
# 306:Dealing with Employee Lifestyle Issues

**Andrea L. Phillips**
*Legal Counsel*
Rolls-Royce North America Inc.

**Richard G. Torra**
*Associate General Counsel*
Investors Bank & Trust Company

# Faculty Biographies

**Andrea L. Phillips**

Andrea L. Phillips is employment counsel for Rolls-Royce, North America, a global provider of power generation services on land, sea, and air with headquarters in Chantilly, Virginia. Her responsibilities include handling all U.S. employment matters, including conducting investigations, providing training and responding to EEO charges, advising on FMLA, ADA, harassment and discrimination issues, among others.

Prior to joining Rolls-Royce, Ms. Phillips was a trial attorney with the U.S. Department of Labor-Office of the Solicitor in Chicago. Her responsibilities included litigating wage and hour disputes, Occupational Safety & Health (OSHA), and FMLA issues. Before becoming in-house counsel, Ms. Phillips also worked as a litigation/labor associate at law firms in New York and Chicago.

In addition to ACCA, Ms. Phillips is a member of the ABA-Labor & Employment Division.

Ms. Phillips received her BA from Oberlin College in Oberlin, Ohio and her JD from Harvard Law School in Cambridge, Massachusetts.

**Richard G. Torra**
*Associate General Counsel*
Investors Bank & Trust Company

 

# SAMPLE POLICIES:

# EMPLOYEE LIFESTYLE ISSUES

 

***Please note, this document is being provided as general business advice and should not be construed as legal advice. Further, this document is "sample language" only, it should not be considered a best practice. Note, many of the provisions within this document may not be applicable to your company. We strongly recommend that the reader seek legal advice from their own attorneys in connection with drafting of codes, guidelines, policies or releases specific to their organization.***

# SAMPLE - COMPANY GUIDELINES FOR ATTIRE

## *[SAMPLE - 1]*

We strive to create a comfortable work environment for our employees, while maintaining a professional business climate for our customers, suppliers and guests. These guidelines are meant to assist employees in presenting a positive, business-like image through neat, clean and professional appearance. Certain departments or business units may determine the need for different attire. The respective function or business leader will make the determination. [*The last page contains photos that give examples of appropriate attire.*]

- Employee may wear business casual clothing.
- No spandex or jogging pants. Slacks and khakis are appropriate.
- Casual shirts and blouses that present a "professional" appearance are acceptable. T-shirts, tank tops or halters are not appropriate. Shirts with printed messages or advertisement that may be offensive to others are not to be worn.
- Casual skirts and pants are acceptable. Shorts, denim pants or jeans are not appropriate.
- No clothes with patches and/or holes are acceptable.
- Comfortable shoes that coordinate with overall attire are appropriate, including dress sandals, as long as they are clean, conservative and in good condition. Athletic shoes are not allowed. Sandals and open-toed shoes are not permitted in the manufacturing and shop areas.
- Safety glasses must be worn in all plant areas except cafeterias, break malls, first-aid stations and enclosed office areas.
- Sleeveless shirts and dresses are appropriate, but backless, strapless or tight-fitting clothing is not allowed.

 

***Please note, this document is being provided as general business advice and should not be construed as legal advice. Further, this document is "sample language" only, it should not be considered a best practice. Note, many of the provisions within this document may not be applicable to your company. We strongly recommend that the reader seek legal advice from their own attorneys in connection with drafting of codes, guidelines, policies or releases specific to their organization.***

## *[SAMPLE 2]*

**[Company]** differentiates itself in the market with its professional approach to client service. That professional approach includes conservative business attire for its employees Monday through Thursday and business casual Fridays, weekends and off-hour shifts. Please use the following guidelines in helping you make the appropriate decisions:

**Business Attire-Men**

- Business suits
- Collared, button-down shirts
- Business dress shirts
- Business ties
- Business socks and shoes

**Business Attire-Women**

- Business suits
- Business blouses and skirts
- Business dresses
- Sheer or opaque nylons
- Business shoes

**Casual Business Attire Men**

- Slacks
- Casual shirts
- Golf Shirts
- Sweaters
- Loafers

**Casual Business Attire Women**

- Casual Pants
- Casual dresses and skirts
- Casual shirts and blouses
- Sweaters
- Casual shoes

**Example of Unacceptable Business Attire for Men and Women**

- Cotton or corduroy jean-style pants or dresses
- Cotton or Khaki (Dockers) pants
- Stretch, stirrup, capri, harem or lycra-spandex pants
- Shorts or culottes, including city shorts and shorts suits
- Mini-skirts
- Casual or faddish styles
- T-shirts
- Denim clothing
- Sweatpants or sweatshirts
- Halter, tube, cropped or tank tops
- Patterned or textured nylons
- Sneakers, cowboy shoes or boots, sandals*

**Example of Unacceptable Casual Business Attire for Men and Women**

- Jeans/Denim clothing
- Stretch, stirrup, capri, harem or lycra-spandex pants
- T-shirts
- Denim clothing
- Sweatpants or sweatshirts
- Patterned or textured nylons
- Sneakers, cowboy shoes or boots, sandals*

* Sneakers worn for commuting purposes must be changed, upon arriving to work.

***Please note, this document is being provided as general business advice and should not be construed as legal advice. Further, this document is "sample language" only, it should not be considered a best practice. Note, many of the provisions within this document may not be applicable to your company. We strongly recommend that the reader seek legal advice from their own attorneys in connection with drafting of codes, guidelines, policies or releases specific to their organization.***

# SAMPLE - COMPANY GUIDELINES FOR INSPECTION OF EMPLOYEE PROPERTY

All lockers, desks, filing cabinets and cubicles are Company property and must be maintained according to Company rules and regulations. The Company reserves the right to inspect all Company property with or without prior notice to the employee and/or in the employee's absence. An employee's personal property, including but not limited to tool boxes, packages, purses, and vehicles may be inspected upon reasonable suspicion of unauthorized possession of Company property, weapons or illegal drugs.

An employee's personal property, including but not limited to tool boxes, packages, purses and vehicles, may be inspected upon reasonable suspicion of unauthorized possession of Company property, weapons, or illegal drugs.

 

***Please note, this document is being provided as general business advice and should not be construed as legal advice. Further, this document is "sample language" only, it should not be considered a best practice. Note, many of the provisions within this document may not be applicable to your company. We strongly recommend that the reader seek legal advice from their own attorneys in connection with drafting of codes, guidelines, policies or releases specific to their organization.***

## SAMPLE – COMPANY GUIDELINES RELATED TO WORKPLACE SECURITY

To ensure the safety and security of Company employees and property, only authorized visitors are allowed in the workplace. Denying access to unauthorized individuals to our facilities and information systems enables us to maintain our safety standards, protects against theft of Company and employee property, ensures the security of equipment, protects confidential information and can avoid unnecessary disturbances.

We promote a safe environment for employees and visitors. As such we are committed to working with you to maintain a work environment free from violence, threats of violence, harassment, intimidation and other disruptive behavior. Violent behavior is defined as the use of physical force or violence to restrict the freedom of action or movement of another person or to endanger the health and safety of another person or property of the Company.

Violence, threats, harassment, intimidation and other disruptive behavior in our workplace will not be tolerated. Any employee who engages in such conduct will be subject to serious disciplinary action, which may include termination of employment.

The cooperation of every employee is essential to effectively maintain a safe work environment. Do not ignore violent, threatening, harassing, intimidating or other disruptive behavior. If you observe or experience such behavior by anyone on Company property, report it immediately to security personnel or a member of your Human Resources representative.

Where reasonable suspicion exists, we reserve the right to inspect employee work areas, lockers, computer and electronic files and personal effects, including persons, briefcases and other like items for the protection of others and the Company.

 

***Please note, this document is being provided as general business advice and should not be construed as legal advice. Further, this document is "sample language" only, it should not be considered a best practice. Note, many of the provisions within this document may not be applicable to your company. We strongly recommend that the reader seek legal advice from their own attorneys in connection with drafting of codes, guidelines, policies or releases specific to their organization.***

# SAMPLE - E-MAIL POLICY

We have adopted an "acceptable use" policy regarding the use of information systems or electronic communications which includes, but is not limited to, voice messaging, e-mails, computers, the Internet, pagers or facsimile machines provided by the Company.

The Company's information system exists for the purposes of conducting Company business. A minimal amount of personal use is acceptable, but should not interfere with or conflict with business use. Use good judgment and limit the frequency of such use. Information systems may not be used for personal gain.

As a user of the Company information systems, you should expect that all electronic records and systems will be monitored/inspected to ensure they are being used for the Company's legitimate purposes and that all laws and Company policies, standards, practices and guidelines are followed. We reserve the right to disclose the contents of our electronic records and systems when a legitimate business need exists.

You may not use any Company information system to access, copy, store or transmit any information or data considered to be of a sexual, pornographic or lewd nature, or any data that when viewed by another employee could be considered inappropriate and contributing to an unsuitable or hostile work environment. The Company's policies and standards against sexual or other harassment apply fully to the e-mail and Company information system, and any violation of those standards is grounds for discipline, up to and including discharge. Therefore, no e-mail messages should be created, sent or received if they contain intimidating, hostile, or offensive material concerning race, color, religion, sex, national origin, disability or any other classification protected by law.

Improper use of these information systems can result in a breach of confidentiality, waiver of attorney-client privilege, loss of productivity, delays in sending and receiving information, damage to or destruction of data and impairment of the work environment. In addition, abuses can, in some circumstances, subject the user and the Company to criminal prosecution and/or civil liability.

You shall at all times use the Company information system in a manner that is ethical, legal and consistent in the best interest of the Company. Any misuse of the Company information system can lead to disciplinary measures, up to and including termination of employment.

For more details, see your manager or Human Resources representative.

 

***Please note, this document is being provided as general business advice and should not be construed as legal advice. Further, this document is "sample language" only, it should not be considered a best practice. Note, many of the provisions within this document may not be applicable to your company. We strongly recommend that the reader seek legal advice from their own attorneys in connection with drafting of codes, guidelines, policies or releases specific to their organization.***

## SAMPLE – COMPANY GUIDELINES RELATED TO PRIVACY OF EMPLOYEE INFORMATION

We respect you as an employee and believe in the confidentiality of your personnel and medical files. As a result, we restrict disclosure of information and access to your files, except to the extent disclosure of such information is required buy law.

You are permitted access to your personnel file and will be allowed sufficient and reasonable inspection time, commensurate with the volume content of the file, in the presence of the Human Resources representative and in accordance with applicable state laws. Copies of all documents bearing your signature will be provided when requested.

At the request of authorized law enforcement or local, state, provincial or federal agencies conducting official investigations, the Company may release information contained in personnel files. Medical information may be disclosed only under very limited circumstances.

Investigation materials, memos of reference checks, medical records, attorney-client communications and records which identify or violate the privacy of others will not be made available for inspection.

Third-Party Requests for Information

- Only your employment date, job title and employment status (active or non-active) will be released if requested by a third party, unless you consent that more information be released.

- Inquiries for verification of payroll information will be provided upon written request to the Human Resources department. Your Human Resources representative will direct these requests, along with credit or mortgage loan application verifications, to the payroll department.

Where applicable, state requirements prevail.

 

***Please note, this document is being provided as general business advice and should not be construed as legal advice. Further, this document is "sample language" only, it should not be considered a best practice. Note, many of the provisions within this document may not be applicable to your company. We strongly recommend that the reader seek legal advice from their own attorneys in connection with drafting of codes, guidelines, policies or releases specific to their organization.***

## SAMPLE – COMPANY GUIDELINES ON CONFIDENTIALITY OF COMPANY INFORMATION

As a Company employee you will have access to various types of company proprietary information. "Proprietary information" includes, but is not limited to, records, lists and knowledge of the Company's customers, suppliers, methods of operation, processes, trade secrets, methods of determination of prices, financial condition, profits, sales, net income and indebtedness.

You should not use or disclose to any person or entity any Company proprietary information acquired during the course of your employment. Also, you should not, directly or indirectly, copy, take or remove from your work site, any of the Company's books, records, customer lists or any other documents or materials. If and when you leave the Company, for any reason, any documents or materials in your possession belonging to the Company must be returned.

Information and technology that the Company considers proprietary must be protected and held in the strictest confidence to ensure the competitiveness of our business. This includes:

- Keeping proprietary documents protected, secure and labeled appropriately;
- Not sharing business information of a proprietary nature received or heard during the course of normal business activities; and
- Advising your manager or Human Resources representative of possible misconduct or breach of confidentiality.

If you have any questions about what material is considered Company proprietary, ask your supervisor or manager. Improper disclosure of Company proprietary information will lead to disciplinary action, up to and including termination of employment.

 

***Please note, this document is being provided as general business advice and should not be construed as legal advice. Further, this document is "sample language" only, it should not be considered a best practice. Note, many of the provisions within this document may not be applicable to your company. We strongly recommend that the reader seek legal advice from their own attorneys in connection with drafting of codes, guidelines, policies or releases specific to their organization.***

# SAMPLE – DISCLOSURE TO EMPLOYEE REGARDING PROCUREMENT OF A CONSUMER REPORT

In connection with your employment by **[Company]**, its affiliates or subsidiaries (collectively, the "Employer"), you understand that a consumer report or an investigative consumer report may be requested that will include information as to your character, general reputation, financial and credit record, personal characteristics, mode of living, work habits, performance, and experience, along with reasons for termination of past employment. You understand that as directed by Employer and consistent with your job at the Employer, the Employer may be requesting information from public and private sources about your: driving record, court record, education, credentials, credit and references. Please be advised that you have the right to request, in writing, within a reasonable time, that the Employer make a complete and accurate disclosure of the nature and scope of the information requested. Such disclosure will be made to you within five (5) business days of the date on which the Employer receives the written request from you.

In the event that information from the report is utilized in whole or in part in making an adverse decision with regard to your employment at the Employer, before making the adverse decision, the Employer will provide you with oral, written, or electronic notice of the adverse action, a copy of the consumer report, a description in writing of your rights under the law and the name, address and phone number of the consumer reporting agency that furnished the report. An adverse decision is a decision for employment purposes that adversely affects a current employee. You will be notified of your rights to dispute the accuracy of the consumer report with the consumer reporting agency.

## RELEASE AUTHORIZATION

I hereby authorize the Employer to obtain a consumer report and/or an investigative consumer report about me for employment purposes. I also hereby authorize, without reservation, any law enforcement agency, institution, information service bureau, school, employer, reference or insurance company contacted by either the Employer, or its representative (including, but not limited to, a consumer reporting agency) to furnish the information described in the above Disclosure to Employee. I hereby release the Employer, its employees, officers, directors, representatives (including, but not limited to, any consumer reporting agency contracted by the Employer) and its agents and all persons, agencies, and entities obtaining or providing information or reports about me from any and all liability arising out of the requests for or release of any of the above mentioned information or reports.

_____

**Please print your full name**

_____

**Signature** **Today's Date**

 

***Please note, this document is being provided as general business advice and should not be construed as legal advice. Further, this document is "sample language" only, it should not be considered a best practice. Note, many of the provisions within this document may not be applicable to your company. We strongly recommend that the reader seek legal advice from their own attorneys in connection with drafting of codes, guidelines, policies or releases specific to their organization.***

# SAMPLE – PROTECTING INFORMATION ASSETS POLICY

## I. INTRODUCTION

**[Company]**, including its affiliated companies (collectively, the "Company"), and its employees have an obligation to protect client data and information (electronic as well as paper-based), and client- and Company-owned equipment and software from loss or misuse. To ensure the confidentiality and integrity of client and Company data, the Company has developed the *Information Security Program for Safeguarding Customer Information* (the "Program"). This Program documents the Company's administrative, technical and physical safeguards to protect clients' information, including provisions and procedures designed to comply with the requirements of Sections 501 and 505(b) of the Gramm-Leach-Bliley Act of 1999 ("GLBA"). Since much of our client and Company information is stored in computer systems and file cabinets, formal guidelines are necessary to control this data. In addition, personal computer hardware, software, and network infrastructure are significant investments for the Company. These assets must be protected and used effectively if we are to gain full value from these investments.

The Program and corporate policies and guidelines can help us meet our obligations to protect information security and assets, but employees at all levels in departments and offices must take this as a primary responsibility.

As an employee, you have obligations in these three areas:

A. Use information, equipment, and software that is assigned to you or that you have access to in a professional, responsible, ethical, and legal manner.

B. Protect the integrity of client and corporate information from damage, loss, misuse, duplication, or inappropriate disclosure.

C. Protect equipment and software assigned to you from damage or loss.

## II. INFORMATION, EQUIPMENT, SOFTWARE

*Use information, equipment, and software that is assigned to you or that you have access to in a professional, responsible, ethical, and legal manner.*

> **A. Business Purposes Only.** Use data/information, equipment and software for business use only. Employees are granted access privileges at the Company for business purposes only. Do not conduct personal business at the Company. Non-business use of the Company's environment will not be tolerated and may subject you to disciplinary action up to and including termination.

 

**B. Policy on E-mail and Voice Mail.** E-mail and Voice Mail systems are provided exclusively to assist in the conduct of business within the Company. Messages sent through E-mail and the contents of any employee's computer as well as messages contained on Voice Mail are the sole property of the Company. Employees should have no expectation of privacy in using the Company's E-mail or Voice Mail systems.

By using the Company's E-mail and Voice Mail, all employees knowingly and voluntarily consent to their usage of these systems being monitored and acknowledge the Company's right to conduct such monitoring. Even when a message is erased, it is still possible to recreate the message, therefore privacy of messages cannot be ensured to anyone.

The Company may override any individual passwords and/or codes or require employees to disclose any passwords and/or codes to facilitate access by the Company to E-mail or Voice Mail. The Company retains the right to access any employee's E-mail or Voice Mail at any time for any reason whatsoever without notice to the employee. Such reasons include, but are not limited to: conducting Company business, investigating conduct or behavior that may be illegal or adversely affect the Company or its clients, assuring compliance with Company policies, and/or determining or preventing personal use of E-mail or Voice Mail. The approval of the Chief Executive Officer, the President or a Senior Vice President must be obtained prior to any access.

The Company's policies regarding harassment apply to E-mail and Voice Mail use. Any communications by employees via E-mail or Voice Mail that may constitute verbal abuse, slander, or defamation or may be considered offensive, harassing, vulgar, obscene, or threatening are strictly prohibited. Offensive content would include but not be limited to sexual comments or images, racial slurs, gender-specific comments, or any comments that would offend someone on the basis of his or their age, race, color, religion, national origin, disability, or veteran status.

Finally, many other Company policies apply to the use of E-mail or Voice Mail. For example, policies regarding solicitation, confidentiality, and use of copyrighted materials all apply to the use of E-mail and Voice Mail. Employees must abide by all Company policies.

**C. Policy on Internet Use.** Internet access is provided only for Company business purposes and use of the Internet for any other purpose may subject the employee to disciplinary action up to and including dismissal. Prohibited uses of Company granted Internet access include:

- personal use;
- viewing or transferring frivolous or any other material not appropriate for business purposes;
- unauthorized viewing or transferring of material that is confidential or proprietary to the Company or its clients, including business or financial information of clients;
- unauthorized posting of any material on the World Wide Web;
- communicating, disseminating, or printing of any copyrighted materials in violation of copyright laws;
- viewing or transferring obscene, pornographic, abusive, slanderous, defamatory, harassing, vulgar, threatening, and/or offensive material; or
- any other activity deemed by the Company to be in conflict with the intent of Internet access granted to the employee. (This list in not intended to be all-inclusive.)

 

Employees accessing the Internet on Company time are representing the Company in a public forum, and so must maintain a professional image at all time and must adhere to all pertinent Company policies. Use of the Company name must be in accordance with policies applicable to printed media. Employees must not engage in any activity or transmit any communication that would reflect unfavorably on the Company or be deemed to be inappropriate by the Company. For example, the Company name (which is embedded in our public E-mail addresses) may not be used when making personal statements in public forums.

The Company retains the right to revoke an employee's access at any time, with or without cause, at the Company's sole discretion.

The Company also retains the right to access any "Internet material" at any time for any reason whatsoever, with or without notice to the employee. Internet material includes, but is not limited to: E-mail messages and attachments, HTML documents, FTP files, scripts, graphics and multimedia files, data or code. All Internet material retrieved, or placed on the Internet from Company facilities or property is the sole property of the Company. By using Company-provided Internet accesses, employees knowingly and voluntarily consent to such usage being monitored and acknowledge the Company's right to conduct such monitoring. Employees should have no expectation of privacy whatsoever related to the use of the Internet or any Internet material and that their use of the Internet and any Internet material is not private. Even when Internet materials are erased, it is still possible to recreate the information; therefore all employees understand that privacy of Internet material cannot be ensured to anyone.

Finally, regardless of time or place, employees may not represent the Company without proper authorization and should therefore not reference the Company affiliation with respect to their private activities. Specifically, this means that employees should not use the Company name when posting to newsgroups and should not construct any electronic links, which point to the Company, without the prior consent of the Company.

**D. Accessing, Intercepting, Modifying or Removing Information, Equipment or Software.** Do not access, intercept, modify or remove someone else's equipment, software, or data/information without appropriate authorization. Employees must not intentionally attempt to intercept or access voice or electronic messages or data not intended for them. All data, electronic messages, and Voice Mail are the property of the Company.

**E. Modifying or Alerting System Files.** Do not modify or alter any system files. System files are configured according to a specific standard by the **[Company's IT Department]**. Modifying or altering these files may result in software failures or corruption of the Company's information assets. If an employee suspects that any systems files may need to be brought back to the original standard or modified for a particular use, that employee should contact the **[Company's IT Department]** help desk at **[Insert Help Desk Number]**.

**F. Report Systems Weaknesses.** Report any security weaknesses you become aware of to the **[Company's IT Department]** help desk at **[Insert Help Desk Number]**.

 

**G. Avoid Specific Prohibitions.** Under no circumstances may the following be knowingly sent or retrieved over the Company's internal or external networks:

- games, executable programs, executable scripts;
- viruses, worms, Trojan horses, or other harmful code;
- threatening or harassing messages;
- unsolicited advertising;
- chain letters or other types of unauthorized broadcast messages;
- offensive, obscene, pornographic, or sexually explicit materials; or
- any materials or usage not complying with all applicable laws, regulations, policies, and procedures of the state or the country in which the communication originates or terminates.

Unauthorized employee use of network traffic capture utilities or password capture utilities is strictly prohibited and is grounds for immediate dismissal. Installation of unauthorized modems in auto-answer mode on personal computers or server machines is strictly prohibited. Finally, setting-up call forwarding to an outside number is also strictly prohibited.

## II. CLIENT AND CORPORATE INFORMATION

*Protect client and corporate information from damage, loss, misuse, duplication, or inappropriate disclosure.*

**A. Protect the Confidentiality of Client and Corporate Information.** Client information may not be disclosed to any third party except as is necessary to perform our services for clients. Similarly, sensitive corporate information may not be disclosed to any third parties. Dispose of sensitive client and corporate information either by shredding or placing in locked recycle bins on each floor.

**B. Protect Sensitive Date from Inappropriate Access.** Store sensitive data on removable media, or provide password protection for files stored on non-removable media (hard disks or file servers). Store disks and other removable media in a secure location.

**C. Back Up Business Related Documents on Network.** Reserve time in your work schedule to carry out the backup. All critical documents and files should be stored on network servers, where they will be backed up by network administrators, or backed up via a second copy on another medium. Call the **[Company's IT Department]** help desk at **[Insert Help Desk Number]** for formal backup procedures.

**D. Sensitive Documents.** Use electronic delivery mechanisms appropriately when dealing with sensitive documents. Prior to communicating with a client via the public Internet, agreement should be made with the client as to what information may be communicated via Internet E-mail or file transfer. Confidential information should not be sent via the Internet unless it is secured in a manner agreed upon with the client. Unless otherwise agreed by the client, do not send a sensitive message to a general-use mailbox such as an office mailbox, or bulletin board, or a fax machine, where anyone walking by can read it. Any business correspondence conducted via E-mail that, if in paper form, would be retained, must be filed electronically or printed and placed in the paper files in accordance with normal filing procedures. E-mail messages are not archived automatically by the E-mail systems. Employees must

 

protect electronic messages, documents, or spreadsheets, in accordance with their sensitivity.

**E. Privacy – Not Guaranteed.** Beware that absolute privacy cannot be guaranteed. Employees must always evaluate the content of their Voice Mail and electronic messages (don't send electronically anything that you would not say over a cellular phone.)

IV. PROTECTING EQUIPMENT, SOFTWARE AND ACCESS

***Protect equipment, software, and access assigned to you from damage or loss.***

**A. Use Properly Licensed Software Only.** It is illegal to use software without obtaining a license for that software. Employees must not "pirate" a copy of an application from anyone. Use of unlicensed software subjects the Company to severe penalties and any employee using unlicensed software will be subject to disciplinary action up to and including dismissal. In addition, software obtained from external sources is a primary source of computer viruses, and may or may not produce accurate results. Employees are in danger from viruses any time they "borrow" software from an unproven source. Employees can spread a virus quickly without realizing it. If an employee has unlicensed software on their machine, they must remove it (or seek help in removing it by calling the help desk at **[Insert Help Desk Number]**).

**B. Viruses.** Be aware that unusual system behavior could be a caused by a virus, and request help in diagnosing it. All machines will have a current version of virus protection software (the list of viruses evolves as new viruses are discovered and must be added to the virus protection software for the software to be effective at stopping new known viruses). Employees must make sure that their machine does have current virus protection software and use it regularly. The local network administrator will check file servers on local area networks. Contact the **[Company's IT Department]** help desk at **[Insert Help Desk Number]** for help if a virus is suspected.

**C. Negligence or Improper Usage.** Do not damage equipment assigned to you through negligence or improper usage. Computer equipment must be secured against theft or misuse. Laptop and notebook computers in particular are easily stolen. Place laptop computers in a cabinet or locked drawer when you leave for the day. Laptop damage due to improper use or handling can result in disciplinary action.

**D. Protect Your Password.** Passwords are the primary means of protecting the security of data on networks. Do not share your password with other employees. A password must be chosen carefully so that it cannot be easily derived. Passwords should comply with company standards for length of characters, contain both letters and numbers, and avoid the obvious such as nicknames, initials, or addresses. Employees must memorize their passwords and never write them down or display them. Passwords must be changed frequently to maintain security at a high level. Most passwords are forced to change on a periodic basis; however, if an employee has reason to believe that the confidentiality of the password has been compromised, they must change it more frequently. Passwords must never be built into access routines (anyone with physical access to the machine could gain access), unless the resulting access is intended to be freely accessible by anyone.

 

**E. Log Off From Workstation.** Log off when you leave a terminal or workstation. Employees must log off when they expect to leave their terminal or workstation for a prolonged period of time. Any damage or misuse through an employee's access privileges is the responsibility of that employee and they will be held accountable. Ensure that unused access privileges are revoked or changed when they are no longer needed.

**F. Dial In Access.** Dial-in access to the Company's computers, and access from the Company's computers to external sites must occur via **[Company's IT Department]** approved services. All access to external networks from network-connected will be made via gateways provided by the **[Company's IT Department]** or via dial-up access via modems to pre-approved sources (e.g., pricing vendors, and client-authorized destinations).

Remote access to the Company's computers must be via services provided by the **[Company's IT Department]**. Procedures for accessing E-mail remotely may differ from those for dial-in access to the network.

Access to the World Wide Web for business-related research purposes is available through a standard internet architecture configuration. Internet connectivity is provided to all personnel as an extension of the technology services. Downloaded material from the Internet that does not pass through any automatic virus scan or firewall must be scanned for viruses before viewing or saving on any networked PC or Server. Employees downloading materials from Internet sites must also respect the intellectual property rights of the owners of the materials. In general, materials published in newspapers or magazines, paper or electronic, are copyrighted. Copyrighted materials may not be posted on bulletin-board-like or information-sharing solutions without permission of the person holding the copyright. Permission may often be obtained for a modest fee.

All other dial-in or dial-out access is prohibited unless specifically authorized by **[Insert Person with Authority to Approve Dial Out Access]** within the **[Company's IT Department]**.

## V. COMMENTS

The Company's CIO is responsible for issuing guidelines to assist offices and departments in fulfilling their responsibility to protect client and Company data in our increasingly computerized environment. The guidelines in this document are a first step in meeting this obligation. Please submit comments and suggestions for guidelines to the Company's CIO.

 

I have received and read a copy of the **[Company]** Information Assets Protection Policy document (attached). I will comply with this policy on and offsite. I understand that any actions in violation of this policy will result in disciplinary action, up to and including termination, as well as any applicable civil and criminal legal actions against me (or my employer if I am a non-employee of **[Company]**). In addition:

1. I agree to use information, equipment, and software that is assigned to me or that I have access to in a professional, responsible, ethical, and legal manner.

2. I agree to protect client and corporate information from damage, loss, misuse, or duplication.

3. I agree to protect equipment and software assigned to me from damage or loss.

NAME: _____
(Please Print)

SIGNATURE: _____

DATE: _____

 

***Please note, this document is being provided as general business advice and should not be construed as legal advice. Further, this document is "sample language" only, it should not be considered a best practice. Note, many of the provisions within this document may not be applicable to your company. We strongly recommend that the reader seek legal advice from their own attorneys in connection with drafting of codes, guidelines, policies or releases specific to their organization.***

# SAMPLE - CODE OF BUSINESS CONDUCT POLICY

This Code of Business Conduct covers a wide range of business practices and procedures. It does not cover every issue that may arise, but it sets out basic principles to guide all employees of **[Company]** and its affiliated companies. We expect that all of our directors, employees, consultants and agents will conduct themselves at all times in an honest and ethical manner. It is critically important that all of our directors, employees, consultants and agents know these rules and guidelines for conducting business. All references to "employee" in this policy shall apply equally to consultants and agents of **[Company]** and its affiliated companies.

This Business Conduct Policy is subject to modification and will be reviewed and approved by the Board of Directors at least annually. All of our directors and employees are expected to study, pledge personal commitment to and annually sign this policy to evidence understanding and compliance.

Anyone who violates this Code of Business Conduct Policy will be acting outside the scope of his or her employment and will be subject to disciplinary action.

If you are in a situation which you believe may violate or lead to a violation of this Code, follow the guidelines described in Section 15 of this Code. We will not retaliate in any way against an employee making a good faith report under this or any other of our policies.

1. **Compliance with Laws, Rules and Regulations**

Obeying the law, both in letter and in spirit, is the foundation on which our ethical standards are built. All employees must respect and obey the laws of the cities, states and countries in which we operate. Although not all employees are expected to know the details of these laws, it is important to know enough to determine when to seek advice from supervisors, managers or other appropriate personnel.

The following paragraphs provide additional detail regarding some of the laws that affect our business.

**[Discuss laws applicable to your business. For example, laws relating to Foreign Corrupt Practice Act, Insider Trading, Public Reporting or Anti-Trust Compliance.]**

A. Foreign Corrupt Practices Act

The Foreign Corrupt Practices Act ("FCPA") has two basic parts: anti-bribery provisions and accounting and recordkeeping requirements. The anti-bribery section prohibits payment of a bribe to a non-U.S. official or non-U.S. political party, party official or candidate for political office. The FCPA defines a bribe as anything of value given or offered to a non-U.S. official for the purpose of influencing an act or decision to obtain cash, retain business or direct business. Employees and directors are prohibited from paying bribes.

The FCPA accounting and recordkeeping requirements restate generally accepted accounting principles. Strict documentation and reporting is required. No

 

employee or director shall make any improper payments, including those which violate applicable laws or regulations, are falsified, unrecorded, or undocumented in our accounting records, or whose source is off-the-record-funds or which aid and abet another party to make or receive illegal payments.

Any employee or director who is convicted of violating the FCPA is subject to substantial fines and/or imprisonment. If convicted, we may also be subject to substantial fines.

B. Insider Trading

Employees and directors are prohibited from engaging in securities transactions or enabling others to do so as a result of material nonpublic information obtained as an employee, director or otherwise. We maintain a detailed Insider Trading Policy which all employees and directors are required to read and certify annually.

C. Public Reporting

We are dedicated to ensuring that we make full, fair, accurate, timely and understandable disclosure in the reports and documents that we file with, or submit to, the Securities and Exchange Commission and in our other public communications. If any employee has a reason to believe that any report, document or other public communication does not meet these standards, that employee should follow the guidelines in Section 15.

D Antitrust Compliance

All employees and directors are expected to observe the highest standards of ethical conduct in relationships with competitors. As such, employees and directors are prohibited from entering into arrangements with competitors for the purpose of setting or controlling prices, rates, trade practices, marketing policies, or disclosing to competitors our future plans which have not been disclosed generally to the public.

**2. Conflicts of Interest**

A "conflict of interest" exists when a person's private interest interferes in any way with the interests of the Company. A conflict situation can arise when an employee or director takes actions or has interests that may make it difficult to perform his or her Company work objectively and effectively. Conflicts of interest may also arise when an employee or director, or members of his or her family, receives improper personal benefits as a result of his or her position in the Company. Loans to, or guarantees of obligations of, directors, employees or their family members may create conflicts of interest.

It is almost always a conflict of interest for an employee to work simultaneously for a competitor, customer or supplier. You are not allowed to work for a competitor as a consultant or board member. The best policy is to avoid any direct or indirect business connection with our customers, suppliers or competitors, except on our behalf.

Conflicts of interest are prohibited as a matter of Company policy, except under guidelines approved by the Board of Directors. Conflicts of interest may not always be clear-cut, so if you have a question, you should consult with higher levels of management or our Legal Department. Any employee or director who becomes aware of a conflict or potential conflict should bring it to the attention of a supervisor, manager or other appropriate personnel or consult the procedures described in Section 15 of this Code.

**3. Corporate Opportunities**

Employees and directors are prohibited from taking for themselves personally opportunities that are discovered through the use of corporate property, information or position without the consent of the Board of Directors. No employee or director may use corporate property, information, or position for improper personal gain, and no employee or director may

 

compete with the Company directly or indirectly. Employees and directors owe a duty to the Company to advance its legitimate interests when the opportunity to do so arises.

**4. Competition and Fair Dealing**

We seek to outperform our competition fairly and honestly. We seek competitive advantages through superior performance, never through unethical or illegal business practices. Stealing proprietary information, possessing trade secret information that was obtained without the owner's consent, or inducing such disclosures by past or present employees of other companies is prohibited. Each employee and director should endeavor to respect the rights of and deal fairly with the Company's customers, suppliers, competitors and employees. No employee or director should take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other intentional unfair dealing practice.

The purpose of business entertainment and gifts in a commercial setting is to create good will and sound working relationships, no to gain unfair advantage with customers. No gift or entertainment should ever be offered, given, provided or accepted by any Company employee, director or family member of an employee or director unless it: (1) is not a cash gift, (2) is consistent with customary business practices, (3) is not excessive in value, (4) cannot be construed as a bribe or payoff and (5) does not violate any laws or regulations. Please discuss with your supervisor any gifts or proposed gifts which you are not certain are appropriate.

**5. Outside Employment**

Any outside activity must not interfere with the duties of the employee or the interests of our stockholders. Acceptance of outside employment, directorship and participation in the affairs of outside organizations carries possible conflict with the employee's primary responsibilities. Accordingly, employees should obtain prior approval of the Director of Corporate Compliance before accepting any outside employment, directorship, fiduciary appointment, or civic responsibility that involves a potential conflict of interest or which would require a significant amount of time during normal working hours.

**6. Protection and Proper Use of Company Assets**

All employees and directors should endeavor to protect our assets and ensure their efficient use. Theft, carelessness and waste have a direct impact on our profitability. Any suspected incident of fraud or theft should be immediately reported for investigation. Our equipment, computers, e-mail, internet access and voicemail systems should not be used for non-Company business, though incidental personal use may be permitted. Use of our information assets are subject to the requirements of our **[Information Assets Protection Policy**] which all employees are required to read and certify annually.

The obligation of employees and directors to protect our assets includes our proprietary information. Proprietary information includes intellectual property such as trade secrets, patents, trademarks and copyrights, as well as business, marketing and service plans, engineering and manufacturing ideas, designs, databases, records, salary information and any unpublished financial data and reports. Unauthorized use or distribution of this information would violate our policy. It could also be illegal and result in civil or even criminal penalties.

**7. Use of Company Name**

Employees and directors may not use our company name in connection with personal activities, except as part of biographical summaries of work experience or except as otherwise approved in writing by the Chief Executive Officer or President.

**8. Record-Keeping**

We require honest and accurate recording and reporting of information in order to make responsible business decisions. For example, only the true and actual number of hours worked should be reported.

 

Many employees regularly use business expense accounts, which must be documented and recorded accurately. If you are not sure whether a certain expense is legitimate, ask your supervisor or your controller. See our **[Travel and Entertainment Policy]** for more details.

All of our books, records, accounts and financial statements must be maintained in reasonable detail, must appropriately reflect our transactions and must conform both to applicable legal requirements and to our system of internal controls. Unrecorded or "off the books" funds or assets should not be maintained unless permitted by applicable law or regulation.

Business records and communications often become public, and we should avoid exaggeration, derogatory remarks, guesswork or inappropriate characterizations of people and companies that can be misunderstood. This applies equally to e-mail, internal memos and formal reports. Records should always be retained or destroyed according to our record retention policies. In accordance with those policies, in the event of litigation or governmental investigation please consult our **[Legal Department]**.

**9. Confidential Information**

Each employee is required to sign a **[Confidentiality Agreement]** upon their employment with us. The **[Confidentiality Agreement]** provides that under no circumstances may confidential information with respect to us, **our** clients, prospective clients, or suppliers be revealed to unauthorized persons. Employees should be careful not to inadvertently disclose information through conversations or careless handling of sensitive documents.

In addition, we conduct certain informational and training programs on a regular basis. All of the data and information, including but not limited to all written materials provided at these sessions are confidential and proprietary to us and are governed by your **[Confidentiality Agreement]**. All employees are expected to use these materials for internal purposes only. All materials must be returned to us upon termination of employment and may not be disclosed or transferred to any third party without the express written permission of the Chief Executive Officer or President.

**10. Contracts and Binding Agreements**

Employees are prohibited from signing any contracts or binding agreements on our behalf without first receiving approval from the Legal Department and the Chief Financial Officer.

**11. Media Relations**

Employees and directors should not respond to inquiries from the media, but rather refer the media to our **[Media Relations Department]**.

**12. Maintaining a Respectful Workplace**

A. Equal Employment Opportunity

We are an equal opportunity employer. It is our policy to administer all human resources actions and policies without regard to race, color, religion, creed, sex, national origin, ancestry, age (40 and above), mental or physical disability, sexual orientation, any veteran status, any military service or application for military service or membership in any other category protected under the law. All employment decisions and personnel actions, including, without limitation, recruiting, hiring, promotion, compensation, benefits, and terminations, are and will continue to be administered in accordance with, and to further the principle of, equal employment opportunity. Performance of supervisors and employees alike will be evaluated on the basis of their equal opportunity efforts as well as other criteria.

B. Harassment Free Workplace

We have a fundamental commitment to treat our employees and directors with respect and dignity. The support of equal employment opportunity includes the recognition that all employees and directors have the right to work in an environment free of harassment, whether on account of race, color, sex, national origin, ancestry, age,

 

religion, physical or mental disability, veteran status, military service or application for military service, sexual orientation or any other category protected by state and federal laws. We will not tolerate harassment or discrimination, whether by directors, management, supervisory personnel, other employees or third-parties with whom we do business. Accordingly, we will not tolerate derogatory racial, ethnic, religious, sexually oriented, sexual orientation related, disability related or other inappropriate advances, remarks, slurs, jokes or physical conduct.

Because we take complaints of harassment and discrimination in the workplace seriously, we will respond promptly to all reported complaints of sexual harassment. Where it is demonstrated to its satisfaction that harassment and/or discrimination did in fact occur, we will respond promptly and impose such corrective action as is necessary, including disciplinary action where appropriate. For further guidance please see the policy prohibiting harassment in the **[Company's Human Resources Manual]**.

C. Workplace Violence Prevention

The safety of all of our employees and directors in the workplace is very important to us. For that reason, violence and threats of violence in the workplace will not be tolerated. For further guidance please see the [Company's Human Resources Manual].

D. Drug Free Workplace

It is our policy to maintain a productive and safe workplace free from the influence of illegal drugs. We wish to alert our employees to the dangers of drug abuse in the workplace. This includes the serious threat to the health and safety of the employee and others. Drug abuse affects an employee's reliability, stability and good judgment necessary in the performance of their job duties. Problems with productivity, reliability and absenteeism can reduce an employee's work effectiveness and can result in termination.

For further guidance please see the **[Company's Human Resources Manual]**.

F. Gambling

Neither directors nor employees are allowed to use our resources, equipment or time to engage in or facilitate any form of gambling or betting, including pools or lotteries. For example, gambling related activities are not permitted on our E-mail, computers, Internet, telephones, copiers, the mail system or bulletin boards, during working and non-working hours. For further guidance, please see the policy prohibiting gambling in the [Company's Human Resources Manual].

**13. Waivers of the Code of Business Conduct**

Any waiver of this Code for executive officers or directors may be made only by the Board or a Board committee and will be promptly disclosed as required by law or stock exchange regulation.

**14. Reporting any Illegal or Unethical Behavior**

Employees are encouraged to talk to supervisors, managers or other appropriate personnel about observed illegal or unethical behavior and when in doubt about the best course of action in a particular situation. It is our policy not to allow retaliation for reports of misconduct by others made in good faith by employees. Employees are expected to cooperate in internal investigations of misconduct.

 

**15. Compliance Procedures**

We must all work to ensure prompt and consistent action against violations of this Code. However, in some situations, it is difficult to know right from wrong. Since we cannot anticipate every situation that will arise, it is important that we have a way to approach a new question or problem. These are the steps to keep in mind:

- Make sure you have all the facts. In order to reach the right solutions, we must be as fully informed as possible.
- Ask yourself: What specifically am I being asked to do? Does it seem unethical or improper? This will enable you to focus on the specific question you are faced with, and the alternatives you have. Use your judgment and common sense; if something seems unethical or improper, it probably is.
- Clarify your responsibility and role. In most situations, there is shared responsibility. Are your colleagues informed? It may help to get others involved and discuss the problem.
- Discuss the problem with your supervisor. This is the basic guidance for all situations. In many cases, your supervisor will be more knowledgeable about the question, and will appreciate being brought into the decision-making process. Remember that it is your supervisor's responsibility to help solve problems.
- Seek help from Company resources. In the rare case where it may not be appropriate to discuss an issue with your supervisor, or where you do not feel comfortable approaching your supervisor with your question, discuss it locally with your office manager or your Human Resources manager. If that also is not appropriate, you may make a confidential or anonymous report to our toll-free **[Compliance and Ethics Hotline]**. If you prefer to write, address your concerns to: **[General Counsel]**.
- You may report ethical violations in confidence and without fear of retaliation. To the extent practical and appropriate under the circumstances, we will not disclose the identity of anyone who reports a suspected violation. We do not permit retaliation of any kind against employees for good faith reports of ethical violations.
- Always ask first, act later. If you are unsure of what to do in any situation, seek guidance before you act.

 

## CODE OF BUSINESS CONDUCT

## CERTIFICATION

I hereby certify that I have read and understand the **[Company]** Code of Business Conduct and I agree to comply with the Policy.

I also certify that I understand that this Code of Business Conduct does not create any obligation on the Company or any other person to continue my employment at the Company.

Date: _____ Signature: _____

Name: _____

(Please Print)

 