DONE FOR YOU
SAMPLE
INTERNET ACCEPTABLE USE POLICY

An Educational EXAMPLE Guide By:
DPC Technology

Published By:
DPC Technology
7845 Baymeadows Way
Jacksonville, FL 32256
USA

Disclaimer and Legal Notices:
While all attempts have been made to verify the information provided in this book and accompanying presentation, neither the Author nor the Publisher assumes any responsibility for errors, inaccuracies, or omissions. Before implementing the strategies outlined within, you must be aware of the various laws governing business transactions, marketing, employment law or other business practices in your particular geographic location as some of the suggestions made in this book and seminar program may have inadvertently introduced practices deemed unlawful in certain states, municipalities, and countries. This document is not intended for use as a source of legal, employment, labor or accounting advice. In all case, you should consult the services of a professional, licensed attorney in all matters pertaining to the operation, delivery, and legal requirements of your business and services.

Policy Area	
Approved Date	
Approved By	
Effective Date	
Current Version	1.0

I. Overview

Information systems are a growing and important resource for CLIENT NAME Staff, one that can provide critical competitive advantage to CLIENT NAME in the form of information gathering, improved external communications, and increased ability to make decisions regarding fundraising and investments. It is important that CLIENT NAME Staff understand and agree on the appropriate procedures to protect CLIENT NAME's assets.

II. Purpose

This policy provides useful tips and techniques to promote effective use of CLIENT NAME's Information Systems. It applies to all CLIENT NAME systems located on or accessed from CLIENT NAME property and systems provided by CLIENT NAME for use in CLIENT NAME business.

III. Scope

This policy applies to all CLIENT NAME Staff that have access to CLIENT NAME's Information Resources.

IV. Policy

CLIENT NAME utilizes sophisticated computer and communications systems to assist Staff in performing their job functions. These technologies support our business activities by enabling closer, more effective and timely communications among personnel within the CLIENT NAME and with our customers, partners and vendors. These guidelines advise all users regarding the access to and the disclosure of Information Systems. These guidelines establish the CLIENT NAME's expectations for all Staff concerning the disclosure of information via CLIENT NAME's Information Systems.

CLIENT NAME maintains and uses many facilities, equipment, and communication systems, such as telephones, regular mail, special delivery services, E-mail, voice mail, fax machines, computers, etc., designed to make the CLIENT NAME's operations effective and efficient. CLIENT NAME's Information Systems are provided to Staff at CLIENT NAME expense to assist Staff in carrying out CLIENT NAME business. Some of these systems permit Staff to communicate with each other internally and with other parties externally. As with all CLIENT NAME assets, CLIENT NAME's Information Systems are for official CLIENT NAME business only. Access to CLIENT NAME Information Systems is provided in conjunction with the official CLIENT NAME business and individual job responsibilities. Use of CLIENT NAME's Information Systems is subject to these policies and guidelines and other relevant CLIENT NAME policies and procedures.

A. Information Access, Content, and Use

The CLIENT NAME makes every effort to provide its Staff with the best technology available to conduct the CLIENT NAME's official business. The CLIENT NAME has installed, at substantial expense, Information Resources to conduct its official business.

This document addresses general Information Systems policies and guidelines, specific issues related to appropriate content, and Staff use of CLIENT NAME's Information Systems. All departments and Staff are required to follow these general policies and guidelines. All CLIENT NAME Staff with access to CLIENT NAME's Information Systems are required to read, understand and comply with CLIENT NAME's policies.

CLIENT NAME's Information Systems are owned by CLIENT NAME and are to be used for business purposes only in serving the interests of CLIENT NAME's customers and in the course of normal business operations.

The use of CLIENT NAME facilities, property, equipment, or communication systems is limited to Acceptable Use as defined in these policies and guidelines. No CLIENT NAME equipment or communications systems, including all hardware and software, may be removed from CLIENT NAME property without prior express consent of the CLIENT NAME.

Personal equipment, including all computer hardware and software, may not be brought onto CLIENT NAME premises or be used for CLIENT NAME's official business without the prior express consent of the CLIENT NAME. Staff are not to use their personal accounts during work hours or use CLIENT NAME equipment to reach personal sites unless it is for legitimate business purposes, as determined solely by CLIENT NAME.

CLIENT NAME encourages the use of CLIENT NAME's Information Systems for business when such business can be accomplished consistent with the following policies and guidelines identified in this document. When using Information Systems, Staff shall conduct official CLIENT NAME business consistent with the CLIENT NAME's mission statement. Official CLIENT NAME business shall comply with all federal and state statutory requirements as well as standards for integrity, accountability, and legal sufficiency. Thus, official CLIENT NAME business conducted via the Internet should meet or exceed the standards of performance for traditional methods (e.g. meetings, use of telephone).

Staff shall base decisions to use CLIENT NAME's Information Systems on sound business practices. The conduct of business using CLIENT NAME's Information Systems is particularly compelling where costs are reduced and/or the services provided by the CLIENT NAME are improved in measurable ways. When using CLIENT NAME's Information Systems, CLIENT NAME Staff shall promote and maintain a professional image.

CLIENT NAME Staff shall disseminate information that is current, accurate, complete, and consistent with CLIENT NAME policy. Information released via CLIENT NAME's Information Systems is subject to the same official CLIENT NAME policies for the release of information via other media (such as printed documents), so that the information disclosed avoids potential problems with copyrights, trademarks, and trade secrets. Information accuracy is particularly important.

CLIENT NAME Staff shall protect confidential and proprietary information entrusted to the CLIENT NAME. Questions regarding confidential or proprietary information should be directed to CLIENT NAME management or his/her designee.

B. Protecting Confidential Information

Maintaining the confidentiality of sensitive information is crucial to CLIENT NAME's success. Confidential information stored on or carried over CLIENT NAME's Information Systems could become the subject of accidental or intentional interception, mis-delivery, hacking or even unauthorized internal review unless Staff take the necessary precautions outlined in these guidelines.

Staff should exercise care when communicating any potentially confidential information outside of CLIENT NAME, as no electronic communications facility is completely secure.

Data shall be classified per the Data Classification Policy. All confidential data should be marked with "Confidential," "Do not reproduce," "Not to be reproduced without approval," or "Do not forward." All E-mail messages containing confidential information should contain "Confidential" in the subject header.

Some directories in the CLIENT NAME's Information Systems contain sensitive or confidential data. Access to these directories shall be restricted. Unauthorized attempts to circumvent such access restrictions are violations of these Guidelines and may result in disciplinary action, up to and including termination of employment, and legal action.

Staff must refrain from entering into discussions with third parties regarding the CLIENT NAME's business prospects, investments, investors, or financial condition. Such information is proprietary to CLIENT NAME and constitutes valuable information that should be protected as a trade secret. The release of such information could become the subject of criminal prosecution.

Staff are asked to respect the privacy of individuals who send them messages. Staff should protect voice mail, and E-mail accounts from unauthorized access. Appropriate protection procedures include ensuring proper password protection to these accounts, closing E-mail messages after reading them and deleting all messages when they are no longer needed.

Staff shall not place CLIENT NAME material (e.g. copyrighted software, internal correspondence) on any publicly accessible Internet computer without prior permission.

The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third-party. Staff must exercise caution and care when transferring such material in any form.

C. Copyrighted Information

CLIENT NAME respects the intellectual property rights of other companies and individuals. Use of all copyrighted material, including literature, software, and graphics shall comply with relevant, valid license terms. CLIENT NAME's Information Systems may provide access to materials protected by copyright, trademark, patent and trade secret and even export laws. Staff should not assume that merely because information is available on an electronic information system such as

the Internet, that it may be downloaded or further disseminated. No copyrighted material should be copied, transmitted, posted, or otherwise distributed without such compliance. If a question arises as to the propriety of downloading information, CLIENT NAME management should be consulted.

All material trademarked or copyrighted by CLIENT NAME should be marked with the appropriate trademark or copyright designation. No CLIENT NAME Staff should remove trademark and copyright notices from third party material.

CLIENT NAME's license to use software is carefully set forth in legal agreements that CLIENT NAME has with the developers and distributors of the software. Staff's use of software must be in compliance with those agreements. If CLIENT NAME gives Staff the opportunity to use certain software, copying of that software is strictly prohibited. Loading of software of a personal interest is prohibited unless Staff are given prior express consent by CLIENT NAME management. When Staff leave CLIENT NAME, all CLIENT NAME owned software, licenses, and media will remain with CLIENT NAME.

Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, Staff members are prohibited from downloading software and/or modifying any such files without permission from the copyright holder.

D. Privacy Statement

This policy is intended to guide Staff in the performance of their duties. It is also intended to place Staff on notice that Staff should not expect CLIENT NAME's Information Systems and their contents, to be confidential or private. All data, including any that is stored or printed as a document, is subject to audit and review.

No Staff member has a reasonable expectation of personal privacy with respect to the use of any of the CLIENT NAME's facilities, property, equipment or communications systems. This includes anything created or received on CLIENT NAME's Information Systems even if used for business purposes and in the normal course of CLIENT NAME operations.

CLIENT NAME reserves the right, but not the obligation, to monitor use of CLIENT NAME's Information Systems including the Internet, E-mail, computer transmissions, and electronically stored information created or received by CLIENT NAME Staff with the CLIENT NAME's Information Systems. All computer applications, programs, work-related information created or stored by Staff on CLIENT NAME's Information Systems, are CLIENT NAME property.

E. Monitoring and Inspecting Information Systems

CLIENT NAME's Information Systems are provided for official CLIENT NAME business. CLIENT NAME's Information Systems are owned and controlled by the CLIENT NAME and are accessible at all times by the CLIENT NAME for maintenance, upgrades and other business or legal purposes.

All Information Systems, including the messages and data stored on the systems, are and remain at all times the property of CLIENT NAME, subject to applicable third party intellectual property rights such as copyrights. By virtue of continued employment and use of CLIENT NAME systems, all Staff are considered to have consented to monitoring and other access by authorized CLIENT

NAME personnel. CLIENT NAME reserves the right to inspect a Staff member's computer system for violations of CLIENT NAME policies.

CLIENT NAME reserves the right to access and conduct an inspection or search all directories, indices, files, databases, faxes, CLIENT NAME computer hardware and software, voice mail, E-mail and communication systems or deliveries sent to any CLIENT NAME location, and other Information Resources no matter to whom it is addressed, with no prior notice. CLIENT NAME may also cancel or restrict any Staff's privilege to use any or all of its facilities, equipment, property, or communication systems.

If a Staff member refuses to cooperate with a search or inspection for legitimate business purposes that is based on reasonable suspicion that the Staff is in possession of prohibited materials, CLIENT NAME may take that refusal into consideration in determining appropriate disciplinary action. A Staff member's refusal to provide their password to CLIENT NAME management will be considered additional grounds for discipline. Discipline, including termination, will be based on all available information, including the information giving rise to the inspection or search.

Access to on-line services, the Internet, blogs, social media sites, or other communications networks is prohibited unless CLIENT NAME has provided prior express consent. As such, no CLIENT NAME equipment, telephone lines, or on-line services may be used to view or download offensive, discriminatory or pornographic material. Employee use of these services may be monitored to include numbers called and the amount of time spent using the services. CLIENT NAME reserves the right to inspect computer systems for viruses, offensive, discriminatory or pornographic material, personal software, etc.

CLIENT NAME management may examine Staff communications or files and such examination should be expected to occur in various circumstances when necessary, including, but not limited to:

- Ensuring that CLIENT NAME systems are not being used to transmit discriminatory, harassing or offensive messages of any kind.
- Determining the presence of illegal material or unlicensed software.
- Ensuring that communication tools are not being used for unauthorized, disruptive, or improper uses.
- Investigating allegations or indications of impropriety.
- Locating, accessing and/or retrieving information in Staff absence.
- Responding to legal proceedings and court orders in the preservation or production of evidence.
- CLIENT NAME reserves the right to review Staff use of and to inspect all material created by or stored on CLIENT NAME Information Systems. CLIENT NAME reserves the right to monitor all use of Information Systems to access, review, copy, delete, or disclose messages and data derived from any use. All messages or data become property of CLIENT NAME, subject to access, review, duplication, deletion, or disclosure by CLIENT NAME management or by other personnel authorized by CLIENT NAME. Staff should be aware that billing practices, firewall protections, and traffic flow monitoring programs often maintain detailed audit logs setting forth addresses, times, durations, etc. of communications both within and external to the CLIENT NAME. Staff should treat CLIENT NAME's Information Systems with the expectation that communications will be

available for review by authorized personnel of CLIENT NAME for legitimate business purposes at any time.

CLIENT NAME reserves the right to access, review, duplicate, delete or disclose for legitimate business purposes any communications, messages or data derived from use of CLIENT NAME's Information Systems.

F. Storing and Archiving Information

CLIENT NAME has developed specific archival procedures to ensure the safe retention of electronic data. Most files are subject to routine back-up procedures. Copies of documents and electronic messages may be retained for long periods of time. By virtue of various archival practices employed at CLIENT NAME, any messages or data stored, even temporarily, on CLIENT NAME Information Systems may be copied to magnetic or other storage media without the specific knowledge of the individual creating the messages or data. Such archives are and remain CLIENT NAME property and may be used by the CLIENT NAME for any business purpose. Simply deleting messages or data from these Information Systems does not provide privacy with regard to such messages or data. The length of time that such archives may be maintained can be almost indefinite. Staff may be required to preserve their electronic data based on pending litigation and/or investigations by the CLIENT NAME. Refer to the Data Retention Policy for more information on storing and archiving information.

G. Employee Usage

Each Staff has the responsibility of complying with CLIENT NAME's policies and guidelines provided in this document. Failure to do so may result in disciplinary action, up to and including termination of employment and legal action.

The use of Information Systems is restricted to official CLIENT NAME business. Personal use of or time spent for personal gain is strictly prohibited unless CLIENT NAME gives prior express consent. Inappropriate personal use includes the creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials, materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited. In addition, any Internet use that could cause congestion, disruption of normal service, or general additional CLIENT NAME expense is prohibited.

Hacking or unauthorized attempts or entry into any other computer is forbidden. Such an action is a violation of the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2510.

Sending threatening, slanderous, racially and/or sexually harassing messages is strictly prohibited. The representation of yourself as someone else, real or fictional, or a message sent anonymously is prohibited.

Staff should be aware that CLIENT NAME's Information Systems and the World Wide Web are not censored and contain information some users may find offensive. CLIENT NAME cannot

accept responsibility for what the Staff accesses. However, if offensive material is accessed, Staff shall disengage from the material immediately.

Staff shall not copy or transfer electronic files without prior CLIENT NAME permission. Almost all software is subject to Federal copyright laws. Care should be exercised whenever accessing or copying any information that does not belong to the Staff. When in doubt, consult CLIENT NAME management. Unauthorized or illegal use of third-party intellectual property is prohibited. Such use includes, but is not limited to, downloading or using copyrighted or patented software, video and audio clips or documents on CLIENT NAME's Information Systems in a manner inconsistent with relevant license terms or other intellectual property rights.

Downloading a file from the Internet can infect CLIENT NAME's systems with a virus. Staff shall not circumvent or disable CLIENT NAME standard virus prevention software and/or Information Resource security mechanisms.

Staff shall not send post or provide access to any confidential CLIENT NAME materials or information to anyone outside of CLIENT NAME.

Staff are obligated to cooperate with any investigation regarding the use of Staff computer equipment and which CLIENT NAME management has authorized.

Alternate Internet Service Provider connections to CLIENT NAME's internal network are not permitted unless prior express consent has been given by CLIENT NAME management and properly protected by a firewall or other appropriate security device(s).

If Staff are using information from an Internet site for strategic official CLIENT NAME business decisions, Staff should verify the integrity of that information. Staff should verify whether the site is updated on a regular basis (the lack of revision date might indicate out-of-date information) and that it is a valid provider of the information.

CLIENT NAME has no control or responsibility for content on an external server not under the control of the CLIENT NAME. Information may be offensive and/or unsuitable for dissemination.

Do not upload or download large files during prime hours due to the network impact on other users. Information Systems may have limits regarding disk space usage. Documents take up space; therefore, Staff should regularly delete and/or archive any files Staff wish to save.

Staff using CLIENT NAME's accounts are acting as representatives of the CLIENT NAME. As such, Staff should act accordingly so as not to damage the reputation of CLIENT NAME.

H. Information Systems Awareness

The use of Information Systems is the responsibility of each Staff. The practices listed below are not inclusive, but rather designed to remind each Staff of the need to raise their Information Systems awareness.

- Protect equipment. Keep it in a secure environment and keep food and drink from electronic systems. Know where the fire suppression equipment is located and how to use it in an emergency.
- Protect areas. Keep unauthorized people away from equipment and data. Challenge strangers in the area

- Protect passwords. Never write it down or give it to anyone. Don't use names, numbers or dates that are personally identified with the Staff. Change the password often and change it immediately if it has been compromised.
- Protect files. Don't allow unauthorized access to Staff files and data. Never leave equipment unattended with the password activated – log off.
- Backing up data. Keep duplicates of critical data in a safe place.
- Report security violations. Staff should tell their supervisor or CLIENT NAME management if Staff see any unauthorized changes to Staff data. Immediately report any loss of data or programs, whether automated or hard copy to the CFO and the IT Vendor.

I. Electronic Mail (E-mail) and Etiquette

E-mail may be sent through each Staff's computer. E-mail will be sent for official CLIENT NAME business only. No personal E-mail shall be sent or received via CLIENT NAME Internet accounts.

CLIENT NAME Staff should not attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading. Management reserves the right, but not the obligation, to access all E-mail files created, received or stored on CLIENT NAME-funded systems and such files can be accessed without prior notification.

CLIENT NAME Staff are expected to maintain their E-mail accounts on a regular basis. This entails deleting E-mail once it has been read or sent. Excess E-mail takes up unnecessary storage space on the server and may cause the entire system to run slowly.

E-mail requires extensive network capacity. Sending unnecessary E-mail, or not exercising constraint when sending very large files, or sending to a large number of recipients consumes network resources that are needed for critical official CLIENT NAME business. When CLIENT NAME grants an individual Staff access to the network, it is the responsibility of Staff to be cognizant and respectful of network resources.

E-mail users are to exercise good judgment and common sense when creating and distributing messages. E-mail is the property of the CLIENT NAME and is to be used exclusively for official CLIENT NAME business. No Staff E-mail is considered private. Similarly, the accessing, reading or copying of E-mail not intended for a Staff member's eyes is prohibited. Staff are strictly prohibited from sending E-mail messages of a harassing, intimidating, offensive or discriminatory nature. Anonymous messages are not to be sent. Staff are prohibited from using aliases while connected to services. CLIENT NAME retains the right to access a Staff member's E-mail at any time for any reason without notice to the Staff. Conduct in violation of this policy will subject any Staff to CLIENT NAME's disciplinary procedures.

Each CLIENT NAME Information System may allow Staff to set or change their password. If so, set the password and change it regularly. Guidelines for choosing and setting passwords should be obtained from the Password Policy. Periodic password changes keep undetected intruders from continuously using the password of a legitimate user. After logging on, the computer will attribute all activity to a Staff member's user id. Therefore, never leave workstations without logging off -- even for a few minutes. Always log off or otherwise inactivate the workstation so no one could perform any activity under Staff's user id when away from the area. Staff should safeguard sensitive information from disclosure to others.

If requested, Staff shall disclose their passwords (e.g. voice mail, E-mail, relevant Internet web site passwords) to their supervisor and/or manager. Staff must maintain secure passwords and never use an account assigned to another user.

CLIENT NAME reserves the right to override the user's password and other security features when it has a need to do so. Should a time come when Staff leaves the CLIENT NAME, or at any other appropriate time, the CLIENT NAME may replace Staff's password with another of the CLIENT NAME's choosing.

K. Protecting Information Systems From Viruses

CLIENT NAME provides virus protection software to help safeguard Information Systems. These systems are not totally foolproof. As such, be particularly cautious when opening any E-mail with an attachment.

Staff shall not disable or remove anti-virus software. Viruses can infect executable files, disk boot sectors, documents, etc. If a virus is received from a sender, that sender should be notified that the file was infected and if possible the type of virus should be identified.

L. Encrypting Data

Only authorized encryption tools (both software and hardware) may be used in connection with Information Systems. Except with the prior written consent of CLIENT NAME management, all encryption tools must permit the CLIENT NAME to access and recover all encrypted information.

If documents are saved to a portal media device (i.e. laptops, USB drives, mobile devices). The device must have an encrypted hard drives. Drive encryption is the best way to ensure the protection of sensitive data should a mobile device be lost or stolen.

M. Securing Mobile Computing Devices

Staff who use CLIENT NAME mobile computing resources (laptops, hand held devices, etc.) must take adequate precautions to ensure that proprietary information contained in such devices is secure and not available to third parties, particularly during travel. Staff are responsible for taking adequate precautions against theft of their mobile computing devices. Please refer to the Bring Your Own Device and Technology Policy for more information.

N. Acceptable Use

- Authorized Use. The authorized use of CLIENT NAME systems is limited to CLIENT NAME's official business. The CLIENT NAME provides Information Systems and communication tools to facilitate business communication and enhance personal productivity. CLIENT NAME reserves the right to prohibit or restrict use of CLIENT NAME systems for any other purpose and at any time.
- Incidental Personal Use. Personal use of CLIENT NAME systems is permitted so long as it is not excessive as determined by the CLIENT NAME, does not interfere with job performance, consume significant resources, or interfere with the activities of other Staff.

O. Unacceptable Use

- Unauthorized Use. Excessive personal and other use of Information Systems inconsistent with this or any other CLIENT NAME policy is unauthorized. Under no

circumstances are CLIENT NAME's Information Systems to be used for personal financial gain or to solicit others for activities unrelated to official CLIENT NAME business, such as solicitations for personal, political, or religious causes. Installation of software without approval from CLIENT NAME management is unauthorized.

- Disruptive Use. Use that may reasonably be considered offensive or disruptive to any individual or organization, or to harmony within the workplace is prohibited. Such disruptive use includes, but is not limited to, transmission, retrieval, storage, or display of defamatory, obscene, offensive, politically motivated, slanderous, harassing, or illegal data, or messages that disclose personal information without authorization. Grossly indiscriminate or "broad band" distribution of E-mail would clearly constitute a disruptive use.
- Prohibited use. Unauthorized or illegal use of third-party intellectual property is prohibited. Such use includes, but is not limited to, downloading or using copyrighted or patented software, video and audio clips or documents on Information Systems in a manner inconsistent with relevant license terms or other intellectual property rights. When in doubt about the existence or scope of a license or about appropriate use of copyrighted, patented, or otherwise proprietary third-party data or software code, Staff should contact CLIENT NAME management. Staff are expressly prohibited from using CLIENT NAME's Information Systems to store or access pornography.

Only DPC Technology is authorized to install software on servers, storage, and other related Information Resources.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Acceptance

I have read CLIENT NAME's Acceptable Use Policy and agree to abide by it as consideration for my continued employment by CLIENT NAME. I understand that violation of the enclosed policies and guidelines may result in disciplinary action including, but not limited to, termination.

This document supersedes all prior electronic equipment policies, guidelines, understandings and representations. I understand that if any of the provisions of this manual are found null, void, or inoperative for any reason, the remaining policies and guidelines will remain in full force and effect.

If I am uncertain about any policy or procedure, I will check with my immediate supervisor or Company management.

_____ _____
Employee Signature Date

_____
Employee Name (Printed)