapman (signed): ___________________________ Date: ___________
Chief Executive Officer, Plan International, Inc

ICT POLICY FOR USERS

Acknowledgement

I understand the terms of Plan's ICT Policy for Users and agree abide by them. I agree that Plan may monitor the e-mail messages I send and receive, my activities associated with accessing the Internet, and any system activity including transmission or receipt of any kind of file. I understand that any violation of any of the policies may result in disciplinary action including termination of employment (or contractual/other relationships) or even criminal prosecution.

Signature: ____

Name: ____

Position: ____

Location: ____

Date ____