21st Century Fox
Principles Governing Electronic Communications
Effective as of July 2013

These Principles Governing Electronic Communications ("Principles") are intended to establish standards for policies and practices applied by 21st Century Fox and its majority-owned business units worldwide (collectively, the "Company") with respect to Electronic Communications by all Company employees and independent contractors of the Company, as well as third-party service providers, who create, store or distribute Electronic Communications using the Systems.

Each majority-owned business unit may create, adopt, and apply its own specific policy with respect to Electronic Communications and, if appropriate and desired, use of social media, that is both consistent with these Principles to the greatest extent possible and compliant with the applicable laws of the particular jurisdictions in which the business unit operates. Each business unit's policy may also take into account the accepted practices of the business unit's industry. To the extent that these Principles conflict with applicable law, applicable law prevails.

Definitions

"Electronic Communications" are created or communicated through the Company's Systems or through Personal Devices accessing the Company's Systems, and include but are not limited to the following: e-mails, instant messages, text messages, blog posts; comments posted on discussion forums, social media or websites; and faxes, documents, files, programs, audio and video content and other data that are stored or transmitted electronically.

"Personal Devices" include equipment or tools used for creating or distributing Electronic Communications but which are not Company-provided, including, but not limited to, individually-owned computers, USB drives, software, tablets and other mobile devices (including smart phones and personal digital assistants).

"Company Systems" include, but are not limited to, Company-provided desktop computers and workstations, laptop computers, USB drives, file servers, networks, other information technology hardware and software, tablets and other mobile devices (including smart phones and personal digital assistants), Internet and intranet access and usage, email systems, telephone systems and voice mail.

Principles

1. The Company expects all employees, independent contractors and third party agents to abide by the highest standards of personal conduct with respect to Electronic Communications, including, but not limited to, strict compliance with all applicable laws.

2. The Company Systems are made available for legitimate Company-related business purposes. If a business unit's policy allows for personal use of Company Systems by individuals who are granted access, such personal use (including, but not limited to, for Electronic Communications) must not be so extensive or so frequent as to interfere with business- related responsibilities and productivity.

3. Electronic Communications should at all times be professional, responsible and lawful in substance and manner.

4. Electronic Communications may not be used for dissemination or distribution of inappropriate materials including, but not limited to, material that is unlawful, discriminatory, harassing, retaliatory, defamatory, obscene, or sexually explicit.

5. Electronic Communications should not be used to access, transmit, receive, download, store, post, display, print, or otherwise disseminate any material that violates any Company policy.

6. Subject to the provisions of applicable law, there should be no expectation of privacy or confidentiality in Electronic Communications that are created, downloaded, displayed, stored, sent or received on the Company Systems, or in Electronic Communications that are created or distributed on or through any Personal Device accessing the Company Systems.

7. Unless otherwise prohibited by applicable law, each business unit may in its sole discretion monitor all usage of Company Systems, including, but not limited to, Electronic Communications.

8. Electronic Communications should not be used to infringe on the intellectual property rights of the Company or of any others.

9. All Company employees, independent contractors and third party agents who access Company Systems share responsibility for the security of those systems. No one who accesses Company Systems may engage in practices that make the Company Systems vulnerable, and must actively protect the Company Systems' integrity and security in accordance with business unit policies and procedures.

If you have any questions about these Principles, please contact your Legal Department, business unit Chief Compliance Officer, or Group Chief Compliance Officer.