Standards of Conduct

You must comply with all applicable state and federal laws while you are acting in the course and scope of your employment with the Company. Like all organizations, the Company requires order and discipline to succeed and to promote efficiency, productivity and cooperation among employees. For this reason, it may be helpful to identify some examples of types of conduct that are impermissible and that may lead to disciplinary action, up to and including immediate termination. Although it is not possible to provide an exhaustive list of all types of impermissible conduct and performance, the following are some examples (in alphabetical order):

- Activity that might result in adverse publicity or notoriety to the Company or otherwise tends to bring the Company into public disrepute.

- Altering or falsifying any time-keeping record; utilizing another employee's password to approve your or anyone else's time record; intentionally punching or recording another employee's time record; allowing someone else to punch or record your time record; supervisors approving incomplete time records or records they know to be inaccurate; removing any timekeeping record from a designated area without proper authorization or destroying such a record.

- Bringing or possessing any weapon (including knives, firearms or any other explosives, and/or dangerous materials or articles of any type) on Company property (including on location or in Company parking lots or structures) or while conducting Company business, consistent with applicable law. The only exceptions to this are: (i) weapons possessed by authorized security personnel; and (ii) weapons or other dangerous materials used solely as props on a Company production, during the production.

- Committing the Company to give its financial or other support to any outside organization or political, religious or other group or activity without the Company's authorization.

- Disloyalty, including release or misuse of confidential information or trade secrets about the Company or its customers in violation of Company policy.

- Engaging in abusive conduct, including threatening, humiliating, or intimidating behavior.

- Engaging in illegal activity.

- Engaging in unauthorized overtime work.

- Failing to cooperate truthfully and completely in a Company investigation, including intentionally withholding information the Company deems relevant.

- Falsifying or making a material omission on a document submitted to the Company, including but not limited to an employment application, resume, expense report or medical documentation supporting any absence from work.

- Fighting or making threats of harm on or while using Company property, while on duty or conducting Company business or in a manner that impacts the work environment, even if there is not intent to harm.

- Harassment of, or discrimination or retaliation against, any job applicant, employee, unpaid intern, volunteer, or other non-employee third parties with whom you interact in the workplace.

- Insubordination, including improper conduct toward a supervisor or refusal to perform tasks assigned by a supervisor in the appropriate manner.

- Leaving your worksite without authorization during work time (which does not include meal or rest periods).

- Misusing, destroying, damaging or losing property of the Company, an employee, a customer, vendor or visitor.

- Possession, distribution, manufacture, purchase, sale, use, transfer, solicitation or being under the influence of illegal drugs or legally obtained marijuana while on Company property, on duty, or operating a vehicle or potentially dangerous equipment leased or owned by the Company or wherever such conduct might adversely affect your job performance or the Company's interests. For purposes of this policy, the term "illegal drugs" means any drug: (i) that is not legally obtainable; or (ii) that is legally obtainable but has not been legally obtained. The term also includes prescribed drugs not legally obtained and prescribed drugs not being used for prescribed purposes.

- Representing the Company or discussing Company affairs with the media without the Company's authorization.

- Selling for personal profit the Company's property (e.g., DVDs or Blu-Rays, t-shirts, tickets, other promotional materials) that has been given to you for your personal enjoyment and use. If you do not want Company property that is offered or given to you, please do not accept it or return it to your supervisor. Purchasing Company property using an employee discount (e.g., at the Studio Store) and reselling that property for more than what you paid for it is similarly prohibited. It is acceptable to donate Company property (e.g., to a charity) given to you provided the Company has not otherwise put restrictions on your use of it.

- Sleeping on the job.

- Theft, unauthorized removal, possession or loss of Company property or the property of any employee, Company customers or vendors, or anyone else on Company property.

- Unauthorized expenses; falsification of expense reports or other financial documents; willful or habitual disregard of the Company's budget guidelines; or other financial improprieties.

- Unauthorized possession, distribution, downloading, uploading, purchase, sale, use, transfer or solicitation of any copyrighted content.

- Unauthorized possession, distribution, manufacture, purchase, sale, use, transfer, solicitation or being under the influence of alcohol while on Company property, on duty, or operating a vehicle or potentially dangerous equipment leased or owned by the Company or wherever such conduct might adversely affect your job performance or the Company's interests.

- Unauthorized/unprotected absenteeism or tardiness.
- Unlawful recording of a conversation.
- Unsatisfactory performance, including but not limited to failing to adequately perform job duties, unprofessional conduct and/or poor attitude.
- Violation of a Company or 21st Century Fox policy.

Confidentiality Obligations of Employees

Confidential Information: During the course of employment, you may become aware of or have access to proprietary information that belongs to the Company or other third parties with which the Company does business, including, without limitation, information concerning the operations, processes, methods and accumulated experience incidental to the creation, sale and distribution of the Company's or a third party's products; matters not generally known to the public or the industry in which the Company is or may become engaged and which pertain to the Company's or a third party's products, including but not limited to non-public information relating to entities (e.g., sports teams) or persons (e.g., actors, athletes) who are doing business with or may do business with the Company; information related to the creation, promotion, marketing, selling and distributing of the products, in forms including but not limited to customer lists, prospect lists, price and discount lists, sales figures, market research, competitive information and other trade secrets. This information is collectively referred to as "Confidential Information." Confidential Information can be in tangible or electronic form, or conveyed verbally.

Be aware that Confidential Information includes but is not limited to all of the Company's creative works that have not been released to the public – including, for example, electronic or physical copies of feature films and television content, and associated materials such as scripts, props or plots.

Duty to Not Disclose Confidential Information: All employees shall keep Confidential Information secret. At no time may an employee directly or indirectly, individually or in combination or association with any other person or entity, divulge or disclose to any third party any Confidential Information or otherwise permit the exploitation, copying or summarizing of any Confidential Information without, in each instance, the prior written consent of the Company. No employee shall use or remove from the Company's premises any of the Company's or other third party's Confidential Information for any non-business related or other inappropriate reason.

Similarly, you should not disclose or otherwise use in your job at the Company any confidential information of any other company or person, including any prior employer(s), without the prior written consent of that company or person, or unless and until that confidential information becomes public through legitimate means.

Company's Ownership of Its Confidential Information: All the Company's Confidential Information is a valuable asset of the Company and is, will be and will at all times remain, the sole and exclusive property of the Company. The Company derives significant financial benefits, good will and a competitive advantage in the marketplace by maintaining its Confidential Information as secret and unavailable to the Company's competitors and the public, and relies on employees to safeguard the Company's Confidential Information entrusted to them.

Obligations Survive Termination: At the time of an employee's resignation or termination for any reason, or upon request of the Company at any time, the employee shall immediately deliver to the Company all Confidential Information in their possession or control. An employee's obligations to safeguard the Company's Confidential Information continue in effect after the termination of an employee's employment.

Remedies: Money damages are insufficient to compensate the Company for the damages it will suffer for breaches of this policy. Therefore, in consideration for continued employment with and compensation

by the Company, in the event the Company seeks to enjoin a breach of this policy, employees may not argue that an injunction is not appropriate because the Company has an adequate remedy at law. Furthermore, the Company is entitled to not less than $10,000 in liquidated damages per breach of this policy as a reasonable estimate of its direct damages associated with the breach of this policy (e.g., costs associated with discovering and investigating the disclosure of Confidential Information). The Company's rights and remedies under this policy are cumulative, in addition to, and do not exclude or waive, other rights and remedies the Company may have for misuse of its proprietary information, including without limitation its rights under criminal and civil trade secrets or theft of property laws.

Notice of Immunity: Federal law provides that no individual may be held criminally or civilly liable under any federal or state trade secret law for directly or indirectly disclosing, in confidence, a trade secret to any federal, state or local government official, or to an attorney, where such disclosure is solely for the purpose of reporting or investigating a suspected violation of law, or is made in a complaint or other document filed under seal in a lawsuit or other proceeding. Nothing in this policy shall be construed to conflict or otherwise interfere with any individual's rights under federal law as provided herein.

Terms and Conditions of Employment Are Not Confidential Information: The terms and conditions of any employee's employment with the Company, including their wages, are not Confidential Information. Nothing in this policy shall be construed to conflict or otherwise interfere with the rights of employees or other individuals retained by the Company to discuss those terms and conditions as they so choose.

Harassment, Discrimination, and Retaliation

The Company is committed to providing a workplace that is free from all forms of harassment, discrimination and retaliation. Conduct under this policy that is harassing or discriminatory based on a person's actual or perceived race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex (including pregnancy status, childbirth, breastfeeding, and related medical conditions), gender, gender identity, gender expression, age, sexual orientation, military or veteran status, or any other legally protected characteristic (collectively, "Protected Characteristics") may violate federal, state and/or local laws. The Company does not tolerate such harassment or discrimination by managers, supervisors or co-workers, and will attempt to prevent and address any such harassment by non-employees. The Company prohibits such harassment, discrimination, and retaliation against job applicants, employees, unpaid interns and volunteers, and other non-employee third parties with whom you interact in the workplace. The Company also does not tolerate retaliation against any employee for engaging in protected activity as defined below or under applicable law.

Unlawful Harassment: The Company prohibits harassment based on Protected Characteristics in any form, including verbal, visual or physical harassment. Conduct that may violate this policy includes:

- Verbal conduct: using demeaning, derogatory, degrading, obscene or threatening terms; making comments, epithets, slurs or jokes; offering or denying employment benefits in exchange for sexual favors; making or threatening reprisals after receiving a negative response to a sexual advance; or making comments about an individual's body or physical attributes;

- Visual conduct: displaying or forwarding demeaning, derogatory, degrading or obscene letters, notes, emails, screen savers, images, invitations, statements or pictorial depictions, including sexually explicit, violent or offensive pictures, videos, objects, cartoons or posters; or leering or making sexual gestures;

- Physical conduct: assaulting another person; impeding or blocking movements; or unwanted touching.

Harassing conduct may include situations where: (i) submission to the conduct is made a term or condition of employment; (ii) submission to or rejection of the conduct is used as the basis for any employment decisions; or (iii) the conduct has the purpose of interfering or tends to interfere with work performance or tends to create an intimidating, hostile or offensive working environment. Your workplace may at times extend beyond the Company's premises, including, for example, to Company-sponsored or other meetings or events relating to the Company's business conducted away from the Company's premises.

Conduct that may not constitute unlawful harassment (e.g., because it is not unwelcome or because it is not sufficiently severe or pervasive to meet the legal standard) may nevertheless violate this policy.

Unlawful Discrimination: The Company prohibits discrimination based on Protected Characteristics and is committed to adhering to and enforcing its obligations under applicable non-discrimination laws. The Company hires, trains, promotes and compensates employees without regard to any Protected Characteristic.

Unlawful Retaliation: The Company prohibits retaliation for engaging in protected activity, which includes opposing harassment or discrimination, making a complaint under this policy or participating in an investigation, proceeding or hearing conducted by the Company, the California Department of Fair Employment and Housing ("DFEH"), the Equal Employment Opportunity Commission ("EEOC") or any other state or federal agency.

Procedure for Addressing Harassing, Discriminatory or Retaliatory Conduct: In all cases in which you believe you have experienced or witnessed harassment, discrimination or retaliation, you must immediately report the facts and the names of the individuals involved to a manager in the Human Resources Department. If you are uncomfortable reporting your complaint to Human Resources, you must contact an attorney in the Employment Law section of the Fox Group Legal Department, who will identify an appropriate person to address your complaint. Members of management who learn of harassing, discriminatory or retaliatory conduct from any source are required to inform a manager in the Human Resources Department immediately. If a manager is uncomfortable reporting the complaint to Human Resources, they must report it to an attorney in the Employment Law section of the Fox Group Legal Department.

Investigation: Reported incidents of harassment, discrimination and/or retaliation will be investigated in a fair, complete, and timely manner by impartial, qualified personnel, with due process given to all parties involved and due consideration given to the surrounding circumstances. Investigations will be documented for progress as appropriate, and the Company will maintain the confidentiality of its investigations to the extent possible. All employees have an obligation to participate truthfully, accurately and completely in all Company investigations. If the Company reasonably determines that a violation of this policy has occurred based on the evidence it has collected, the Company will take appropriate remedial action, up to and including termination of employment.

DFEH, EEOC, and Analogous Agencies: In California, job applicants, employees, unpaid interns or volunteers who believe they have been unlawfully harassed, discriminated or retaliated against may also file a complaint with the DFEH. The DFEH has the authority to endeavor to end unlawful employment practices it determines to have occurred by conference, conciliation, or persuasion, as well as the authority to seek remedies on behalf of employees or job applicants, including back pay and other monetary damages, fines, and orders relating to hiring or reinstatement, promotion and/or changes to an employer's policies or practices. For more information, please contact the DFEH (or analogous governmental agency in your state). Contact information for the DFEH may be found on the Internet.

In all states, employees or job applicants who believe they have been unlawfully harassed, discriminated or retaliated against may also file a complaint with the EEOC, which has authority similar to the DFEH and analogous governmental agencies in other states. Contact information for the EEOC may also be found on the Internet.

Electronic Communications

This policy applies to all employees of the Company, independent contractors and consultants retained by the Company, unpaid interns and volunteers, and other outside service providers who access or use Company's Systems in the United States (collectively, "Users"). All Users shall use the Company's Systems in a professional, responsible and lawful manner in accordance with this policy.

The Company's electronic communications systems include all devices, software and services accessing, utilizing or connected to the Company's Systems, including but not limited to desktop computers and workstations, laptop computers, USB drives, file servers, networks, software and other information technology hardware, Internet and intranet access and usage, telephone systems, cell phones, smartphones (e.g., Blackberries and iPhones), tablets (e.g., iPads), personal digital assistants (PDAs), voicemail, and cloud storage and collaboration tools (collectively, the "Systems").

Electronic communications include emails, instant messages, text messages, blogs, posts, comments posted on "guestbooks" or discussion forums, messages or communications sent through social or multimedia networking websites (e.g., Facebook, Twitter, LinkedIn, hi5, Second Life, Flickr, Instagram, Tumblr, Snapchat, YouTube) or any other website where content can be posted, faxes, documents, files, programs and other data that reside on, or are transmitted through, electronic communication systems (collectively, the "Electronic Communications").

"Personal Devices" include equipment or tools used to create or distribute Electronic Communications that are not Company-provided, including but not limited to individually-owned computers, USB drives, software, tablets and other mobile devices (e.g., iPhones, Blackberries, and Android devices).

The Company has established this policy to:

- advise Users on the acceptable use of Company Systems and the Company's position on monitoring of those Systems;

- set standards for the acceptable use of Company Systems;

- protect the Company's Systems from misuse, unauthorized access, alteration, theft, copyright violation and sabotage;

- protect its employees and other Users from unlawful conduct, including discrimination, harassment and retaliation.

Questions concerning this policy should be directed to a manager in the Company's Human Resources Department. Any violation of this policy by an employee may result in disciplinary action up to and including immediate termination of employment and/or legal action. Any violation of this policy by an independent contractor, outside service provider, or other User may result in the termination of their services and/or legal action.

Company Property, Privacy and Monitoring: The Systems provided by the Company, the associated equipment and software, and all the Electronic Communications transmitted by, stored or received on such Systems, are to be used for Company business and shall remain at all times the exclusive property

of the Company. Accordingly, the Company (including any of its designees) has the right, without notice, in its sole discretion and without regard to content: (1) to monitor and access the existence and content of any use of these Systems, including voicemail, email and messages sent or received (whether using a Company account, a non-Company account or a social networking website), documents, files or programs stored on an employee's Company computer, USB drives, or network drives, or on any Personal Device accessing, utilizing or connected to Company Systems; (2) to access and monitor Internet usage and to block access to any Internet site; (3) to copy, transfer, and/or disclose to any third party any Electronic Communication transmitted or stored by or on its Systems, including if that third party is located outside the country where the Electronic Communicated was originally collected; (4) to download, print, and examine email and other messages; (5) to use automated monitoring tools and applications to search for words or patterns that indicate a violation of this or any other Company policy or to protect the security of Company Systems and its personal or business information; and (6) to remotely reset (or "wipe") any Company System or Personal Device on which the Company believes Company information has been or is being stored. These Company rights support, among other functions, maintenance, operations, auditing, investigative activities, cybersecurity, staff training or assessment, compliance with Company policies and applicable law, prevention or detection of crime and otherwise further the Company's business interests. The Company's right to access, monitor, copy and/or disclose use of its Systems, and all Electronic Communications or content transmitted by or stored on the Company's Systems, exists whenever a User utilizes the Company's Systems and/or Company-owned equipment and software, regardless of whether the User is working in the office, at home or at another location, and whether or not such use is during official office hours.

Your use of the Company's Systems constitutes your consent to such access, monitoring, disclosure, transfer, deletion and/or copying by the Company. Consequently, you should not expect privacy or confidentiality in anything you create, download, display, store, send or receive on the Company's Systems, even if it has been deleted or is marked "confidential," "private," "personal," "privileged" or other words or phrases intended to convey it is private. If you wish to avoid Company access to and review of personal communications, documents, files or data, you should not use the Company's Systems for personal purposes or save personal material on Company Systems.

Users are prohibited from taking any action that might interfere with the Company's ability to access, monitor, delete, copy and/or disclose Electronic Communications transmitted by or stored on the Company's Systems. Password protecting or encrypting emails or other forms of Electronic Communication transmitted by or stored on the Company's Systems or in the cloud other than as directed by the Company or otherwise for legitimate business purposes is prohibited.

Appropriate Use: Company Systems and Electronic Communications using those Systems, including email, telephone and Internet access, should be used for business-related purposes. Individuals who have been given Company email accounts should use those accounts (and not their personal accounts) for business functions. Personal email accounts should not be used for business-related purposes without first obtaining permission from an authorized Company executive. Occasional or incidental personal use of Company Systems is permissible so long as, in the Company's opinion: (1) it does not consume more than an insignificant amount of Company resources and User time; (2) it does not interfere with the User's responsibilities and productivity; (3) it does not preempt, interfere or conflict with any business-related activity; and (4) it does not preempt, interfere or conflict with other Company policies. Nothing in this policy or any other Company policy shall be construed to conflict or otherwise interfere with the

rights of employees or other individuals retained by the Company to use the Company's Systems during their non-working time to communicate with others about union organizing, union representation, or other matters of concern between employees regarding the terms and conditions of their employment with or retention by the Company, including their wages, hours, and/or other working conditions.

Any personal email, telephone and Internet usage, and any other use of or storage on the Company's Systems for personal purposes will be treated the same as business-related System usage under this policy, and all the provisions of this policy, including those relating to Company monitoring, apply.

Electronic Communications transmitted by or stored on the Company's Systems are subject to all the same Company policies against harassment or threats, discrimination, retaliation, defamation and sexual explicitness as traditional communications (such as mail, inter-office memoranda and oral conversations). Anything that would be inappropriate to send or state in a non-electronic communication (e.g., by memo or letter) is similarly inappropriate if sent electronically (e.g., by email or telephone). Since Electronic Communications may be copied, forwarded, saved, intercepted and archived, Users should be careful about the words they use and the documents they transmit electronically, as well as the Internet sites they access, using Company Systems.

Employees are prohibited from using the Company's Systems to access, transmit, receive, solicit, download, store, post, display, print or otherwise disseminate (by email, via the Internet, or through any other form of electronic or voice communication) any:

Unlawful material.

- Material that intimidates others, interferes with the ability of others to conduct Company business, creates a hostile work environment.

- Material that is discriminatory, harassing, retaliatory or defamatory in nature, that contains ethnic slurs, racial epithets, or that may be perceived as derogatory of others based on an individual's actual or perceived race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex (including pregnancy status, childbirth, breastfeeding, and related medical conditions), gender, gender identity, gender expression, transgender status, age, sexual orientation, military or veteran status, or any other legally protected characteristic.

- Material that is obscene or sexually explicit.

- Material related to private business activities or other non-Company business endeavors. Employees may only use the Company's Systems for charitable purposes if they obtain the prior written permission of a manager in the Human Resources Department.

- Company-wide or other internal mass emails or similar communications unrelated to Company business, unless the employee obtains the prior written permission of a manager in the Human Resources Department and a senior executive in the employee's Department. Chain letters and communications that are illegal, contrary to the 21st Century Fox Standards of Business Conduct or any other policies of the Company, or that are contrary to the Company's business interest, are similarly prohibited.

Employees encountering or receiving any such prohibited material should not redistribute it and are required immediately to report the incident to their supervisor and to either a manager in the Human Resources Department or an attorney in the Employment Law Section of the Fox Group Legal Department.

Using the Company's Systems to send personal Electronic Communications through social or multimedia networking websites (such as Facebook, Twitter, LinkedIn, Instagram, Tumblr, Snapchat, YouTube or any similar websites) is permitted but should be kept to a minimum. Absent the prior approval of your supervisor, using the Company's Systems to send Electronic Communications for a Company business purpose through external social or multimedia networking websites is prohibited. Please refer to the Social Media policy for more information on this topic.

Users are cautioned that downloading material from the Internet could constitute copyright infringement or violate other intellectual property rights. The unauthorized possession, distribution, uploading, downloading or use of content protected by the copyright, trademark, or other intellectual property laws is prohibited. This prohibition specifically includes and bans the downloading and use of any licensed or unlicensed entertainment or other software, including peer-to peer software. Users should not download with or use any of these programs on the Company's Systems. Use of these programs to download copyrighted works is illegal. Further, these programs often contain viruses and spyware and may create vulnerabilities to the Company's Systems. There is generally no legitimate business reason for the download and use of these programs, and the Company will vigorously enforce this requirement.

Retention of Email, Electronic Files and Other Electronic Communications: Unless retention is required for legal or business reasons, email messages that are no longer needed – both those that you have sent and those that you have received – and electronic files that are no longer needed, should be deleted from the Company's Systems. Employees should refer to the 21st Century Fox Records Management policy for more information on retention of Electronic Communications.

Lost or Damaged Company Property and Return of Company Systems: A User may be responsible for loss of or damage to any Company System that was within their custody or possession, regardless of whether the Company System is mobile (e.g., a, smart phone, tablet or PDA) or has been provided to the User for use outside the office (e.g., a computer for use at home), including reimbursing the Company for replacing or repairing the equipment to the extent allowable by law.

Users are prohibited from deleting or copying data from, or (re)formatting hard drives of, any Company System upon termination of employment or services. All Company Systems in a User's possession must be returned to a manager in the Human Resources Department or other executive designated by the Company upon termination of employment or services.