# Policy Manual

October, 2019

Washington School of Psychiatry
5028 Wisconsin Avenue NW
Suite 400
Washington DC 20016

Table of Contents

**Page**

# Washington School of Psychiatry Staff Manual

## I. Introduction

This manual is intended to outline and explain Washington School of Psychiatry's ("WSP") practices and policies. This policy handbook also summarizes current company policies. This manual is not a contract, express or implied, guaranteeing employment for any specific duration.

Neither the policies in this manual, nor any other written or verbal communication by a company officer, manager or supervisor are intended to create a contract of employment or a warranty of benefits. The policies in this manual may be amended, modified, deleted or otherwise changed by WSP without prior notice.

This manual supersedes and replaces all prior policy manuals, handbooks, policies or procedures. If you have any questions about any of the policies or procedures in this manual, please consult the Executive Director.

## II. Non-Discrimination Policy

It is WSP's policy to provide equal opportunity for all. WSP does not unlawfully discriminate on the basis of actual or perceived race, color, religion, sex (including, but not limited to, pregnancy, childbirth or related medical conditions, breastfeeding, and reproductive health decisions), national origin, ancestry, age, physical disability, mental disability, medical condition, genetic information, personal appearance, family care status, veteran status, political affiliation, marital status, sexual orientation, or gender identity or expression.

WSP reasonably accommodates those with disabilities (including temporary disabilities), those who are pregnant, those with sincerely held religious beliefs, and those who have been victims of domestic violence.

WSP prohibits the harassment of any individual on any of the basis listed above.

## III. Policy Against Harassment

WSP does not tolerate unlawful harassment based on actual or perceived race, color, religion, sex (including but not limited to pregnancy, childbirth or related medical conditions, breastfeeding, and reproductive health decisions), national origin, ancestry, age, physical or mental disability, medical condition, genetic information, personal appearance, sexual orientation, gender identity or expression, marital status, family care status, political affiliation, or military or veteran status or in any other group protected by federal, state or local law. With respect to sexual harassment, WSP prohibits the following:

1. Unwelcome sexual advances; requests for sexual favors; and all other verbal and physical conduct of a sexual or otherwise offensive nature, especially where:
    a. Submission to such conduct is made explicitly or implicitly a term or condition of employment;
    b. Submission to or rejection of such conduct is used as the basis for decisions affecting an individual's employment;
    c. Such conduct has the purpose or effect of creating an intimidating, hostile or offensive working environment.
2. Offensive comments, jokes, innuendos, and other sexually-oriented statements.

Examples of such conduct include, but are not limited to the following:

a. Touching, such as rubbing or massaging someone's neck or shoulders, stroking someone's

hair or brushing against another's body.

b. Sexually-suggestive touching.
c. Grabbing, groping, kissing, fondling.
d. Violating someone's "personal space".
e. Whistling.
f. Lewd, off color, sexually-oriented comments or jokes.
g. Foul or obscene language.
h. Leering, staring stalking.
i. Suggestive or sexually-explicit posters, calendars, photographs, graffiti, or cartoons.
j. Unwanted or offensive letters or poems.
k. Sitting or gesturing sexually.
l. Sexually offensive e-mail, voicemail messages, text-messages, or other messages sent via electronic equipment, regardless of whether such equipment was provided by the Company.
m. Sexually offensive posts on social media sites including, but not limited to, Facebook, Twitter and LinkedIn.
n. Sexually-oriented or explicit remarks, including written or oral references to sexual conduct, gossip regarding one's sex life, body, sexual activities, deficiencies or prowess.
o. Questions about one's sex life or experiences.
p. Repeated requests for dates.
q. Sexual favors in return for employment requests or threats if sexual favors are not provided.
r. Any other conduct deemed sexually inappropriate by WSP.

Anyone who believe they have been subjected to harassing conduct are encouraged to promptly advise the offender that his or her behavior is unwelcome, and request that such conduct be stopped. However, you are not required to do so. Anyone who feels, for any reason, that it would be inappropriate to discuss the matter with the offending person should promptly utilize the complaint procedure set forth below..

## IV. Internal Complaint Review Procedure

### A. Purpose and Scope

The purpose of the "Internal Complaint Review Policy" is to afford all contractors and affliates of WSP the opportunity to seek internal resolution of their complaints. This policy is intended to supplement the "Open Door Policy" set forth in this Handbook/Manual, which states the philosophy of WSP that all staffs, contractors, and volunteers have free access to their immediate supervisors or to other Company supervisors of their choice to informally express their work-related concerns.

### B. Procedure

#### 1. Filing of Complaint

A complaint should be written to the Executive Director as soon as possible after the events that give rise to the related concerns. The written complaint should set forth in detail the bases for the complaint.

#### 2. Investigation

The Executive Director dates and logs all written complaints and sends an acknowledgment that the complaint is under review.

The Executive Director or his/her/its designee investigates the complaint, meeting separately with the complainant and with others who either are named in the complaint or who may have knowledge of the facts set forth in the complaint. WSP will attempt to treat all internal complaints and their investigation as confidential, recognizing, however, that in the course of investigating and resolving internal complaints some dissemination of information to others may be appropriate.

On completion of the investigation, the Executive Director orally reports its findings and conclusions to the complainant. If the complaint is resolved, the terms of the resolution should be recorded and signed by both the complainant and a representative of the Executive Director.

### C. Appeal

If the complaint is not resolved to the satisfaction of the complainant, he/she may submit a written request for review of the complaint to the Chair of the Board of Directors. On completion of the appeal review, the complainant should receive an oral explanation of the conclusion reached and the reasons for that conclusion. Decisions resulting from appeal reviews by the Chair of the Board of Directors will be final.

### D. Non-Retaliation

No one will face any reprisal or retaliation for making a good faith or *bona fide* complaint to WSP of a threat or assault in violation of this policy at any time. Further, anyone who believes he or she has been subjected to an adverse action as a result of making a report pursuant to this policy should contact the Executive Director.

## V. Holidays and Vacation

### A. Holidays

WSP observes the following standard holidays and provides all full-time staff time off with pay at their normal base rate unless otherwise provided in this policy:

- New Years Day
- Martin Luther King Jr. Day
- Presidents Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- Friday immeidately followings Thanksgiving
- Christmas Day

#### 1. Weekends and Vacations

Holidays falling on a Saturday or Sunday are normally observed on the preceding Friday or the following Monday, respectively.

## B. Vacation

WSP does not provide vacation benefits to contractors or volunteers. However, WSP believes this time is valuable for its contractors as well, in order to enhance their productivity and to make their work experience with WSP personally satisfying. Please refer to your contract or immediate supervisor regarding your vacation schedule.

### 1. Vacation Scheduling

Scheduling of vacations is to be done in a manner consistent with WSP's operational requirements and the terms agreed upon by your supervisor. Vacation requests should be submitted by to your supervisor for approval at least two weeks prior to the commencement of a vacation period.

# VI. Workplace Rules and Procedures

## A. Rules of Conduct and Discipline

### 1. Policy

Contractors and Volunteers are expected to observe certain standards of job performance and good conduct. When performance or conduct does not meet Company standards, WSP will endeavor when in its sole discretion it deems appropriate to provide the contractor or volunteer with a reasonable opportunity to correct the deficiency. If, however, the contractor or volunteer fails to make the correction, he or she will be subject to discipline up to and including termination.

These rules are intended to you with fair notice of what is expected, however, such rules cannot identify every type of unacceptable conduct and performance. Therefore, you should be aware that conduct not specifically listed below but which WSP in its sole discretion determines adversely affects or is otherwise detrimental to the interests of WSP, other staff s, or customers, may also result in our terminating the relationship.

### 2. Performance

You may be separated for poor performance, including but not limited to the following:

- Unsatisfactory work quality or quantity;
- Poor attitude (for example, rudeness or lack of cooperation);
- Excessive absenteeism, tardiness, or abuse of break and lunch privileges;
- Failure to follow instructions or Company procedures; or
- Failure to follow established safety regulations.
- Failing to maintain proper licensing to perform your assigned task.

### 3. Misconduct

Contractors or Volunteers may be disciplined for misconduct, including but not limited to the following:

- Insubordination;

- Dishonesty;
- Theft;
- Discourtesy;
- Misusing or destroying Company property or the property of another on Company premises;
- Violating conflict of interest rules;
- Disclosing or using confidential or proprietary information without authorization;
- Falsifying or altering Company records, including the application for employment;
- Interfering with the work performance of others;
- Altercations;
- Harassing, including sexually harassing, staff s or customers;
- Being under the influence of, manufacturing, dispensing, distributing, using, or possessing alcohol or illegal or controlled substances on Company property or while conducting Company business;
- Gambling on Company premises or while conducting Company business;
- Sleeping on the job or leaving the job without authorization;
- Possessing a firearm or other dangerous weapon on Company property or while conducting Company business; or
- Being convicted of a crime that indicates unfitness for the job or raises a threat to the safety or well-being of WSP, its staff s, customers, or property; or
- Failing to report to WSP, within five days, any conviction under any criminal drug statute for a violation occurring in the workplace].

### 4. Attendance

Where appropriate, to the general rules stated above, contractors or volunteers may be separated for failing to observe the following specific requirements relating to attendance:

- Reporting to work on time, observing the time limits for rest and lunch periods, and obtaining approval to leave work early; and
- Notifying the supervisor in advance of anticipated tardiness or absence.

## B. Conflicts of Interest

Contractors and Volunteers are expected to use good judgment, to adhere to high ethical standards, and to avoid situations that create an actual or potential conflict between the staff 's personal interests and the interests of WSP. A conflict of interest exists when loyalties or actions are divided between WSP's interests and those of another, such as a competitor, supplier, or customer. Both the fact and the appearance of a

conflict of interest should be avoided. If you are unsure whether a certain transaction, activity, or relationship constitutes a conflict of interest should discuss it with their immediate supervisor or the Personnel Manager/Executive Director for clarification. Any exceptions to this guideline must be approved in writing by the Executive Director.

While it is not feasible to describe all possible conflicts of interest that could develop, some of the more common conflicts, from which staff s should refrain, include the following:

- Accepting personal gifts or entertainment from competitors, customers, suppliers, or potential suppliers;
- Working for a competitor, supplier, or customer;
- Engaging in self-employment in competition with WSP;
- Using proprietary or confidential Company information for personal gain or to WSP's detriment;
- Having a direct or indirect financial interest in or relationship with a competitor, customer, or supplier, except that ownership of less than one percent (1%) of the publicly traded stock of a corporation will not be considered a conflict;
- Developing a personal relationship with a subordinate that might interfere with the exercise of impartial judgment in decisions affecting WSP or any staff s/contractors/volunteers of WSP.
- Using Company assets or labor for personal use;
- Acquiring any interest in property or assets of any kind for the purpose of selling or leasing it to WSP; or
- Committing WSP to give its financial or other support to any outside activity or organization; or

Failure to adhere to this guideline, including failure to disclose any conflicts or failure to seek an exception, will result in discipline, up to and including termination of employment.

## C. Solicitation, Distribution and Bulletin Boards

In the interest of maintaining a proper business environment and preventing interference with work and inconvenience to others, you may not distribute literature or printed materials of any kind, sell merchandise, solicit financial contributions, or solicit for any other cause during working time.

## D. Security and Confidential Information

The security of property everyone shares responsibility to ensure that proper security is maintained.

### 1. Proprietary and Confidential Information

Company property includes not only tangible property, like desks and computers, but also intangible property such as information. Of particular importance are proprietary information and confidential information. Proprietary information includes all information obtained by employees, contractors, volunteers, etc.,during the course of their work. This Manual, for example, contains proprietary information. Confidential information includes all patient information, medical images and reports, which includes but is not limited to individually identifiable health information such as demographic information collected from an individual, and related to the past, present or future physical or mental health of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an

individual; and identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. Confidential information also includes any Company information that is not known generally to the public or the industry. Customer lists, customer files, personnel files, computer records, financial and marketing data, process descriptions, research plans, formulas, and trade secrets are examples of such confidential information.

Given the nature of WSP's business, protecting proprietary and confidential information is of vital concern to WSP. This information is one of the most important assets of WSP. It enhances WSP's opportunities for future growth, and indirectly adds to the job security of all staff s.

Contractors and Volunteers must not use or disclose any proprietary or confidential information that they obtain during employment with WSP, except as required by their jobs. This obligation remains even after contractual or volunteer relationship with WSP ends. If you are in a position that gives your access to particularly sensitive information, you may be required to sign a written nondisclosure agreement. In addition, all contractors and volunteers must observe good security practices. You are expected to keep proprietary and confidential information secure from outside visitors and all other persons who do not have a legitimate reason to see or use such information.

Company rules regarding document control, restricted access to areas of the facility, and other such procedures must be strictly observed. Failure to adhere to Company policies regarding proprietary and confidential information will be considered grounds for termination.

In addition to observing this policy, you will be asked to sign a written nondisclosure agreement.

### 2. Obligations on Termination

On termination of employment, whether voluntary or involuntary, all Company documents and other tangible Company property in possession or control must be returned to WSP.

## E. E-mail, the Internet, and Other Electronic and Telephonic Communications

The purpose of this policy is to provide information and guidance on (i) appropriate use of WSP's electronic and telephonic communications systems (the "Systems"), (ii) the Company's monitoring of its Systems, and (iii) appropriate data/information security protocols while using the Systems.

Inappropriate use of the Systems exposes WSP to certain risks, some of which could result in legal liability. These risks include malware attacks, data extrusion/theft and misuse, compromise of network infrastructure and services, and limitations to service availability. Therefore, it is the responsibility of every user of the Systems to be familiar with the guidelines set forth in this policy, and to conduct themselves accordingly.

Data security is an important aspect of appropriate use of the Company's Systems. Users will be trained on this topic from time to time. The Company's monitoring of the Systems, in large part, stems from the need to ensure an adequate level of data security.

If at any time, a user of the Company's Systems has any security-related or other questions about the use of the Systems, they should promptly see the Executive Director/Designee. Proper use of the Systems, and particularly information security, is a team effort involving the participation and support of every single user of the Systems.

### 1. Company Property

The Systems, as well as all communications and information transmitted by, received from, or stored in the Systems, are the property of WSP. While limited personal use of any software and business equipment, (including voicemail, telephone equipment, scanners, copy machines, facsimiles, computers, the Company's email system, internal or external Instant Messaging, the internet, smartphones, or other

personal handheld or wireless devices) is permissible, such use should be limited, and must not interfere with the user's work for the Company.

## 2. No Expectation of Privacy

During the course of carrying out their responsibilities, staff may access or monitor the Company's Systems. Therefore, users should have no expectation of privacy in any message, file, data, document, or any other form of information, whether Company-provided or personal, that is accessed, transmitted to, received from, or stored on any of the Company's Systems. For purposes of this policy, such messages, files, data, documents, and other forms of information are referred to as "Communications."

Neither the use, creation, or change of any password, code, or any other method of encryption; nor the ability to delete or purge Communications (whether authorized by the Company or not), should be interpreted as giving a user of the Systems any expectation of privacy in any Communications transmitted to, received from, or stored on the Company's Systems. All inbound and outbound email (Company-sponsored or otherwise) may be automatically tracked by, among other factors, sender name, receiver name, subject line, and subject matter. This information is maintained pursuant to the policies and procedures of the Company, and is considered public information to Company management. Therefore, any information sent via the Company's Systems may be utilized as the Company's needs dictate.

The Company reserves the right to review, audit, access and disclose all Communications sent or received via the Company's Systems without any prior notice to any sender or recipient of the Communication. The Company reserves the right to intercept and read email messages or listen to voicemail messages. Authorized Company representatives may review the email and telecommunication records of all users of the Systems to determine, among other things, whether there have been any breaches of security, violations of policy, or other misconduct on the part of any user.

Erasing a message from a user's email or voicemail system does not necessarily erase all copies of the message from the Systems. Archived copies may be stored for substantial periods of time, and are subject to the provisions of this policy regarding content, review, access, and disclosure. As business records, emails and voicemails are subject to court inspection and review by regulatory bodies. As such, nothing should be posted online, or sent by email or any other form of communication, that might embarrass you or another individual, or damage the Company's business interests.

In addition, there should be no expectation of privacy in any conversation conducted through the Company's Systems, including but not limited to, all telephone lines. It is unacceptable (and prohibited) for a user to engage in any form of harassment via the Systems, including by email, telephone, or Instant Message, whether such harassment takes the form of harassing language, or is harassing merely due to the frequency or size of such messages.

## 3. Use of Computer Systems

### *a. Monitoring*

The Company expressly reserves the right to monitor the use of its computers, mobile devices and telecommunication systems in its discretion, without prior notice. Such monitoring may include, but is not limited to, (1) reading and printing email; (2) monitoring and/or recording telephone calls; (3) reviewing voice mail stored on an staff 's telephone; (4) monitoring hits on Web sites; (5) monitoring mobile device use; and (6) monitoring instant messaging use. Further, information discovered may be shown to third parties, whether or not you are notified. As such, you should have no expectation of privacy with respect to the use of such equipment and systems.

### *b. Encryption*

WSP recommends that any information that users consider to be sensitive or vulnerable be encrypted. The Company has the ability to transmit encrypted emails outside of our network. If a user has information that needs to be encrypted before transmission, the user should contact the Executive Director.

### *c. Passwords*

The Company issues private passwords to users for access to its computer and telecommunications systems. These pass codes are intended to prevent unauthorized use of Company resources. All passwords are the property of the Company, and no user may use a password that has not been issued to them. Similarly, it is expressly prohibited for users to utilize equipment that is assigned to another user without express authorization to do so. Users are prohibited from hacking or breach testing the Company's computer and telecommunications network to gain unauthorized or elevated privileges to Company or outside electronic resources. Users are responsible for securing passwords. They must not be revealed, shared, posted, or stored in a manner that makes them easily available by others (including being sent in clear text). If a user is required to share or otherwise reveal a password, the user should contact the Executive Director. At no time should the password be stored or posted along with the user's account information.

Users will be required to change passwords that allow access to business data from time to time, at intervals directed by the Company (e.g., every six (6) months). These policies are subject to change at the direction of the Chief Technology Officer, and users are expected to comply with all requests that the Company may make relating to data security.

### *d. Network Access*

The Company's Systems provide access to WSP's confidential and business-critical information and assets. Only computer equipment with express authorization to be connected to the Company's network may be given access. All other equipment requires advance written approval by the Executive Director before it may be installed or connected. When staff, contractors, or volunteers leave the Company, off-boarding procedures will be followed to ensure that network access has been fully revoked.

### *e. Malicious Emails*

Although WSP has an appliance that scans all emails and attachments for viruses, email bombs, or Trojan horses, users must use extreme caution when opening email attachments received from unknown senders.

Users must immediately inform the Executive Director if they suspect that their computer has been compromised through any means (including malware or social engineering). Should any virus/worm/malware or malicious software be discovered on a user's computer or device that is causing network disruption or is attempting to spread across the network, that machine or device will be immediately taken offline to prevent disruption and potential spreading of malware. A spare machine or device will be provided to that user until the original can be repaired. Excessive offenses for malware-related incidents will be investigated, and appropriate disciplinary action will be taken, where warranted.

### *f. Preservation of Data*

Extensive backups of individual workstations and laptops are NOT routinely created. However, it is the responsibility of all personnel to ensure that all documents and records are correctly preserved.

Every user has access to a shared space on the Company network (known as [NAME(S)]) where important documents should be stored and where appropriate backups are taken.

All documents that users create or maintain in the course of their work must be saved in the appropriate file share for their department or group.

Other than for short periods for the purpose of editing, users must not store important documents or any corporate records on their workstation desktop or in the local "Documents" or "My Documents" folders.

If users have any doubt as to how to access their File Share, they should contact the Executive Director.

### *g. Unacceptable Use*

The following activities are generally prohibited. Users may be exempted from certain of these restrictions during the course of their legitimate job responsibilities.

Under no circumstances is a user authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing the Company's Systems.

The list below is by no means exhaustive. It attempts to provide a framework for activities that fall into the category of "unacceptable use."

The following System and network activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by WSP.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which WSP or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate member of the Company's management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
5. Revealing a user's account password to others or allowing use of an account by others. This includes family and other household members when work is being done at home.
6. Using WSP's Systems to actively engage in procuring or transmitting material that is in violation of applicable harassment, discrimination, or other equal employment opportunity laws or Company policies.
7. Making fraudulent offers of products, items, or services originating from any WSP account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning without prior notification to WSP's Executive Director.
11. Executing any form of network monitoring that will intercept data not intended for the user's host, unless this activity is a part of the user's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the user's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, customers' staff s to parties outside WSP.

### *h. Personal Files*

Users are responsible for exercising good judgment regarding personal use of WSP's equipment. If there is any uncertainty, users should consult the Executive Director immediately. Further, users should not have any expectation that personal files will be backed up or protected in any manner.

## 4. Use of the Internet

WSP provides access to the internet. The internet represents a useful tool for the Company in conducting its business, but like any other tool, it must be used properly. For purposes of this policy, the term "internet" includes all services provided on the internet, including, but not limited to the World Wide Web (www), file sharing, and streaming media.

Since all internet transactions conducted from the Company's network could be perceived as authorized Company activities, users must comply with all applicable local, state, federal and international laws, and regulations, as well as all applicable Company policies. Users must exercise care and responsibility, as well as the use of good judgment, common sense, and careful discretion when accessing the internet, browsing the Web, downloading and uploading files, and using other applications on the WSP network.

While limited personal use is permissible, internet access is generally to be used for WSP's business purposes. Users must not access, view, copy, upload, download, print, save, send, post, or otherwise transfer Communications that contain sexually explicit, derogatory, abusive, harassing, or similarly objectionable material or language, that defames or libels others, that infringes the privacy rights of others, or that is illegal or obscene. Use of the internet to attempt to gain unauthorized access to remote systems is also prohibited.

As a general rule, users may not forward, distribute, or incorporate into another work, material retrieved from a Web site or other external system. Very limited or "fair use" may be permitted in certain circumstances. Any staff desiring to reproduce or store the contents of a screen or Web site should contact the Executive Director to ascertain whether the intended use is permissible.

Use of the World Wide Web includes all restrictions that apply generally to the use of the Company's Systems, as noted above. In addition, the following rules apply with respect to internet usage:

1. No Browsing of Restricted Content Web Sites: The Company has blocked access to Web sites which contain pornographic material, hate speech, and other unacceptable content. However, the World Wide Web changes on a daily basis. In this connection, users who become aware of an un-blocked site containing pornographic materials are required to report such sites to the Executive Director.
2. No Downloading of Non-Business Related Data: The Company allows the download of files from the internet. However, downloading files should be limited to those, which relate directly to Company business.
3. No Downloading of Application Programs: The Company does not permit the download or installation on Company computers of application software from the internet. Such software may not only contain embedded viruses, but also is untested and may interfere with the functioning of standard Company applications.
4. No Participation in Web-Based Surveys without Authorization: When using the internet, the user implicitly involves the Company in his/her expression. Therefore, users should not participate in Web or email based surveys or interviews without authorization.
5. No Use of Subscription-based Services without Prior Approval: Some internet sites require that users subscribe before being able to use them. Users should not subscribe to such services without the express approval of the Executive Director.
6. No Violation of Copyright: Many of the materials on the internet are protected by copyright. Even though they may seem to be freely accessible, many of the intellectual property laws that apply to print media still apply to software and material published on the internet. Users are permitted to print

out Web pages and to download material from the internet for informational purposes as long as the purpose for such copying falls into the category of “fair use.” Please do not copy or disseminate material that is copyrighted. Users having any questions regarding such materials should contact the Executive Director for guidance.

The Company may use internet monitoring software to track all sites visited by its users. Therefore, all users should be aware that there is no expectation of privacy with respect to the internet access or use. The Company reserves the right to monitor each user’s use of the internet.

## 5. Electronic Mail Policy

WSP provides electronic mail (email) facilities to staff s for business purposes. Electronic communications provide an efficient way to communicate with others. Nevertheless, users must remember that the ease of using email is not a license for unprofessional conduct. Users should exercise good judgment, forethought, and common sense when creating and distributing email messages.

Whenever a user sends email, their name, user ID, and location are included in each email message. Users should also be aware that the messages can be as permanent as (or even more so than) conventionally mailed letters and materials.

Email can be archived in any system through which it passes. Deleting email from one’s inbox does not remove it from the Company’s Systems. Accordingly, users should consider each email message to be a letter and compose it accordingly. Users should not include anything in an email message that he or she would not want disclosed in a legal or other proceeding. This is true for external as well as internal email.

All users are responsible for making sure that the applicable Company disclaimer, if any, is utilized, and is located on each outgoing email.

Each user will be held accountable for ensuring that his or her use of the Company’s Systems is not offensive or rude.

### *a. Unacceptable Use of Company Email*

The following are unacceptable uses of Company email:

1. Sending "junk mail" or other advertising material to individuals who did not specifically request such material (email spam);
2. Sending or receiving harassing, threatening, obscene, racist, sexist, discriminatory, inappropriate, embarrassing or other objectionable messages via email to anyone (such messages include, but are not limited to, threats, jokes, cartoons, unwelcome propositions, chain letters and love letters);
3. Unauthorized use, or forging, of email header information;
4. Solicitation of email for any other email address, other than that of the poster’s account, with the intent to harass or to collect replies;
5. Use of unsolicited email originating from within the Company’s Systems or other Internet service providers on behalf of, or to advertise, any service hosted by the Company or connected via the Company’s network;
6. Actual or attempted forgery via email message;
7. Attempts to read, copy, modify or delete email messages of other users;
8. Proselytizing for commercial ventures or religious causes via Company email; and
9. Disseminating videos by email (except in limited circumstances in connection with the user’s job responsibilities).
10. Creating or forwarding “chain letters,” “Ponzi,” or other “pyramid” schemes of any type.
11. Solicitation of email for any other email address, other than that of the poster’s account, with the intent to harass or to collect replies.

12. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam) when such posting is likely to clog Company resources.
13. Sending Company-wide emails with large logos and/or photos, as such emails tend to take up a lot of space on the Company's exchange server.

## 6. Email Etiquette

Email is a tool that allows the Company to maximize client/customer services and provide fresh approaches to all of our efforts. When using Company email, however, certain things must be kept in mind:

1. Staff s who use email to communicate with clients and/or customers are expected to promptly respond to all messages.
2. Address emails to essential recipients only – beware of mechanisms that automatically identify a recipient when the first few letters are inserted.
3. Choose every word with care, and re-read every email before sending to be sure only the intended message is conveyed.
4. Use caution when attaching files, and open and review attachments prior to sending the email.

## 7. Email Etiquette

From time to time, the Company may tape, record, or otherwise monitor conversations or other communications between staff s and/or between staff s and non-staff s for legitimate business purposes, such as customer service training, to protect the integrity of certain business transactions (for example, sales orders taken over the telephone). In addition, Company telephone lines may be monitored and taped consistent with applicable federal and state law. Such monitoring or taping may also be the result of a Company investigation into allegedly unlawful or unethical activities, in conjunction with regulatory or other enforced authorities, or for any other business reason in the Company's sole discretion. The Company hereby reserves the right to monitor users' phone usage. By accepting and agreeing to the comply with this policy, the user consents to such taping and monitoring.

### a. Blogging/Social Networking/Social Media Policy

The Company encourages everyone to make positive use of the Internet, and welcomes the dissemination and exchange of ideas that this mode of communication makes possible. At the same time, the WSP's legitimate interests can, in certain circumstances, be compromised by inappropriate uses of these media. As stated otherwise in this Manual everyone is expected to use good judgment, both in person and online.

Accordingly, this blogging/social networking/social media policy is intended to respect everyone's rights to personal expression while limiting the WSP's legal liability and protecting the Company's proprietary information and business interests. Importantly, this policy applies to all Company contractors, staff, volunteers, etc. and pertains to blogging/social media/social networking:

- Performed both on and off WSP time;
- Performed both on and off the WSP's premises; and
- Regardless of whether it is performed on WSP equipment (computers, smartphones, tablets, etc.), or on the staff 's or any third party's equipment.

For purposes of this policy, the term "social networking" includes, but is not limited to, the use or viewing of such sites as Facebook, Twitter and LinkedIn.

Blogs/posts may not contain any content that:

- violates any laws, including laws pertaining to intellectual property;
- infringes any third party rights (including intellectual property rights);
- is defamatory or libelous or might be construed as harassment or disparagement in violation of WSP policy on the basis of race, color, religion, sex, sexual orientation, national origin, age, disability, genetic information, or any other status protected by applicable law;
- violates any policies, rules, standards or requirements applicable to the Company, including but not limited to any confidentiality or privacy policy, or the terms of any confidentiality agreement entered into by an staff ;
- discloses any trade secrets, "insider information" or similar confidential or proprietary information of the WSP;
- supports or comments favorably on a competitor of the Company or its affiliates; or
- is adverse to the reputation of the products and/or services provided by the Company.

The following are permitted only with the express prior written permission of both the Executive Director:

- Blogs or social networking that imply sponsorship or support by the WSP;
- Blogs or social networking that use any logos or trademarks of the WSP or its affiliates in any manner that expresses or implies that the communication is from or is endorsed by the Company; or
- Blogs or social networking that use the WSP's time, facilities, resources, or supplies.

If a blog or social networking post refers to the WSP or its operations, personnel, products or services, and the staff 's name is generally associated by the general public with the Company (an staff who is unsure of whether this applies to him or her should consult the Executive Director, the staff blogger/poster must (i) notify his or her manager and the Legal Department of the existence of the blog or post, and (ii) include a statement in the blog/post that all views expressed are those of the blogger/poster and have not been reviewed or approved by the Executive Director. Similarly, if staff blogs or otherwise posts online an endorsement of the WSP or its products, the staff must identify him- or herself as a Company staff.

Unless blogging or posting as part of his or her job at WSP, blogs or posts may not be crafted so as to appear as if they were being made by the Company or on its behalf. If any blog or post would appear as if

it is being made on behalf of the Company, the blogger/poster must include a statement in the blog/post that all views expressed are those of the blogger/poster and have not been reviewed or approved by the Company.

Management reserves the right to require an employee, contractor, volunteer, etc., to stop posting any blog or post which contains content that it deems to violate this policy.

This policy is a statement of legal and ethical principles for individual and business conduct. Failure to comply with this policy may subject an employee, contractor, or volunteer to disciplinary action, up to and including termination of employment. If you have any questions regarding this policy, please contact the Executive Director.

Nothing in this policy is meant to prevent staff s from discussing the terms and conditions of their employment as permitted by law or engaging in any other activities protected under Section 7 of the National Labor Relations Act or any other applicable federal, state or local law.

**b. Bring Your Own Device**

In order to be entitled to use a personal mobile electronic device to access information that constitutes Confidential Information of WSP (as that term is defined in the WSP CONFIDENTIALITY AGREEMENT/POLICY, staff s must sign a document acknowledging and agreeing as follows:

1. Only mobile devices which have been authorized by the Company can be synchronized with the Company's systems. The Company reserves the right to reevaluate its authorized device list, and if a change is made that affects an staff 's device, the staff must provide his or her device to the Company so that it may be disconnected from the Company's systems.
2. Since staff s' mobile devices have the ability to access Confidential Information of the Company, staff s must utilize security access codes on their devices. If the Company establishes any rules pertaining to security codes (such as length and/or complexity), staff s must comply with such rules, and permit the Company's IT staff to confirm such compliance.
3. Since staff s' devices have access to Company Confidential Information, staff s may not give their devices to anyone else to use.
4. If an staff is unable to access his or her device for any reason, including a failure to properly enter the security access code, only the Company's IT staff should address the situation and reconfigure a new security access code.
5. Only the Company's IT staff is authorized to configure a mobile device for synchronization with the Company's systems.
6. Staff s may not provide their login information to anyone, including family members and the staff in the store where the device was purchased. Staff s may be required to provide their login information to the Company's IT staff.
7. If an staff loses his or her device, the staff must contact the Company's IT staff immediately. The device may be wiped of all data (or if possible, only Company data) by the IT staff. (All Company data remains on the Company's systems, and can be synchronized with the staff 's new device (or with the old one if it is found)).
8. When an staff 's employment with the Company terminates for any reason, the staff must provide the Company's IT staff with access to his or her mobile device, so that all Confidential Information of the Company can be removed from the device.
9. Staff s must, to the extent possible based on their device's specifications, include user information, such as my telephone number, on the home screen of the mobile device, so that even when it is locked, a person who finds the device can contact the staff to return it.

**Conclusion**

This policy is a statement of legal and ethical principles for individual and business conduct. Failure to comply with this policy may subject staff to disciplinary action, up to and including termination of employment. If you have any questions regarding this policy, please contact the Human Resources Department or the Legal Department.

## F. Drug-Free Workplace

It is the policy of WSP to create a drug-free workplace. The use of controlled substances is inconsistent with the behavior expected of contractors and volunteers, subjects everyone coming to our facilities to unacceptable safety risks, and undermines WSP's ability to operate effectively and efficiently. In this connection, the unlawful manufacture, distribution, dispensation, possession, sale, or use of a controlled substance in the workplace or while engaged in WSP business off WSP's premises is strictly prohibited. Such conduct is also prohibited during nonworking time to the extent that in the opinion of WSP, it impairs an staff 's ability to perform on the job or threatens the reputation or integrity of WSP.

If you have been convicted of controlled-substance-related violations in the workplace, including pleas of *nolo contendere* (i.e., no contest), must inform WSP within five days of such conviction or plea. Violating any aspect of this policy may be subject to disciplinary action, up to and including termination of the relationship.

## G. Inspections and Searches on Company Premises

### 1. Purpose of the Guideline

WSP believes that maintaining a workplace that is free of drugs, alcohol, and other harmful materials is vital to the health and safety of its staff s and to the success of WSP's business. WSP also intends to protect against the unauthorized use or removal of Company property. In addition, WSP intends to assure its access at all times to Company premises and Company property, equipment, records, documents, and files. Accordingly, WSP has established this Guideline concerning inspections and searches, on Company premises. This Guideline applies to all staff s of WSP.

### 2. Definitions

For purposes of this Guideline:

"Prohibited materials" means firearms or other weapons; explosives and/or hazardous materials or articles; illegal drugs or other controlled substances as defined in WSP's Drug-Free Workplace Guideline; drug-related paraphernalia; and alcoholic beverages or Company property that an staff is not authorized to have in his or her possession.

"Company property" includes all documents, records, software, and files relating to WSP's business; and all equipment, hardware, and other property of any kind, whether owned, leased, rented, or used by WSP.

"Company premises" includes all premises and locations owned or leased by WSP or under the control of WSP, including parking lots, lockers, and storage areas.

"Reasonable suspicion" includes a suspicion that is based on specific personal observations such as an staff 's manner, disposition, muscular movement, appearance, behavior, speech or breath odor; information provided to management by an staff , by law enforcement officials, by a security service, or by other persons believed to be reliable; or a suspicion that is based on other surrounding circumstances.

"Possession" means that an staff has the substance or company property on his or her person or otherwise under his or her control.

## 3. Inspections and Searches

### a) Access to Company Property

In order to ensure access at all times to Company property, and because staff s properly in possession of Company property or information related to company business may not always be available to produce the property or information when needed in the ordinary course of WSP's business, WSP reserves the right to conduct a routine inspection or search at any time for Company property on Company premises. WSP reserves the right to access information and communications stored on company technology resources, at all times.

Routine searches or inspections for Company property may include an staff 's office, desk, file cabinet, closet, computer files, voice mail, or similar places where staff s may store Company property or Company-related information.

Because even a routine search for Company property might result in the discovery of an staff 's personal possessions, all staff s are encouraged to refrain from bringing into the workplace any item of personal property that they do not wish to reveal to WSP.

### b) Inspections and Searches for Prohibited Materials

- Inspections or searches for prohibited materials in or on Company premises also will be conducted whenever WSP has reasonable suspicion that a particular staff or staff s may be in possession of such materials in violation of this Guideline.

- Inspections or searches for prohibited materials may be conducted by an independent security service or by WSP with its own personnel. In all cases, a member of management should be present.

- Inspections or searches for prohibited materials may include an staff 's office, desk, file cabinet, closet, or other locations where staff s may place personal possessions, including, but not limited to, staff lockers and vehicles, when on company premises, and/or other items of personal property worn or carried while on company premises.

- Staff s who refuse to cooperate during an inspection or search will not be forcibly detained or searched. They will be informed, however, that WSP will base any disciplinary decision on the information that is available, including their refusal to consent to the search as well as the information that gave rise to a reasonable suspicion that the staff was in possession of prohibited materials, if applicable, and that their failure or refusal to cooperate could deprive WSP of information that may clear them of suspicion. In addition, WSP reserves the right to take appropriate action to prevent the unauthorized removal from Company premises of Company property.

### c) Disciplinary Action

- Contractors, Volunteers, or Staff who are found to be in possession of prohibited materials in violation of this Guideline or have used Company property in an unauthorized manner and/or are found to be in violation of other WSP policies and guidelines will be subject to discipline, up to and including discharge, regardless of WSP's reason for conducting the search or inspection.

- If an you refuse to cooperate with a search or inspection that is based on reasonable suspicion that you are in possession of prohibited materials, WSP may take that refusal into consideration in determining appropriate action. The action taken will be based on all available information, including the information giving rise to the reasonable suspicion. It is therefore to the staff 's advantage to cooperate with the search or inspection whenever prohibited material are present.

## H. Termination

### 1. Voluntary Termination

WSP will consider the following as a voluntary Termination:

- Elects to resign from WSP;
- Fails to return from an approved leave of absence on the date specified by WSP; or
- Fails to report for work without notice to WSP for three consecutive days.

### 2. Involuntary Termination

You may be terminated involuntarily for reasons that include poor performance, misconduct, or other violations of WSP's rules of conduct, as set forth below. Notwithstanding this list of rules, WSP reserves the right to discharge with or without cause and with or without prior notice.

### 3. Termination Due to Reorganizations, Economics, or Lack of Work

From time to time, WSP may need to terminate a relationship as a consequence of reorganizations, job eliminations, economic downturns in business, or lack of work. Should WSP consider such terminations necessary, WSP will attempt to provide all affected with advance notice when practical.

# VII. Workplace Safety

## A. Policy

WSP is committed to providing and maintaining a healthy and safe work environment for everyone. You also are required to report immediately to your supervisor any potential health or safety hazards, and all injuries or accidents. First aid supplies are located in the kitchen. Safety Rules

Safety is to be given primary importance in every aspect of planning and performing all WSP activities. We want to protect you against industrial injury and illness, as well as minimize the potential loss of production. Please report all injuries (no matter how slight) to your manager immediately, as well as anything that needs repair or is a safety hazard. Below are some general safety rules. Your manager or department head may post other safety procedures in your department or work area:

- Avoid overloading electrical outlets with too many machines.
- Use flammable items, such as cleaning fluids, with caution.
- Walk – don't run.
- Report to your manager if you or a co-worker becomes ill or is injured.

- Ask for assistance when lifting heavy objects or moving heavy furniture.
- Keep cabinet doors and file and desk drawers closed when not in use.
- Sit firmly and squarely in chairs that roll or tilt.
- Avoid “horseplay” or practical jokes.
- Start work on any machine only after safety procedures and requirements have been explained (and you understand them).

Remember, failure to adhere to these rules will be considered serious infractions of safety rules and will result in disciplinary actions.

# VIII. Miscellaneous

## A. Open Door Policy

We want to hear from you. If you think of a better way of doing your job or have ideas about how the Company can improve its operations, reduce costs, or make other beneficial changes, WSP welcomes your input and suggestions. Further, misunderstandings and conflicts can arise in any organization. In order to work together effectively, it is important to resolve such matters before serious problems develop. If a situation persists which you believe to be detrimental to you or the Company, a candid discussion with your manager is encouraged.

If for any reason, a staff member feels he or she cannot discuss an issue with his or her manager, or if the situation is not resolved satisfactorily by the staff’s manager, the staff member should contact the Executive Director. Any questions, suggestions and concerns will be handled professionally and confidentially to the extent possible and practical. Retaliatory action against staffs expressing concerns in good faith will not be tolerated.

## B. Workplace Violence

**Background**

WSP is concerned about the increased violence in society, which has also filtered into many workplaces throughout the United States. WSP has taken steps to help prevent incidents of violence from occurring at its various locations. In particular, WSP has adopted this Workplace Violence policy in order to:

- raise staffs’ awareness regarding the threat of workplace violence;
- empower staff against the threat of workplace violence; and
- establish clear protocols in the event staff members are faced with, or otherwise become aware of, the threat or infliction of workplace violence.

“Workplace violence” is any violent threat or act directed toward persons at work or otherwise on duty. Such acts can range from an attempt or threat to inflict physical injury to actual wrongful physical contact (regardless of whether such contact actually causes a physical or emotional injury). Importantly, this includes verbal and non-verbal threats (including threats made online) and related actions. It also includes bullying behavior. Therefore, bullying of coworkers is expressly prohibited at WSP.

**Statement of Our Policy**

WSP has zero tolerance for workplace violence. In other words, WSP expressly prohibits any acts or threats of violence against any person in or about any of WSP’s locations at any time.

**Where do Threats Come From?**

We recognize that, aside from acts or threats of violence, such acts or threats of violence can also be made towards staffs by visitors, customers, business partners, persons formerly affiliated with WSP, or persons in an staff member's personal life (e.g., a current or former spouse, partner, boyfriend, or girlfriend). As a result, it is important to be aware that domestic violence, sexual violence, dating violence, and stalking can result in an instance of workplace violence.

**Obligations of Staff s Subject to this Policy**

In keeping with WSP's commitment to provide a safe and healthful work environment, the following protocol must be followed in the event that you becomes aware of any threat of violence against any staff by any person:

1) Anyone working at WSP as a staff member, contractor or volunteer, who becomes aware of an actual threat of violence against any other staff has a duty to warn WSP by contacting WSP's Executive Director. Reports made pursuant to this policy will be held in confidence to the maximum extent possible and practical under the circumstances.
2) Threats do not only come from co-workers. If you have been threatened by a person in your personal life, or if you become aware that a colleague has been threatened by someone in his or her personal life, such as a stalker or an unstable significant other, you are obligated under this policy to warn WSP by contacting WSP's Executive Director.
3) Any threats of violence made online or in any electronic format such as by e-mail, text-message or via social media, as well as verbal threats made over recorded phone lines are subject to the requirements set forth in this Workplace Violence policy. With respect to such threats, to the extent possible, staff s should take steps to preserve and maintain such threats and should forward same to the Executive Director.
4) In addition to contacting the Executive Director, if you believe you are in immediate harm, or that another staff is in immediate harm, you may always contact 911 or their local police precinct directly.
5) Staff s and visitors are prohibited from carrying unauthorized firearms or other weapons into WSP locations. Any person found doing so in violation of this Policy and/or applicable laws will be prosecuted to the maximum extent permitted by law.
6) Contractor, Volunteers, or Contractors are prohibited from utilizing any workplace resources, such as work time, phones, e-mail, computers, fax machines or other means, to threaten, harass, intimidate, or otherwise harm another person.

**No Retaliation**

You will not face <u>any</u> reprisal or retaliation for making a good faith or *bona fide* complaint to WSP of a threat or assault in violation of this policy at any time. Further, if you believe that you have been subjected to an adverse action as a result of making a report pursuant to this policy should contact the Executive Director.

**Additional Information**

WSP will take prompt remedial action, up to and including immediate suspension or termination, with respect to any staff who engages in any threatening behavior or acts of violence or who uses any obscene, abusive, or threatening language or gestures. Such action may also include notifying the police or other law enforcement personnel and prosecuting violators of this policy to the maximum extent permitted by law.

WSP has established viable security measures to ensure that WSP's locations are safe and secure to the maximum extent possible and to properly handle access to WSP locations by the public, off-duty staff s, and former staff s. If any staff wishes to obtain further information on our security measures, or has any questions or concerns, he or she may contact the Executive Director.

Any staff s with questions about this policy or the procedures described in this policy should contact the Executive Director.

## C. Contact with Media

Contact with the media is not to be initiated by anyone without first informing the Executive Director or designee and discussing the best method of approach.

If a representative of the media approaches you should refer the media to the Executive Director for a statement of agency policy or position. In all instances, the Executive Director should be informed of the media contact.

**Contact with the Public**
Employees asked by an outside agency or organization to appear on behalf of the Washington School of Psychiatry must bring the request to the Executive Director before agreeing to participate.

## D. Contracting Authority

The school has to develop uniform standards of practice that limit our liability and exposure to risk.
The only person who has the authority to bind the organization contractually is the Executive Director. All costs associated with contracted speakers or any person delivering a service on behalf of the school or the clinic must be approved by the Executive Director - in writing.