End User Information Protection Policy
Effective date: January 2016

INTRODUCTION

Information related to Twenty-First Century Fox's business and operations, content, employees, talent and consumers is among the company's most valuable assets. Additionally, some types of information are highly sensitive and/or regulated by law and must be protected accordingly. Twenty-First Century Fox respects the privacy of our employees, talent, consumers and third parties with whom we do business, and is committed to handling personal and other confidential information responsibly and in compliance with applicable laws. Please review this Policy with care as it details your obligations with respect to safeguarding this information.

TO WHOM DOES THIS POLICY APPLY?

This Policy applies to Twenty-First Century Fox, Inc. and its majority-owned affiliated companies (collectively "Fox" or the "Company"). Please note that in certain territories additional or different requirements may apply. In such cases, those local requirements will control. The Policy applies to all full-time and part-time or temporary employees, trainees, interns, and other workers (collectively "employees" for the purposes of this Policy) and any third parties (such as contractors, service providers, and/or consultants) who provide services to the Company.

WHAT INFORMATION IS COVERED BY THIS POLICY?

Confidential Information is non-public information related to the Company's business operations or about individuals (including the Company's employees, talent and consumers) that could adversely affect the Company's business or individuals if lost, accessed by or disclosed to unauthorized persons.

The term Confidential Information includes **Highly Sensitive Confidential Information**, which is information that is protected by law or could cause serious harm to the Company or to individuals if lost, accessed by or disclosed to unauthorized persons, such as information related to the Company's highly confidential business operations or highly sensitive personal information about individuals.

Examples of Confidential Information and Highly Sensitive Confidential Information are listed below. Some information may be publicly available (such as an individual's name or email address), but if it is grouped together with other Confidential Information as part of a confidential file or record then the entire file or record requires appropriate protection.

This Policy applies to all types of Confidential Information regardless of the manner in which it is collected, transmitted and/or stored (physical or electronic media), or the source from which it is collected or developed.

The following chart lists the main types of Confidential Information and Highly Sensitive Confidential Information covered by this Policy. Each of the Company's business units must designate personnel who will be responsible for identifying and classifying the businesses' Confidential Information (including Highly Sensitive Confidential Information) pursuant to this Policy.

If you are unsure of how to categorize a particular type of information, please speak to your manager, a lawyer in your Legal Department or the Privacy Department

.

Highly Sensitive Confidential Information

Includes:

Company Business Operations

- Film or video content prior to release or broadcast window or during live broadcast or streaming
- Non-public intellectual property/trade secrets (such as pending patent applications, inventors' journals, and patent disclosures)
- Highly sensitive strategic plans such as expansion/acquisition and divestiture plans
- Company Board Meeting Minutes
- Non-public pricing and other financial information
- Journalistic sources
- System passwords, encryption keys and other passwords

Personal Information

- Government-issued identification numbers (such as Social Security Numbers, Passport Numbers, Driver's License Numbers, National or State ID Numbers)
- Credit card numbers
- Financial account information
- Compensation information (such as salary, bonus, pension)
- Personal Health Information ("PHI") (information relating to a person's physical or mental health condition including the provision of heath care services, as well as any health insurance information (e.g. a subscriber identification number))
- User name or email address, in combination with any password, pin, or security question and answer
- Unique biometric data, such as a fingerprint, voice print, or retina image
- Date of birth

Confidential Information

Includes:

Company Business Operations

- Draft marketing materials
- Contracts with third parties
- Business or project plans
- Company Policies not posted on a public-facing Company website
- Information received from third parties that is required to be kept confidential (for example, under a non-disclosure agreement)
- Tax ID Numbers (that are not Social Security Numbers)

Personal Information

- Personal information not classified as Highly Sensitive Confidential Information such as the combination of an employee, talent, or consumer name and personal email address, address, or phone number

WHAT ARE YOUR OBLIGATIONS RELATED TO CONFIDENTIAL INFORMATION?

You are responsible for protecting all types of Confidential Information. Unauthorized access to, loss, or misuse of Confidential Information could cause the Company and affected individuals legal, financial or reputational damage. **Failure to comply with this Policy may lead to disciplinary action against the responsible employee, which may include termination of employment and/or legal action**.

There are additional legal requirements that apply to the protection of Highly Sensitive Confidential Information, including highly sensitive personal information, which are noted below. Employees who work in departments with regular access to Highly Sensitive Confidential Information or who are responsible for developing websites (or contracting for coding services), applications and systems that collect or store Highly Sensitive Confidential Information have specialized procedures and other requirements that apply to their positions, some of which are specified below.

Your responsibilities include:

Access & Control:

- You may access Confidential Information only as necessary and authorized to perform your job duties.
- You must not discuss Confidential Information in public places.
- You must use strong and unique passwords, must not re-use passwords on multiple systems, must not re-use Company system passwords for personal accounts, and must not share their passwords with others. When you select a password, you must comply with the Company Password Directive - https://21cf.box.com/password-policy
- You should not write your passwords down on paper or save them in an electronic file.
- You should watch for attempts by hackers and identity thieves to obtain Confidential Information through sophisticated phishing schemes, infected websites, and malware. You should not install software on Company equipment without the approval of your IT department. You should not open emails or click on links and attachments from unknown senders, and should exercise caution when visiting unfamiliar websites. Contact your IT Department with any concerns.

Storage:

- If you have a legitimate and authorized need to move Confidential Information from your workstation, you must keep the information within your control at all times. All laptops must be encrypted. Laptops, tablets, mobile phones, and other devices that contain or can access Confidential Information must be under your control at all times (e.g. do not leave them unattended in a car and, when traveling, secure them in a hotel safe, if available), and always powered off when not in use.
- You must use approved, enterprise standard file sharing tools. Employees who have a legitimate and authorized business need to use a different, non-Company, third party application to share Confidential Information (for example, those employees who collaborate on projects with external partners) may only use those third-party applications approved by their IT Department.
- All physical records, papers or files containing Confidential Information should be kept in a locked environment (e.g. cabinet, desk, filing room or office) to which only the minimum necessary number of persons have authorized access.

In addition to the obligations noted above, the following obligations also apply to storage of Highly Sensitive Confidential Information:

- Highly Sensitive Confidential Information kept in digital format must not be stored on any personal storage medium such as external hard drives, thumb drives, or third-party personal storage, including personal cloud services.
- You should not use your email Inbox or other active email folders (e.g. folders you create in Outlook to store emails) to store Highly Sensitive Confidential Information. Such Information should be stored in a secure document management system or a database that is capable of being encrypted, such as an encrypted file share folder. Contact your IT Department for guidance.

- Storing Highly Sensitive Confidential Information in a cloud service requires careful consideration and approval by the IT and Legal Departments. Ask your IT Department for approved services. At a minimum, encryption must be applied to Highly Sensitive Confidential Information stored in a cloud service and the encryption keys should be stored separately outside of the cloud service.

Transmittal:

- You must have a legitimate and authorized business need to transmit Confidential Information, both inside and outside of the Company.
- You must not transmit any Confidential Information to or from a personal email account.

In addition to the obligations noted above, the following obligations also apply to transmittal of Highly Sensitive Confidential Information:

- Unencrypted Highly Sensitive Confidential Information may be transmitted only within Company systems that have been approved by your IT Department.
- Highly Sensitive Confidential Information that contains highly sensitive personal information (such as government-issued identification numbers, credit card numbers, financial account information, compensation information or PHI):
    - may only be transferred outside Company systems using a method of encryption approved by a Company IT Department such as: TLS; secure hyper-text transfer protocol (https); secure file transfer; commercial encryption such as PGP; or a custom interface provided by the Company (contact your IT Department with questions); and
    - may not be included in the subject line or body of an email.
- All digital transfers of Highly Sensitive Confidential Information that consists of audio-visual materials (e.g., film or video content prior to release or broadcast windows) must be done through secure and approved IT systems. Contact your IT Department with questions.

Mobile/Remote Worker Policy:

- All mobile devices (tablets, smartphones) that are managed by your IT Department or access the Company's Confidential Information must have current operating systems (e.g. IOS or Android) installed and be password or PIN protected.
- With the exception of those managed by IT, mobile and other remote devices are not permitted to connect directly to Company internal networks. All remote and IT-managed devices (including PCs/Apple Macs, laptops and notebooks) that are allowed to connect to Company internal networks must use 2-factor authentication.
- IT security has the right to remotely wipe any mobile device that is connected to the Company internal network or that accesses or stores Company Information.
- Highly Sensitive Confidential Information must never be stored locally on a mobile device that is not managed by your IT Department, encrypted and capable of being remotely wiped. Your business unit's approved file sharing tool's mobile app should be used to ensure that all such Information is appropriately stored and encrypted in the cloud.
- You must immediately report any lost or stolen laptop or mobile device to the contact designated by your local IT Department. If you suspect unauthorized access to Company Information, it should be immediately reported as well.
- You must not allow the removal of limitations on your device imposed by the manufacturer (e.g., allow the device to be "jailbroken"), or allow the installation of any software/firmware that is designed to gain access to functionality that should not be exposed to the user.
- You must not load pirated software or illegal content on your mobile device.
- Applications must only be installed from an official and trusted platform. If you are unsure if an application is from an approved source, please contact your IT Department.

Third Parties:

- Any third party with which Confidential Information is to be shared must be vetted in advance by your Legal Department and Fox Group Cyber Security and contractually required to provide administrative, physical and technical safeguards sufficient to protect the Confidential Information in a manner consistent with this Policy. Contact your Legal Department regarding appropriate contractual provisions.

Retention and Disposal:

- All employees must follow the Records Management Policy and Record Retention Schedule and must securely destroy Confidential Information that has exceeded retention dates and that is not required to be maintained for business or legal reasons (such as a Hold Order).
- Secure destruction of paper or other hard copies of Confidential Information includes shredding or pulverizing so the information cannot be read or reconstructed.
- Secure destruction of electronic and magnetic media includes erasing, purging or modifying to make the information un-readable or un-decipherable through any means (for example, the device must be physically destroyed or overwritten many times).

QUESTIONS OR CONCERNS

- To obtain an exception to any of the requirements in this Policy, you must contact and receive approval from your Legal Department.
- If you believe someone has accessed, used or shared Confidential Information without authorization, your laptop or other device is lost or stolen, or there has been a breach of a Company system, you must immediately notify the contact that has been designated by your local IT Department. If you receive suspicious emails or SPAM messages, please immediately contact your local IT Department.
- If you believe there has been a violation of this Policy, or if you have questions please contact a manager in the Human Resources or IT Departments.