INFORMATION AND COMMUNICATIONS SYSTEMS POLICY

Contents

INTRODUCTION
Islamic Relief views the internet and e-mail as essential tools for its employees. However, the use of those tools can expose the organization to technical, commercial and legal risks if they are not used sensibly. The aim of this policy is to:
Provide guidance on staff use of the internet and e-mail at work to minimize the organization's exposure to these risks.
Explain what is permitted and what is not.
Provide some explanation of the legal risks that staff need to be aware of when using the internet and e-mail.
Explain the consequences for members of staff and the organization if the rules set out in this Policy are not complied with.

ANY BREACH OF THE RULES OUTLINED IN THIS POLICY COULD RESULT IN DISCIPLINARY ACTION BEING TAKEN AGAINST A MEMBER OF STAFF WHICH COULD LEAD TO DISMISSAL.MISUSE OR BREACH OF THE POLICY COULD ALSO LEAD TO CIVIL OR CRIMINAL ACTIONS AGAINST A MEMBER OF STAFF OR THE ORGANISATION.

THIS POLICY IS THUS DESIGNED TO PROTECT EMPLOYEES AS WELL AS ISLAMIC RELIEF.
This Policy reflects Islamic Relief's agreed strategy for access and usage of e-mails and the internet. This strategy has been developed by the Support Division and has been endorsed by the Executive Committee on 30 December 2003. The ultimate responsibility for this Policy rests with the Support Division Manager.
It is essential that the following sections are read very carefully. Islamic Relief will take breaches of this Policy very seriously. If there is anything that is not understood, it is the responsibility of individual staff members to approach their Line Managers for clarification.
Having read the Policy, staff must sign and return the Declaration sheet to the Support Divisional Manager to indicate that it has been read, understood and accepted. Staff members are urged to retain a copy for their reference.
Acts for Referral:
43 of the Telecommunications Act 1984
Obscene Publications Act 1959 and 1964
Data Protection Act 1998
Criminal Justice Act 1988

GENERAL INFORMATION ABOUT THE IT POLICY GUIDE

Islamic Relief's information policy is intended to address all aspects of computers in the workplace and information security issues. It should be noted that best-crafted policies may not stop violation completely but, good policies will minimize the opportunities for violation and therefore minimize the organization's liability.
following guidelines, if complied with, should maximize the use of IT equipment as well as the security of the equipment.
of the computer and information security problems posing a potential threat to organizations of all sizes are easy to correct. problems occur when individuals attempt to gain access to computer

systems and data, through various security holes. The procedures outlined herein explain how policies can plug security holes.
the most common threat for any organization is the existence of viruses, worms, and other hostile programming codes. While it may be impossible to completely guard against all such threats, compliance with the following policies will minimize the threat potential.
policy will include:
Educating users on the threats
Setting out policies that minimize the infection potential
Installing and regularly updating anti virus software
Installing all of the security patches for operating systems, web browsers, email clients, and applications
employees will be provided with a copy of the computer policies and required to sign a statement that they have received, read, understood, and agree to abide by them. This applies to all existing employees, contractors, temporary workers, etc, as well as all new personnel.
of staff should read thoroughly all areas of the policy regardless of whether or not they apply. The topics are inter-related and thus discussion of one may provide additional insight into another.
Will abide by the logon banners below that reiterate emphasis on the organizational policy. The additional reinforcement provided by the logon banners should also serve to strengthen the organization's right to inspect email and other computer files should the need arise. This applies to all employees, or other non employees, contractors and anyone who has access to Islamic Relief equipment.

LOG ON BANNER

The existing computer system is the property of Islamic Relief. The computer system, including all related equipment, storage devices, networks, and network devices, is provided solely for the use of authorized users; this includes Internet access and electronic mail (email).

All information contained on Islamic Relief's computer systems, storage devices, and networks is the exclusive property of Islamic Relief. The computer systems and networks may be monitored and/or reviewed at anytime for any reason deemed appropriate by Islamic Relief.
reasons for monitoring include, but are not limited to:
Ensuring that access is authorized
Ensuring compliance with policy, rules, regulations, and/or laws
Management of the system
Monitoring may include, but is not limited to:
Examination of email
Examination of the user's activity
Examination of any computer files.
All information, including any personal information, placed on this computer system, on any storage device, or sent via Islamic Relief's computer systems or networks is subject to monitoring and/or review. Any information discovered during monitoring and/or review may be stored and/or used for any purpose Islamic Relief deems appropriate. Use of this system, whether authorized or unauthorized, constitutes consent to any and all monitoring and/or review by Islamic Relief.

INTERNET USE

This policy applies to anyone using Islamic Relief's equipment for Internet access systems. This includes employees, non employees, subcontractors, temporary staff and visitors.
Islamic Relief's Internet access is to be used for business purposes only; no personal use of the Internet access is permissible. All information created, sent, or received via Islamic Relief's computers, networks, Internet access, and/or email systems are the property of Islamic Relief.
Islamic Relief reserves the right to monitor, filter, and/or review, at anytime, all Internet usage via Islamic Relief Internet access. Islamic Relief further reserves the right to reveal any Internet access related information to any party that it deems appropriate. The use of coding, the labeling of a communication as private, the deletion of a communication, or any other such process or action, shall not diminish the rights of Islamic Relief in any way.
Islamic Relief will disclose Internet access information to any party that it may be required within reason by law or regulation. This may include law enforcement search warrants and discovery requests in civil action but only on the authorization of Islamic Relief. Also users will not access any material that is not directly relevant to their assigned duties, or the organization.

It will be a breach of Islamic Relief policy for users to download software from the internet unless prior written approval has been obtained from the Head of Information Technology or management staff. Further, the internet access system shall not be used for any purpose in violation of Islamic Relief's policies.
Each user is responsible for ensuring that their use of Islamic Relief internet access is consistent with this policy, and any other Islamic Relief policies. Internet sites containing jokes, pornography, sexist material, racist material, defamatory material, obscene material, pirated software, or any other inappropriate material shall not be accessed.
Islamic Relief internet access will not be used for any commercial or non-commercial activity that is not beneficial to Islamic Relief.
Users should be aware that the internet sites they visit collect information about visitors. This information will link the user to Islamic Relief. Users will not visit any site that might in any way damage Islamic Relief's image or reputation.
Users should be aware that much of the material available on the internet is copyrighted or trademarked. Other than viewing publicly available material, users will not use any material found on the Internet in any manner without first establishing that such use would not be in violation of a copyright or trademark or Islamic Relief policy. Users will not enter any internet chat rooms or chat channels. Users will not give their passwords to anyone.

VOICEMAIL

Voicemail in this policy refers to any type of equipment or system that records messages from unanswered incoming telephone calls. This includes answering machines.
All voicemail systems and all communications stored therein are the exclusive property of Islamic Relief. Islamic Relief may review stored messages at any time, for reasonable purpose, with the consent of managerial staff. Users having voicemail are to check it regularly and return telephone calls as soon as possible, as a matter of good professional conduct.
Voicemail greetings should include the user's name and a request that the caller leave their name, telephone number and a brief message, as is standard on Islamic Relief phones.
Users who will be out of the office for an extended time should change their greeting to advise callers of their absence.
Retrieving voicemail messages
Please use the following guide to make full use of the voicemail service:

Press the # key once and follow the menu:
Press Replay the message
2 Next message
3 Delete message
4 Reply or Call back
5 Previous message
6 Save message
7 Undelete message

PHYSICAL SECURITY OF COMPUTER ASSETS

Employees will ensure that all computer assets (computers, monitors, laptop computers, printers, etc.) that are assigned to or regularly used by them are maintained and used in a manner that is consistent with their function and such that the possibility of damage and/or loss is minimized.
Computer equipment will not be removed from company premises without prior authorization from the Head of Information Technology. Users will not modify company computer equipment in any manner including, but not limited to attaching external disk drives, external hard drives, changing the amount of memory in the computer, and attaching/installing any peripheral device. This however shall not apply to Information Technology staff while performing their assigned duties.
Whenever possible all portable computing equipment (laptop computers, palm top computers, electronic organizers, etc.) will be maintained under the direct supervision of the user that they have been issued to.
Computer and electronic equipment are generally delicate and should be treated accordingly.
Damage to or loss of computer electronic equipment caused by negligence and/or violation of this policy may result in the responsible party being charged for the repair or replacement costs.

Laptops and portable equipment purchased by Islamic Relief will be treated as property of Islamic Relief. Any laptop used internally or externally will remain the property of Islamic Relief but will be the sole responsibility of the user when in use. The maintenance will remain the responsibility of Islamic Relief when the laptop is not in use, this will include the general maintenance of hardware, software and licensing.

OWNERSHIP OF INFORMATION, DATA, AND SOFTWARE

DEFINITIONS:
Information: Knowledge, in any form that is of value to Islamic Relief

Data:

Any computer information, including, but not limited to, information that has been entered into a computer, stored in a computer, or retrieved from a computer. Examples would include spreadsheet and database entries, emails and internet information.

Software:

Computer operating systems and programs
All information and data generated or gathered by an employee, in the course of their employment and/or utilizing Islamic Relief's assets, will be the exclusive property of Islamic Relief. No information or data shall be transferred to, given to, or loaned to any other organization or outside individual except for those instances where it is in the approved course of business, and with the express authorization of managerial staff.
All software purchased by, licensed by, or created by Islamic Relief is the exclusive property of Islamic Relief and may not be transferred to, given to, or loaned to any other organization or outside individual without the express written authorization of managerial staff.

ACCESS TO COMPUTER INFORMATION AND HARDWARE

Computer related resources under the control of Islamic Relief exist for the furtherance of the organization's pursuits. Islamic Relief may inspect or monitor any company owned, leased, or controlled computer, computer device, network, computer facility, or storage device at any time for any reason. This includes the inspection of email (incoming, outgoing, or stored) and the monitoring of Internet usage. Islamic Relief may divulge any information found during such inspections or monitoring to any party it deems appropriate.
use of encryption, the labeling of an email or document as private, the deletion of an email or document, or any other such process or action, will not diminish the organization's rights in any way. the organization's authorized encryption may be utilized. All passwords/encryption keys will be kept on file with the Head of Information Technology upon utilization of Islamic Relief equipment.
phones, wireless applications and attachments that are purchased as Islamic Relief equipment will only be used for work carried out for Islamic Relief. All other applications owned by employees cannot be used whilst carrying out employment for Islamic Relief. Non Islamic Relief equipment and attachments may only be used with the authorization of the appropriate line manager and the Head of the Information Technology Department. Use of non authorized equipment will be regarded an infringement of the Information policy and users will be subject to internal disciplinary action.
pen drives, portable hard disks and flash devices represent an easy and convenient method of moving data between computers. Whether the device is Islamic Relief's or personal property the user will be responsible for its use. However the maintenance is the responsibility of the IT department if purchased by Islamic Relief for work purposes. The following must be adhered to:
The physical security of the device is crucial, as a lost device may carry sensitive data. Users will have to delete data that is not required, and lock data that is contained on the device with protective passwords. Files contained on the device should always be backed up at other locations (hard disk or CDROM). This will ensure that valuable data is not lost through viruses, theft or other means.
regular and routine maintenance, virus checks will need to be made, which will be the duty of the user, before and after the device has been used, as viruses can be transferred to other equipment when the attachment is used and often destroy valuable data. Due to privacy and security issues all attached equipment that is used as a course of employment and for the users own use, must be authorized by the respective manager and a member of staff in the IT Department.

of staff need to understand what information is confidential or sensitive and how to handle it. Staff also needs to know what information is important to their daily activities and be given a means to back it up.

Security is more than protecting equipment from theft or disclosure. More information is lost through poor practices than through intrusions. Many organizations are specifically engaged in recovering data that has been accidentally deleted, accidentally overwritten, is on a hard drive that was reformatted, or is on a hard drive that is no longer accessible. Where it is possible, recovering data can be time consuming and costly. Routine backup can avoid excessive costs.

data that is critical or needs to be maintained for long periods of time should be archived to CD-ROM. Magnetic media (hard drives, diskettes, tapes, removable disks, etc.) are all susceptible to magnetic fields, as well as temperature and humidity. Relying on any magnetic media for long-term storage of critical data is an invitation to disaster. Diskettes that have been properly stored have been known to become corrupted over the course of a few years. CD-ROMs, on the other hand, are known for their ability to store data for extreme periods of time without corruption. CD-Rom is a far better media for storing important data.

Zip disks are a great media for moving large files from one computer to another, they should not be considered for long-term storage. The Zip drive is just as susceptible to problems as long term storage on a magnetic field.

is important to remember that the best tape backup devices will not be of any use if the critical data located on your computer is not backed up. Human nature being what it is, when backing up data we will do so for a short period of time then gradually stop backing up. Eventually data that could have been backed up can be lost, but this can be avoided if the data is backed up periodically. Backing up on CD is often very inexpensive compared with the loss of important and valuable data.

area that is often overlooked in information security is refuse. Avoid putting any information with personal details of anyone in the organization into the bins, or data that is strictly confidential. Any such documents should be shredded. Important documents that need to be shredded should be done as soon as possible to avoid the data being left around or lost. Staff should make use of the organization's shredders.

All computers should be set to require a unique password to boot, even if the computer has a password protected screen saver activated (all computers should be set up with a password protected screen saver that activates in a reasonably short period of time). If a staff member does not have this function then it can easily be set up.

Vigilance is needed with portable equipment. The theft and loss of laptops is so great, that added steps need taken to safeguard their contents. The entire hard drive should be encrypted and a password for access requested. Even though the hardware may be lost, at least the information will be safe. As with other passwords, each computer should be have a unique password that is known to only to the user and specified members of the Information Technology Department.

Organizations adopt the approach of only protecting data that they believe is important. This is contrary to the proper method as it may not necessarily be whether a particular file has value or not to outsiders. Protecting data after it has been accessed by individuals who had no need to access it or after it has been stolen is a poor measure.

Information vulnerability that must be guarded against is computer viruses. Antivirus solutions are very affordable, compared to the price of viruses destroying important data. Islamic Relief has deployed anti virus software on every machine and every PC. Virus infections originate from any number of sources. Some of the most common are: shared word processing documents; email attachments; Internet downloads; and diskettes used for transferring files from one computer to another. While some viruses are a mere annoyance, many can cause computer crashes and data loss. Lost productivity directly equates to a waste of resources.

Viruses appear continuously. It is not enough to just install anti virus software; the software must be updated periodically and on most machines this is automatic. Likewise, the latest security updates for operating systems, web browsers, applications, and email clients have been installed and are available.

INFORMATION SECURITY POLICY

Confidential information refers to any information, in any form, that is an advantage to the organization in any way. This includes:

Client/customer lists

Employee lists
Business projections
Business plans
Proprietary processes
Information on research and development
Pending sales
Pending purchases
Pending contracts
Production costs
Production schedules
Design drawings
Organization's financial information or personnel information
IDs and/or passwords should not be written down and kept within the general area of the computer. Users should not utilize internal passwords or substantially similar passwords on external systems (i.e. websites, web based email, etc.). Users should not allow any person to access, in any manner, their assigned computer equipment unless that person is specifically authorized to.
Attempt by another person to obtain a login ID and/or password, or any other suspicious activity, will be immediately reported to the appropriate staff. All information created by, obtained by, or utilized by users in the course of their employment is the exclusive property of Islamic Relief.
When physically able to, users should not access any information other than that which they are specifically authorized to and is necessary for the performance of their assigned duties. The information created at Islamic Relief cannot be utilized for the benefit of any other person or organization. Unless specifically designated otherwise, all information is considered to be confidential. that is a Sensitive or private and confidential should never be distributed or given by any means, to persons outside of Islamic Relief unless all of the following conditions are met:
The information given is expressly approved, in advance, by the author or designated department.
Confidential information is encrypted, if a computer file, or otherwise sealed in
It is in an envelope or other appropriate container, specifically written with the intended said persons name.
The document, letter or email text includes a warning to the recipient that the material is Sensitive, or Confidential for an intended person and is the property of Islamic Relief.
The transmittal letter or email text contains a specific statement of why the recipient is receiving it, what they may do with the information, and who, if anyone, they may disclose it to.
A copy of the transmittal letter or email is permanently archived by the user whether by ways of hard or soft copy.
All users must ensure that their computer files are properly backed up. The system back up is the responsibility of the I.T Department but the individual user is responsible for their own data that needs to be backed up.

All users must ensure that any material to be discarded which contains sensitive, private or confidential information, in whole or part, will be properly and immediately destroyed.
All computers have anti virus software installed. This software is to remain activated at all times. The I.T Department will ensure that the software is updated as appropriate. It is the individual member of staff’s responsibility to report any virus affecting their equipment to the appropriate persons. Failure to do so may result in valuable data being lost and a high recovery cost.
The I.T Department will ensure that all security updates for operating systems, web browsers, server applications, and email clients are installed as soon as they become available. If not available then staff should notify the appropriate department who will consider the request.
The I.T Department will ensure that the hard drive of any computer to be discarded or sent out of house for repair will have all sensitive, or confidential information thoroughly removed from it.

INSTALLATION AND USE OF SOFTWARE

Employees will not be allowed to install software on the organization's computers without authorization from the I.T Department or managerial staff. Any employee committing software piracy on the organization's computers exposes the organization to civil liability or criminal proceedings.
It is essential that an employee who wishes to install their personal software provides a copy of the license to the I.T Department and signs a statement that specifies that its use on the organization's computer will not violate the license. Otherwise a proof of purchase will be needed. (I.e. if the license is for a single installation, the employee cannot have it installed on their home computer also).
Software downloaded from the Internet poses a particular hazard to Islamic Relief in addition to the potential for virus infection, unless it is specific downloadable software that has been purchased.

Again the use of this software must have a relevant license. must also be aware of the significant burden put on the I.T Department when support is required.
Without the prior authorization of the Information Technology Department, users must not:
Install any software on company owned computer equipment.
Install company owned software on any non-company owned computer equipment.
Provide copies of the organization's owned or licensed software to anyone.
Users must not engage in any acts of software piracy. The heads of the appropriate departments shall ensure that all software installed or utilized on company machines is properly licensed, and copies of the licenses are forwarded to the I.T department. Software piracy is utilizing software in violation of its licensing agreement.

PERSONAL USE OF COMPUTER HARDWARE AND SOFTWARE

The equipment at Islamic Relief refers to assets that have been purchased for the organization's use, and are tools for performing necessary functions. The use of the organization's assets for commercial purposes not relating to the organization (i.e. the employee has their own business on the side, or other activities) is not allowed. Doing so exposes Islamic Relief to a liability created by the employee's side business. The use of such assets is a violation of this policy and may cause the organization to face grave consequences.

POLICY

Islamic Relief owned computer hardware and software may only be utilized for business purposes relating to Islamic Relief. No personal use of company assets is allowed; this includes the company's email system and Internet access and resources.
Such use must not include:
Political activity at any level.
Pornography
Sexist Material
Racist Material
Any illegal act
Any other inappropriate behavior
Photocopying, Printing and fax machines are used solely to for work purposes and are not to be used for personal use. If personal use is required then your line manager must authorize this. All maintenance of equipment will remain with the Support department excluding equipment purchased by individual departments, for which they have sole responsibility.

ELECTRONIC BACK-UP POLICY

Purpose of the backup policy

Data can become damaged, corrupted, destroyed or inaccessible through a variety of mechanisms e.g. user error (deletions, overwrites, hard drive reformats), hardware theft, hardware failure (disk drive, controller etc), catastrophic software failure, network failure, power supply failure (fluctuations, outage etc) and environmental and other accidents (fire, flood etc). It may also become a legal obligation for Islamic Relief to maintain archives of content or data for a certain minimum period of time, in case of subsequent demand by authorized government agencies.

Who does the data belong to?

In case of misconception company machines should not hold any personal data. Only data belonging to Islamic Relief should reside on Islamic relief hardware thus assuring that no ones personal privacy will be threatened should issues of data, software or hardware scrutiny arise.

Whose responsibility is it to backup/archive?

As employees generate, collect and share data on their local machines as well as the servers, they should know what needs to be backed up or archived. Backing up and archiving data that is on individual PCs is thus solely the individual’s responsibility. A general rule is that no more than ~50Mb

of backup space per user should be allowed on servers as it is only required for active files or files in hand. Once the active files are complete and become non-active they should be archived. Backing up databases on the servers on the other hand is the responsibility of the database administrators, backup supervisors and network administrators.
Media used to store backups can be anything from floppy disk, tape, zip, cd, DVD etc. These are purchased through individual departmental budgets not obtained from the IT department. Additional specifications and advice on what to purchase can be obtained from the IT department, at the staff members own discretion.
Backup is primarily intended for disaster recovery. It is not possible to safeguard and protect Islamic Relief's most valuable data asset 100% against loss but it is possible to maintain an operational status if a disaster should occur and data loss happens.
The assumption in most cases is that backed-up data will not be read. The purpose of this policy is to provide a plan and mechanism to achieve disaster recovery, bearing in mind that there are three backup categories to consider: system data (win xp, win 98 etc), application data (MS Office, Adobe Acrobat Reader etc), company data: emails, contacts, files, favorites, databases, Records, reports, folders, Forms, pictures, movies, sound files, databases etc). While systems and applications can be readily backed up from CDs, active company data cannot, therefore has to be regularly backed up. It is essential to have clean, virus free backups and archives of data.
Archive, is the moving and storage of inactive files from online disk storage to another medium for long term storage. This means disk files are deleted after copying. The process is used to release the limited and finite online storage for re-use. Archives are kept because there is a possibility that they might be required at some point in the future e.g. for monitoring and management.
Even when a member of staff leaves the organization, valuable data needs to be archived and handed over to line mangers or the Human Resources Department. Files are archived after the technical team has been notified that a user is no longer entitled to use IR computing facilities. It is not normal for an account to be restored from archive in its entirety.Users who change their status within IR and are issued with a new login/e-mail account should arrange for their general file store to be transferred to their new account before their old account is archived.
Restore process is always more important than the backup process so individuals need to verify and make sure that the backed up data is capable of being restored.

Why everyone should manage their data

Managed data is audited, organized & structured into separate categories as follows:
Critical/non-critical data
Sensitive/insensitive data
Active/ non-active data.
It also tends to be located in fewer locations. This inherently helps to increase performance and productivity. Work in hand (or active data) is regularly backed up while non-active data is archived e.g. once a month/ once a year. Here the importance, priority and frequency of backup and storage requirements will be well known to the person who generates and organizes the data.
Unmanaged data tends to be dispersed in many different locations. This inherently introduces duplication, complicated file and folder searches, and time wastage and business process slow down. The end result is huge amounts of clutter and a flood of systems (PCs, servers, backups and archives). Here, clearing up the mess obviously entails costs in terms of maintenance, support, hardware, media and many wasted man-hours.
Backup of user machines
Individual users of IR hardware (laptops, desktops, PDAs, tablet PCs etc) who generate or collect data are responsible for ensuring that the data is properly backed up or archived. Depending on others to backup data should not be assumed as individuals need to make their own backups to protect data against loss.
Writeable CD-ROM drives have been provided on all new machines for back-ups and archiving. (More drives could be purchased if necessary). Other higher capacity removable disk-drives, tape-drives, DVD drives etc could also be used. Properly labeled backups and archives should be retained under lock and key for as long as necessary.

Backup of servers

It is the responsibility of the database administrators, backup supervisors and network administrators to maintain crucial data backups of the server and maintain server service functionality. While these staff members will ensure that all attempts are made to back-up all critical server data on a daily/

weekly/ monthly basis as deemed fit, remote off-site backups, though beneficial, will only be put in place once feasible. These backups will be regularly monitored against failure using the onsite backup test & verification facility. Servers will be protected through a combination of measures: system images (Ghosts), Emergency Repair Disks (ERDs) or reinstalled afresh from original CDs/DVDs if required.
Users should try to minimize and eliminate human error. All attempts will be made to automate the backup processes using a robotic auto-tape loader and library. A job completion auto-alert by email will alert failures. It should be noted that due to limited time to do backups and limited backup capacity of 500Gb on 10 tapes, not all data can possibly be backed up so most of the tapes will have to be recycled and overwritten. (Some PCs alone hold in access of 80 Gb). This scenario could change if individual departments were to supply more tapes and pickup the backups. Tapes are labeled according to barcode numbers. A list of tape versus server name and date of backup should easily be possible. It should also be also possible to retain full daily backup data for a week (Mon-Fri) before being overwritten.
Backups of home directories and departmental shares are generally taken for disaster recovery purposes. Hence they do not provide security against accidental deletion of individual files. In any case a file which is accidentally deleted on the same day that it has been created or modified will not have been backed up in its latest form.
It is the responsibility of employees to keep individual server user home folders and e.g. departmental share(s)minimal, clutter free and organized. Appropriate measures might need to be applied, for example introducing disk quotas, on troublesome users in order to counter excessive backup clutter especially if it fails to show any sign of abating.
Temporary shares (on disks) and File Transfer Protocol (FTP) servers will not be backed up as they are only used to transfer files not to store files.

How to properly dispose of old backups, archives (and hard drives).

Most people believe that when a file is deleted, it is permanently and irrecoverably erased but this isn't the case. Not only can data still exist in its entirety on the user's hard drive even after repartitions and reformats, but the evidence that certain files once existed on the user's machine could also still be intact. It should however be noted that the I.T department cannot be held responsible for being able to recover this type of data loss.
While this can be useful in data recovery operations after accidental deletions etc, the potential of near instant availability of this information to irrelevant 3rd parties running data recovery tools on the once 'permanently erased' (sensitive) hardware should not at all be possible.
Obviously, this poses significant security problems when disposing of old hardware. To ensure that all disposed files have been permanently deleted beyond all possible techniques of recovery, utilities like (Active Kill Disk 2.0, Drive Scrubber 2.0a professional, system Shield etc) that conform to the US Department of Defense (DoD) clearing and sanitizing standard (5220.22-M) should be used. These tools will over-write and re-write all file allocation tables (FATs) as well as directories and data areas on the hard drive with 1s and 0s. Tape media can be made beyond use through incineration. CDs etc can also be incinerated or badly scratched.

E-MAIL & INTERNET POLICY

CONTENTS.

III. Legal Issues.

Introduction
Bullying and Harassment
Breach of Copyright
Unwanted Contracts
Defamation
Obscene Materials
Protection of Personal Data

INTRODUCTION

Perhaps no area of computer policy is more important than an email policy. In the modern connected world, email messages are often substituted for telephone calls, memorandums, and letters. Email messages are generally informal and as a result, people often write things in an email that they would never consider writing in a memorandum or letter.
Potential problem with employee use of email is the possibility of an employee unwittingly committing the organization to a course of action (purchase, sale, etc.) that they are not actually authorized to do. An example would be an email that is "signed" by including the author's name can be considered a legally binding document. However employees can place a disclaimer at the bottom of their email message stating that nothing contained in the email is to be considered as a contract. Employees may be required to include a statement in their signature line that delineates their lack of authority to enter into agreements on behalf of the organization.
greatest threat to an organization's computers comes in the form of computer viruses and worms. These bits of hostile programming code are often delivered via email, exploiting advanced features of email client software. Email attacks can cause immeasurable losses to organizations around the world by clogging email servers, destroying files, and wasting employee time in dealing with them.
is important to know that security updates for the email client as well as the antivirus software used on each workstation scans incoming email. The mail server is in-house, and contains email server antivirus software packages as an additional safeguard. This is another reason for not allowing personal email accounts; a virus or worm could slip into the network by bypassing security mechanisms established on the organization's email accounts.
Need to be clear about the following:
May be reviewed at any time by the employer
Email may be produced to third parties to comply with laws or regulations.
(i.e. in response to a law enforcement search warrant, or in response to a
Discovery request in civil litigation, etc.)
Even when emails are deleted copies may remain
Marking an email as "private" does not necessarily ensure privacy
Encrypting an email does not does not necessarily ensure privacy

MAIL POLICY

The email system is a means of sending and receiving electronic mail (email), including internal email and internet email. Confidential information includes information associated with Islamic Relief in any way. This includes:
Client/customer lists
Employee lists
Business projections
Business plans
Proprietary processes
Information on research and development
Pending sales
Pending purchases
Pending contracts
Production costs
Production schedules
Design drawings
Company financial information
The following policy applies to any persons having access to the Islamic Relief email system:

Relief's email system is to be used for business purposes only; no personal use of the email system is permissible.
Email created, sent, or received via Islamic Relief computers, networks, and/or email systems are the property of Islamic Relief. Islamic Relief reserves the right to monitor and/or review, at any time, any email created, sent, or received via Islamic Relief's computers, networks, and/or email systems. Relief further reserves the right to reveal the contents of such email to any party that it deems appropriate. The use of encryption, the labeling of an email as private, the deletion of an email, or any other such process or action, does not diminish Islamic Relief's rights in any manner.

Islamic Relief will disclose email to any party that it may be required to by law or regulation. This may include law enforcement search warrants and discovery requests in civil proceedings. Copies of deleted email messages however may still remain on servers and backup tapes.
Emails that are addressed to any person(s) outside of Islamic Relief will have a standard disclaimer at the bottom of the text, stating "Nothing contained in this email is intended to be an offer to commit Islamic Relief to any purchase, sale, contract, or other course of action." This does not apply to emails written by users who are authorized to enter into agreements on behalf of Islamic Relief when the email is part of an authorized course of business.
Emails that are addressed to any person(s) outside of Islamic Relief will clearly identify the user by full name and official title. The user's telephone number may also be included.
to the potential for security breaches, users will exercise extreme caution in downloading and executing any files attached to email. If the attachment is not clearly business related and/or expected from a known source, it should never be opened or executed. Such emails and attachments should be deleted immediately or forwarded to the IT Department as there may be a risk of viruses. Users will not subscribe to any email lists that are not directly relevant to their assigned duties.
That is treated as private or confidential will never be emailed to persons outside of the Islamic Relief unless:
The email transmission is expressly approved, in advance, by an authorized person or the confidential information is encrypted.
The email text includes a warning to the recipient that the material is private and confidential and is the property of Islamic Relief
The email text contains a specific statement of why the recipient is receiving it, what they may do with the information, and who, if any one, they may disclose it to and that a copy of the email is permanently archived by the user.
Each user is responsible for ensuring that their use of the Islamic Relief email system is consistent with this policy and any other applicable organization's policy, and appropriate business practices.
shall not contain jokes, pornography, sexist remarks, racist remarks, defamatory remarks, obscene remarks, anything of a commercial nature not related to Islamic Relief business, anything of a political nature, or any other inappropriate remarks. The email system shall not be used for any purpose in violation of the organization's other policies.
than those specifically assigned or approved by the IT Department, using Islamic Relief owned computer assets to access any email account or service by a user is expressly forbidden.
Users will not reveal their email passwords to anyone. Excluding members of the IT Department in the course of their assigned duties, users will not use or access email accounts belonging to any other user in the organization.

RULES PERTAINING TO INTERNET AND EMAIL USE

Permitted and Prohibited uses

E-mail is only permitted for business use. Business use means that the message must be directly related to Islamic Relief's objectives, working practices and goals. Staff is not allowed to use e-mail for personal purposes.
Staff should only access the World Wide Web (Internet) if such use is required as part of their. Staff must not under any circumstances use any chat lines, messenger providers or bulletin boards on the internet during working hours. The internet must not be used at any time for gambling activity.
Failure to adhere to these rules will be treated as a serious disciplinary matter which may lead to dismissal.

Offensive, Illegal and Defamatory Materials

IR staff must not under any circumstances use Islamic Relief's e-mail system or internet accessibility to access, download, send, receive or view any materials that will cause offence to any person by reason of :
any sexual explicit content
any sexist remarks
any racist remarks
any political opinions
any remarks relating to a person's sexual orientation, or gender reassignment
any remarks relating to a person's religious beliefs
any remarks relating to a person's disability
any remarks relating to a person's age
Islamic Relief's Equal Opportunity Policy applies to e-mail communication and must be complied with.
Staff must not under any circumstances use Islamic Relief's e-mail system or internet accessibility to access, download, send, receive or view any materials that are, are suspected to be:
Illegal
Contrary to public policy
Unlawful
Note: It may be illegal to copy many materials appearing on the internet including computer programs, music, text and video clips. If it is not clear whether permission is granted to copy materials off the internet, then staff are urged do so.
Staff must not attempt to post any material on Islamic Relief's official web site.

Staff must not send or circulate any materials on the internet or by e-mail that contain any defamatory, or otherwise negative remarks about other persons or organizations unless it is guaranteed that the material is factually correct. If in any doubt, do not send it.
Any use of Islamic Relief's e-mail system or internet accessibility for any of these prohibited purposes will be treated as a serious disciplinary matter which may lead to dismissal of the employee concerned.

Monitoring

Islamic Relief reserve the right to monitor and inspect all e-mails sent by staff using the e-mail system.Such monitoring is intended to ensure that this Policy is being adhered to and is effective and that Islamic Relief and its employees are acting lawfully. It is imperative that Islamic Relief remains beyond reproach.
Staff should therefore have no expectation of privacy when using Islamic Relief's e-mail system. Other methods of communication should be used for any private messages.
All connections to the internet throughout the computer network from Islamic Relief are monitored and recorded in log files.Such monitoring of internet usage is solely to ensure that this Policy is being adhered to and that Islamic Relief and its employees are acting lawfully. These log files record information of which internet web site has been accessed, detailing site address, date, time and by whom. They are checked on a regular basis.

Confidentiality and Sensitive Information.

It is important to remember that e-mails are not necessarily a secure way of sending information. If staff want to use e-mail to send any information which is highly confidential (i.e. it could cause Islamic Relief loss or embarrassment if it were publicly disclosed or fell into wrong hands), then the following rules apply:
Such information must be encrypted. Please contact I.T. Services who will be able to advise on encryption methods.
Obtain authorization from your line manager.
Following extracts of information will be treated as highly confidential:
Extracts from Islamic Relief's various databases
Personnel Records
Payroll Records
Legal Records
All information received under a duty of professional confidence from a client / partnership / professional organization.

All e-mails must contain the Islamic Relief standard notice containing a confidentiality statement, organizational information and a disclaimer. A copy of this notice is available form the Support Division and any person using the e-mail system that currently does not have this notice is encouraged to obtain it. This notice should not be removed in any circumstances.
Any failure to follow these rules may lead disciplinary action which may result in dismissal.
Staff should also be aware that e-mail messages, like paper based documents, can be required to be produced in legal proceedings. Staff, who would not like an e-mail to be produced in a court of law, should refrain from using e-mail.

Viruses

Non-text e-mail attachments (e.g. software, computer games, executable files, music and bitmaps / jpegs) and software downloaded from the internet may contain computer viruses or other harmful content which can seriously disrupt Islamic Relief's computer system.
IR staff must not open, download or copy any non-text e-mail attachments or software from the internet unless they have been checked for viruses or other harmful content by the I.T. Department.
All computers should have been installed with anti virus software, but sometimes the software is not adequate to prevent viruses or other harmful content getting onto computers.
It is highly recommended that staff adjust individual settings on their computer's e-mail application so that in the "in box" the "Preview Pane" is not active. If employees are unsure or do not know how to do this then they should contact I.T. Services who will either advise on how to do this or will in fact do it themselves.
Failure to adhere to these rules will be treated as a serious disciplinary matter which may result in dismissal.
Any employee who knowingly distributes a computer virus or any harmful code using Islamic Relief's e-mail system will be subject to disciplinary action which in turn may result in dismissal.

Security

Staff must not in any circumstances disclose their passwords to any other employees within Islamic Relief, with the sole exception of their immediate line manager.
Staff must not impersonate any other employee when sending an e-mail and must not amend messages received – there is always the original copy.
Individual members of staff are responsible for the security of their computer and e-mail box and must not allow them to be used by any unauthorized person.
Failure to adhere to these rules will be treated as a serious disciplinary matter which may result in dismissal.

Housekeeping

The following rules will enable Islamic Relief's systems to work more efficiently and so need to be adhered to at all times:
All important e-mail messages must be printed off and filed or stored electronically in a secure file on individual computers.
Always obtain confirmation from the recipient that an important e-mail has been received.
If a member of staff receives a wrongly delivered message it should be re-directed to the intended person if known, otherwise it should be returned to the originator with a brief explanation. If the e-mail contains confidential information that information and must not be disclosed.
Messages should be deleted on a regular basis or stored in a suitable electronic file on individual computers, this ensures adequate storage space is maintained on the mail server.
Staff should not subscribe to e-mail services which will result in e-mails being sent automatically unless these are useful for their particular job.
Trivial or personal e-mail messages should not be sent. These lead to congestion of the e-mail system and reduce its efficiency.
Remember. Treat e-mail in the same way as you would treat a letter or a fax. Do not e-mail a message that you would not shout out in a crowded room or that you would not want read out in a court of law.

ISSUES

Introduction.

This section of the Policy is intended to give employees guidelines on the most important legal issues which may arise from the use of Islamic Relief's e-mail system and internet accessibility.
It is very important that staff read this section to understand the relevant issues as this will help IR employees and Islamic Relief avoid problems.
These are not just theoretical issues. If the law is broken then this could result in one or more of the following consequences:
Civil and / or criminal liability for staff members and Islamic Relief.
Disciplinary action against staff members including dismissal.

Bullying and Harassment

Islamic Relief intends that all employees are treated with dignity at work, free from harassment and bullying of any kind. Harassment can take the form of general bullying, or be manifest on the grounds of sex, race, disability, sexual orientation, age or religion. Harassment could include sending sexist or racist jokes, making sexual propositions or general abuse by e-mail. Staff must not send any messages containing such material. Bullying and Harassment of any kind will be treated as a serious disciplinary matter which may lead to dismissal.
If a member of staff is subjected to or knows about any harassment or bullying, whether it comes from inside or outside Islamic Relief, they are encouraged to follow the Grievance Procedure outlined in Section 4.1.20, and should report the incident immediately.

Breach of Copyright

Materials encountered on the internet or received by e-mail are likely to be protected by copyright.This will apply to written materials, software, music recordings, graphics and artwork and video clips.
Only the owner of the copyright, or other persons who have the owner's consent, can copy those materials or distribute them.
If any such materials copy are amended or distributed by staff members without the copyright owner's consent, then they may be sued for damages by the copyright owner. Islamic Relief may also be liable and, in some circumstances, criminal liability can arise for both the staff member and Islamic Relief.
Particular care should be taken not to copy text or download software or music unless there is certainty that is permitted. Staff should always check the materials in question to see if they contain any written prohibitions or permissions before being copied or download.
Staff should never download any software, music recordings or other materials that are known to be fakes or "pirate copies".
Failure to follow the Policy's rules will be treated as a serious disciplinary matter which could lead to dismissal.

Unwanted Contracts

An exchange of e-mail messages can lead to a contract being formed between the sender or Islamic Relief, and the recipient. Contracts can arise easily; all that is required is the acceptance of an offer with the intention that legal obligations should arise and some payment or other consideration should be made for the performance of those obligations. Breach of contract can expose Islamic Relief to a claim for damages.
Contracting by e-mail is subject to the same requirements as any other form of contract. Staff must adhere to Islamic Relief's established policies and procedures about purchasing and contracting.
Staff should never commit Islamic Relief to any obligation by e-mail without ensuring that they have the authority to do so.If employees have any concerns that what they are doing will form a contract, then the Support Division's legal representative should be contacted. All e-mails relating to contractual negotiations should be marked "Subject to Contract".
Members of staff should also ensure that any person with whom they wish to enter into a contract is adequately identified and authorized to do so. All e-mail contracts will require the use of digital signature technology to ensure that identity is affirmed and to ensure the integrity of the content of the contract. For guidance and advice, contact I.T. Services on the use of digital signatures.
Any contract entered into via e-mail must contain the following statement:

"Any contract formed by this e-mail will be governed and construed in accordance with the laws of England and the parties submit to the non-exclusive jurisdiction of the English courts".
Beware of any attempt by third party with whom you are dealing to incorporate its own terms and conditions into a contract.
to follow the Policy's rules will be treated as a serious disciplinary matter which could lead to dismissal.

Defamation

Sending an e-mail (even an internal e-mail) or posting any information on the internet, which contains remarks which may adversely affect the reputation of another organization or person, will expose both the staff member and Islamic Relief to the risk of legal action for defamation.
This is a real risk. Other companies have been sued for the defamatory contents of e-mails sent by employees and have been required to pay out considerable sums of money as a result.
to follow the Policy's rules will be treated as a serious disciplinary matter which could lead to dismissal.

Obscene Materials

Staff must not under any circumstances use Islamic Relief's e-mail system or internet accessibility to access, display, circulate or transmit any material with a sexual, or otherwise obscene or unlawful content. This may constitute a criminal offence and both Islamic Relief and the member of staff personally could be liable. Sexual Harassment will be treated as a serious disciplinary matter which may lead to dismissal.
The display on screen of material with a sexual content and / or its transmission to another may amount to sexual harassment which will be treated as a serious disciplinary matter which may lead to dismissal.

Protection of Personal Data

Please note that Islamic Relief is required to comply with legislation concerning the protection of personal data.Failure by Islamic Relief to adhere to that legislation could expose Islamic Relief to civil liability and enforcement action by the data protection authorities.
Obligations of Islamic Relief under that legislation are complex but employees can help ensure compliance by adhering to the following rules:
Do not disclose any information about a person in an e-mail or on the internet which you would object to being disclosed about yourself.
Be particularly careful when dealing with information concerning a person's racial or ethnic origin, sexual life, political beliefs, union memberships, religious beliefs, physical or mental health, financial matters and criminal offences.
Do not send any personal data outside the European Union.
Islamic Relief reserves the right to modify this Policy having given reasonable notice.
Failure to follow these rules may lead to disciplinary action including dismissal.

DECLARATION OF ACKNOWLEDGEMENT CONFIRMATION

Employee Name: …….

Department: …….

I have read, I understand and I accept Islamic Relief's E-mail & Internet Policy.

I acknowledge that any breach of this policy could result in disciplinary action being brought against me, which could include my dismissal.
I also understand that I may be reported to the police for any criminal offence that arises out of such breach.

Signed: …….

Dated: ……