COMCAST CORPORATION

Code of Conduct

Facing ethical and compliance issues with integrity.

Last Updated: January 2016
# Table of Contents

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>2</td>
</tr>
<tr>
<td>Statement of Integrity</td>
<td>3</td>
</tr>
<tr>
<td>Resources for Employees</td>
<td>4</td>
</tr>
<tr>
<td>What to Know About Our Code</td>
<td>5</td>
</tr>
<tr>
<td>Purpose</td>
<td>6</td>
</tr>
<tr>
<td>Governing Principles</td>
<td>6</td>
</tr>
<tr>
<td>Ethical Decision-Making</td>
<td>6</td>
</tr>
<tr>
<td>Applicability</td>
<td>7</td>
</tr>
<tr>
<td>Interpretation, Approvals and Waivers</td>
<td>7</td>
</tr>
<tr>
<td>Which Law Applies</td>
<td>7</td>
</tr>
<tr>
<td>Penalties for Violation</td>
<td>8</td>
</tr>
<tr>
<td>Business Unit Policies and Procedures</td>
<td>8</td>
</tr>
<tr>
<td>Integrity Websites</td>
<td>8</td>
</tr>
<tr>
<td>What Employees Must Do</td>
<td>8</td>
</tr>
<tr>
<td>What Supervisors Must Do</td>
<td>9</td>
</tr>
<tr>
<td>What Happens When Concerns Are Raised</td>
<td>10</td>
</tr>
<tr>
<td>Code Policies</td>
<td>11</td>
</tr>
<tr>
<td>Our Commitment to Each Other</td>
<td>12</td>
</tr>
<tr>
<td>Fair Employment Practices</td>
<td>12</td>
</tr>
<tr>
<td>Environmental, Health and Safety</td>
<td>14</td>
</tr>
<tr>
<td>Privacy</td>
<td>15</td>
</tr>
<tr>
<td>Our Commitment to Our Company</td>
<td>18</td>
</tr>
<tr>
<td>Intellectual Property</td>
<td>18</td>
</tr>
<tr>
<td>Security and Crisis Management</td>
<td>20</td>
</tr>
<tr>
<td>Conflicts of Interest</td>
<td>22</td>
</tr>
<tr>
<td>Gifts and Business Entertainment</td>
<td>24</td>
</tr>
<tr>
<td>Our Commitment to Our Shareholders</td>
<td>27</td>
</tr>
<tr>
<td>Financial Responsibility</td>
<td>27</td>
</tr>
<tr>
<td>Insider Trading and Stock Tipping</td>
<td>29</td>
</tr>
<tr>
<td>Our Commitment to Our Business Partners</td>
<td>31</td>
</tr>
<tr>
<td>Supplier Relationships</td>
<td>31</td>
</tr>
<tr>
<td>Interacting with Governments and Political Activities</td>
<td>33</td>
</tr>
<tr>
<td>Our Commitment to the Law</td>
<td>37</td>
</tr>
<tr>
<td>Complying with Competition Laws</td>
<td>37</td>
</tr>
<tr>
<td>Anti-Corruption Laws</td>
<td>39</td>
</tr>
<tr>
<td>Money Laundering Prevention</td>
<td>41</td>
</tr>
<tr>
<td>International Trade Controls</td>
<td>42</td>
</tr>
<tr>
<td>Our Commitment to Our Company</td>
<td>18</td>
</tr>
<tr>
<td>Intellectual Property</td>
<td>18</td>
</tr>
<tr>
<td>Security and Crisis Management</td>
<td>20</td>
</tr>
<tr>
<td>Conflicts of Interest</td>
<td>22</td>
</tr>
<tr>
<td>Gifts and Business Entertainment</td>
<td>24</td>
</tr>
<tr>
<td>Our Commitment to Our Shareholders</td>
<td>27</td>
</tr>
<tr>
<td>Financial Responsibility</td>
<td>27</td>
</tr>
<tr>
<td>Insider Trading and Stock Tipping</td>
<td>29</td>
</tr>
<tr>
<td>Our Commitment to Our Business Partners</td>
<td>31</td>
</tr>
<tr>
<td>Supplier Relationships</td>
<td>31</td>
</tr>
<tr>
<td>Interacting with Governments and Political Activities</td>
<td>33</td>
</tr>
<tr>
<td>Our Commitment to the Law</td>
<td>37</td>
</tr>
<tr>
<td>Complying with Competition Laws</td>
<td>37</td>
</tr>
<tr>
<td>Anti-Corruption Laws</td>
<td>39</td>
</tr>
<tr>
<td>Money Laundering Prevention</td>
<td>41</td>
</tr>
<tr>
<td>International Trade Controls</td>
<td>42</td>
</tr>
</tbody>
</table>
Pioneering new ideas while also acting with the highest standards of integrity are key principles that have gotten us to where we are today. In fact, we believe that integrity, honesty and respect are the foundation of a productive working environment and a strong company.

Comcast is well situated at the intersection of media and technology and will help shape the future for consumers around the things they love most — technology, entertainment and communications. However, it is our actions — how we perform day in and day out — that will ensure our success. It’s as simple as doing the right thing and treating people the right way.

As we innovate together, our brands continue to stand for integrity, trust and respect. Our Code of Conduct is the common framework for operating with integrity, the principles that we must apply every day in all we do. I am personally asking you to commit to following the Code of Conduct as a guide for your interactions with our customers, our viewers, our fellow employees, our business partners, and anyone else with whom you come in contact.

Each of us is responsible for knowing when to speak up, asking tough questions and reporting any possible violation of the Code of Conduct. Since no code or policy can spell out the appropriate behavior for every situation, you should talk with your supervisor — or refer to any of the resources listed throughout the Code — when you have questions or concerns. Remember, our policy strictly prohibits retaliation of any kind for reporting in good faith a suspected violation of the Code.

We each hold our company’s reputation in our hands. We want the world to recognize us as a company that not only delivers for our shareholders, customers and viewers, but one that does so with an unwavering commitment to integrity. With your help, we will do just that.

Brian L. Roberts
Chairman and Chief Executive Officer

January 2016
Resources for Employees

We want you to speak up, ask questions and get answers. We offer several channels for raising concerns. Use the option that is most comfortable for you.

Resources Within Your Business Unit:

If you have something on your mind – whether it’s about a day-to-day workplace issue, a concern about suspected illegal or unethical conduct or any other matter – you may contact any of these resources.

- **Supervisor** – Generally, your supervisor will be in the best position to resolve your concerns quickly. You may also contact your supervisor’s manager or other local leader.

- **Human Resources** – You may also contact your business unit’s Human Resources representative (including a Comcast Listens representative).

- **Law Department** – The law department within your business unit can also assist you, especially with questions concerning applicable laws and policies.

- **Additional NBCUniversal Resource** – If you are an employee of NBCUniversal, you may also contact the NBCUniversal Integrity Helpline by calling 1-800-622-6221 from the U.S. or Canada, or +44 (0) 20 36186210 from all other locations. You may also send an email to integrity@nbcuni.com or contact an NBCUniversal Ombudsperson from the list on the NBCUniversal Integrity Website at my.inbcu.com/integrity.

Additional Resources:

The Comcast Listens helpline and web portal are additional resources for asking questions or raising concerns:

- Call Comcast Listens at 1-877-40-LISTENS (1-877-405-4783)
- Visit Comcast Listens online at www.ComcastListens.com

These channels are available around the clock. Where allowed by law, you may choose to remain anonymous when using these channels. However, we encourage you to identify yourself so we can follow-up and provide feedback to you.

Comcast Audit Committee Resource:

The Audit Committee of the Comcast Board of Directors has created a process by which employees may raise complaints about accounting, internal controls or auditing matters to the Chair of the Audit Committee. If you wish to raise a question or concern of this type, you may send an email to Audit_Committee_Chair@comcast.com.

For more information on many of the resources described on this page, including contact information, please visit the Integrity section of your business unit’s intranet.
What to Know About Our Code

Click headings below to navigate through the document.

Purpose .................................................. 6
Governing Principles ................................. 6
Ethical Decision-Making .............................. 6
Applicability ............................................ 7
Interpretation, Approvals and Waivers .......... 7
Which Law Applies ...................................... 7
Penalties for Violation ............................... 8
Business Unit Policies and Procedures .......... 8
Integrity Websites ...................................... 8
What Employees Must Do ............................ 8
What Supervisors Must Do ........................... 9
What Happens When Concerns Are Raised ...... 10

< 5 >
What to Know About Our Code

Purpose
We believe that a business has ethical as well as economic responsibilities and will prosper most in an environment that is ethically sound. We are committed to acting with the highest ethical standards and to protecting our reputation for integrity. Our Code of Conduct provides standards of business conduct for all of our employees, officers and directors to live up to in order to achieve our ethical standards and commitment to integrity.

Governing Principles
The foundation of the Code consists of the following important standards of business conduct, which are the key ingredients in establishing and maintaining trust:

- Comply with all applicable laws, regulations, policies and contracts governing our businesses.
- Be honest, fair and trustworthy in all your business activities and relationships.
- Treat one another fairly and foster a safe, diverse and environmentally responsible workplace.
- Protect our assets and information and the assets and information entrusted to us by others.
- Avoid conflicts of interest, and the appearance of such conflicts, between work and personal affairs.
- Compete responsibly in the marketplace.
- Ask questions, seek guidance and raise concerns.
- Through leadership at all levels, create and sustain a culture where ethical conduct is recognized, valued and practiced by all employees.

Ethical Decision-Making

WHAT TO DO:
In today's rapidly changing workplace, you may encounter unfamiliar situations that present ethical dilemmas. In these circumstances, the right thing to do is not always clear. For this reason, you should become familiar with the contents of the Code. The Code contains a broad overview of key policy areas and examples within each area. It is not all-inclusive. Situations will arise that are not covered here. For those situations, ask yourself these questions:

- Does it potentially violate any applicable law, regulation, policy or contract?
- Does it feel right?
- Should I check with my supervisor or another local leader?
- How would it look if it was covered in the news?
- Would I feel comfortable explaining it to my family?
- Could it appear improper?

WHAT TO WATCH OUT FOR:
Sometimes, it is difficult even to recognize an ethical problem. When in doubt, ask your supervisor, a Human Resources representative or a Company lawyer. Don't disregard a potential issue because you think:

- It's none of my business.
- The Company wants me to do this.
- Everyone does it.
- No one will ever know.

If you find yourself thinking these thoughts, ask yourself the questions listed above to help guide your actions, or contact any of the resources listed under Resources for Employees.
Applicability
The Code applies to all employees, officers and directors of Comcast and its subsidiaries, all of whom are required to periodically acknowledge that they have received and are in compliance with the Code, and that neither the Code nor any of its provisions constitutes an express or implied contract of employment or guarantee of employment for any specific period of time. Use of the term “Company” refers to all of these entities and their respective business units. Nothing in the Code limits employees from exercising any right provided by law.

Interpretation, Approvals and Waivers
For help interpreting and applying the Code or any applicable law, regulation, policy or contract to a given situation, you may contact any of the resources within your business unit listed under Resources for Employees of the Code, including your supervisor. Supervisors, however, are generally not permitted to grant approvals or waivers under the Code (unless otherwise specified in a particular Code policy). We believe that consistent application of the Code is essential. To promote this objective, approvals and waivers under the Code may only be granted by the appropriate authorized employees, as specified in the Code. In some sections of the Code, approvals must be obtained by “Authorized Approvers.” Authorized Approvers are:

- Senior HR Professionals defined as
  - the lead Human Resources professional in your business unit or
  - senior vice president or higher-level Human Resources professionals in your business unit

- Senior Attorneys defined as
  - vice president or higher-level attorneys in the law department of your business unit
  - the General Counsel of Comcast Corporation or
  - the Senior Executive Vice President with supervisory responsibility for the General Counsel of Comcast Corporation

Click here for a current list of Authorized Approvers and their contact information. This information can also be found in the Integrity section of your business unit’s intranet.

If a supervisor is asked by an employee to grant an approval or waiver under the Code, the supervisor must escalate the matter to an Authorized Approver. Any waiver of the Code for any Comcast Corporation executive officer or director may only be granted by the Comcast Board of Directors and will be disclosed to the public as required by law.

Which Law Applies
The Company conducts business in many countries around the world. Our employees are citizens of many different countries. As a result, our operations are subject to the laws of many countries, provinces, states and municipalities, and multi-jurisdictional organizations such as the European Union. An important challenge for all of us is to understand how these laws may apply to our operations.

Comcast Corporation is a corporation organized in the United States. The laws of the United States generally extend to all operations of the Company and its subsidiaries throughout the world, as well as to the business activities of employees wherever they live and work. Other countries may also apply their own laws outside of their borders to their own citizens and to corporations that are organized under their laws, such as company subsidiaries.

The references in Company policies to the laws of the United States and the other countries where we do business reflect the reality that a global company is regulated by many different laws at the same time. In some instances, there may be a conflict between the applicable laws of two or more countries. When you encounter such a conflict, it is especially important to consult the law department of your business unit to understand how to resolve that conflict properly.

For employees working, or actions being taken, outside of the United States, references to U.S. currency in the Code mean the applicable foreign currency equivalent, and references to GAAP mean the applicable foreign equivalent to U.S. generally accepted accounting principles.
Penalties for Violation

Employees, officers and directors who violate the Code or applicable laws, regulations, policies or contracts are subject to disciplinary action up to and including termination of employment or service. Misconduct that may result in discipline includes:

- Directly or indirectly violating the Code or Company policy.
- Directing or assisting others to violate the Code or Company policy.
- Failure to promptly raise a known or suspected violation of the Code or Company policy.
- Failure to cooperate in Company investigations of alleged Code or policy violations.
- Retaliation against another employee for reporting a potential concern about illegal or unethical conduct or assisting in an investigation.
- Failure to supervise, to the extent the circumstances of a violation reflect a supervisor’s disregard for the Code.

What Employees Must Do

COMPLY WITH THE CODE

- Personally commit to following the Code.
- Periodically certify that you have read, understood and complied with the Code.
- Disclose circumstances that require approval under the Code to your supervisor or an Authorized Approver.

RAISE YOUR CONCERNS

- Promptly raise any concerns about actual or suspected illegal or unethical conduct. The longer you wait to address a concern, the worse it may become.
- Understand the different channels for raising concerns listed under Resources for Employees.
- If a concern you raise is not resolved, pursue the issue. Raise it through one of the other channels.
- Cooperate in Company investigations related to concerns about illegal or unethical conduct.
- Notify the law department of your business unit immediately if you have notice of, or believe it is reasonably foreseeable that the Company will be the subject of, an external investigation, litigation matter or other legal or governmental proceeding.

SATISFY YOUR COMPLIANCE OBLIGATIONS

- Understand the laws, regulations, policies and contracts relevant to your job.
- Promptly complete required trainings assigned to you.
- Periodically visit the Integrity section of your business unit’s intranet for Code of Conduct learning aids, copies of Company policies, and information on how to raise concerns.

Business Unit Policies and Procedures

Your business unit may issue its own policies and procedures relating to appropriate business conduct consistent with the Code. You must follow those policies and procedures in addition to those described in the Code.

Integrity Websites

For more information on many of the topics in the Code, as well as policies that may be applicable to your role in the Company, please visit the Integrity section of your business unit’s intranet.
What Supervisors Must Do

In addition to their responsibilities as employees, supervisors must also:

SET THE RIGHT EXAMPLE

• Assure that your own ethical behavior is a model for all employees—every day.
• Demonstrate that business needs and results are never more important than our ethical standards and commitment to integrity.
• Give your employees the support they need to satisfy their compliance obligations, including by providing the necessary time to complete trainings.

CREATE AN OPEN REPORTING ENVIRONMENT

• Foster an environment where employees feel safe and comfortable asking questions and reporting concerns.
• Make yourself available to listen to employee concerns. Ensure you have enough time to adequately discuss their concerns. If not, schedule an alternate time and communicate to the employee that your desire to do so is to ensure that they have your full attention.
• Be an active listener and ask for clarification and additional information in such a way that employees don’t feel intimidated or defensive.
• Thank employees for bringing issues to your attention.
• If an employee doesn’t come to you first, support his/her choice and consider why he/she didn’t approach you.
• Ensure that there is absolutely no tolerance for retaliation.
  – Bear in mind that many employees may be sensitive to perceived slights or perceived retaliation following submission of a report of misconduct. It is imperative that you continue to treat employees with dignity and respect, including the following:
    » Evaluate them based on actual performance.
    » Provide meaningful assignments.
    » Share information needed to get work done.

KNOW HOW TO RESPOND TO CONCERNS

• For workplace issues, such as day-to-day problems with a co-worker or questions about Company benefits, take immediate action to resolve the issue or contact your supervisor or a Human Resources representative for assistance so that you may provide a timely response to the employee.
• For allegations of suspected illegal or unethical conduct, immediately report them to any Human Resources representative, the Comcast Listens helpline or web portal (by calling 1-877-40-LISTENS or visiting www.comcastlistens.com) or the Chair of the Audit Committee (by sending an email to Audit_Committee_Chair@comcast.com). Alternatively, if you are an NBCUniversal employee, you may contact the NBCUniversal Integrity Helpline by calling 1-800-622-6221 or emailing integrity@nbcuni.com.
• If an employee asks you to grant a Code approval or waiver, escalate the matter to an Authorized Approver.
• If an employee asks you to interpret or apply the Code or any applicable law, regulation, policy or contract to a given situation, and you’re unsure how to respond, escalate the matter to an Authorized Approver.
• Do not investigate known or suspected Code violations yourself.
• Do not hire an outside investigator.
What Happens When Concerns Are Raised

CONCERNS ABOUT ILLEGAL OR UNETHICAL CONDUCT WILL BE INVESTIGATED

• An objective team with the necessary knowledge and experience will be assigned to conduct the investigation.
• The team will determine the facts through interviews, review of documents and/or other appropriate means.
• If wrongdoing is confirmed, appropriate discipline and corrective action will be taken regardless of the position of individuals involved.
• The employee raising the concern will receive feedback on the outcome to the extent the Company can appropriately provide it.

CONFIDENTIALITY IS RESPECTED

The identity of the employee (if provided) and the information provided will be shared only on a “need-to-know” basis with those responsible for addressing and resolving the concern.

RETRIALTION VIOLATES COMPANY POLICY

Our policy strictly prohibits retaliation against any employee, officer or director reporting in good faith an actual or suspected violation of the Code or applicable laws, regulations, policies or contracts (even if the concern is eventually unsubstantiated). No employee, officer or director should be discharged, demoted, suspended, threatened, harassed, intimidated, coerced or retaliated against in any other manner as a result of his or her making, or assisting in the handling or investigation of, a good faith complaint. Note, however, that an allegation of retaliation does not exempt an employee from normal standards of performance and conduct.

If you feel that you have been retaliated against, speak up. Retaliation for raising a good faith integrity concern is prohibited by the Code and could lead to disciplinary action up to and including termination of employment. For more information on this subject, you should refer to your business unit’s employee handbook section titled “Anti-Retaliation Policy.”
Click headings below to navigate through the document.

Our Commitment to Each Other .............................................. 12
Our Commitment to Our Company ...................................... 18
Our Commitment to Our Shareholders ................................. 27
Our Commitment to Our Business Partners .......................... 31
Our Commitment to the Law ............................................. 37
Our Commitment to Each Other

Our Company is only as strong as our workforce. That means that we can only succeed by investing in our people and ensuring we have a fair, inclusive and diverse workplace. We commit to maintaining a work environment of mutual trust and respect where all employees are recruited, developed and advanced on the basis of their qualifications, talents and achievements. We commit to lessening our impact on the environment and providing a safe and healthy workplace where no one is subject to unnecessary risk. We commit to handle personal data of our employees and customers responsibly and act in compliance with applicable privacy laws worldwide.

- Fair Employment Practices
- Environmental, Health and Safety
- Privacy

Fair Employment Practices

INTRODUCTION

Fair employment practices do more than keep us in compliance with applicable labor and employment laws. They help contribute to a culture of respect. We are committed to complying with all applicable labor and employment laws wherever we operate, including laws pertaining to freedom of association, privacy, immigration, wages and hours, as well as laws prohibiting employment discrimination and forced, compulsory and child labor. Beyond legal compliance, we strive to create an environment considerate of all employees wherever we conduct business.

WHAT TO KNOW

- We are committed to creating and maintaining a work environment in which everyone is treated with respect and dignity.
- Each individual has the right to work in a professional atmosphere that provides equal employment opportunity.
- We prohibit discrimination and harassment based on race, color, religion, creed, gender, gender identity or expression, age, national origin or ancestry, citizenship, disability, sexual orientation, marital status, pregnancy, veteran status, membership in the uniformed services, genetic information and any other characteristic protected by national, state or local law (“protected characteristics”).
• We prohibit discrimination against and the harassment of individuals employed by our suppliers, contractors and other third parties that do business with us.

• We prohibit retaliation against anyone for having reported in good faith a potential Code violation or concern or participated in an investigation relating to a potential violation or concern. This means that employees are prohibited from taking adverse employment actions (e.g., terminating someone’s employment) or other steps intended to “punish” an individual because he or she raised a good faith concern or complaint.

WHAT TO DO

• Base employment decisions on job qualifications (e.g., education and prior experience) and merit. Merit can include, but is not limited to, an individual’s skills, performance, values, leadership and other job-related criteria.

• Make all employment decisions, including those related to hiring, compensation, discipline, promotion and termination, without regard to an individual’s protected characteristic(s).

• Provide a work environment free of unlawful discrimination and harassment.

• Take lawful and good faith actions, consistent with applicable laws intended to ensure equal employment opportunities for women, minorities, people with disabilities and veterans.

• Promptly raise any concern about an actual or suspected violation of this policy to your supervisor or Human Resources representative. As with all concerns, escalate the matter if you do not receive an appropriate response.

• If a conflict arises between the requirements of this policy and the laws, customs or practices of a particular area, consult with a Company lawyer to determine the most appropriate course of action.

WHAT TO WATCH OUT FOR

• Allowing harassment that could create a hostile work environment by, for example:
  – telling jokes or displaying materials that ridicule or offend members of a particular gender, race or ethnic group;
  – displaying sexually suggestive materials in the workplace or on Company computers or mobile devices; or
  – pursuing a romantic relationship with a co-worker who has indicated that he or she is not interested.

• Considering a protected characteristic in hiring, promotion, compensation, discipline, termination or other employment decisions.

• Violating a labor law (e.g., hiring a child under the legal minimum age without required permits).

• Taking a retaliatory action against an employee because the employee raised a good faith concern about a violation of law, regulation, policy or contract.

ADDITIONAL RESOURCES IN THE INTEGRITY SECTION OF YOUR BUSINESS UNIT’S INTRANET

• Frequently Asked Questions
• Anti-Retaliation policy in your business unit’s Employee Handbook
• Equal Employment Opportunity policy in your business unit’s Employee Handbook
• Harassment policy in your business unit’s Employee Handbook
Environmental, Health and Safety

INTRODUCTION
We are committed to protecting the environment, as well as the health and safety of employees. Through management leadership and employee commitment, we strive to provide a safe and healthy work environment and to avoid adverse impact and injury to the environment and the communities in which we conduct business.

WHAT TO KNOW
- Unsafe activities and conditions may include, among other things:
  - Failure to use personal protective equipment (appropriate footwear, safety glasses, hearing protection, gloves, monitors, etc.)
  - Unlabeled or unapproved chemicals
  - Exposed or unsafe wiring
  - Blocked fire or emergency exits
  - Unsafe or distracted driving, failure to wear seat belts or failure to follow Company driving policies
  - Working in high places without fall protection
  - Working beneath heavy, suspended loads or improperly using cranes
  - Disabling safety controls or guarding on equipment and machinery
  - Working on electrical or powered equipment without following safety procedures
  - Potential exposure to serious infectious diseases

WHAT TO DO
- Comply with applicable national, state and local environmental, health and safety (“EHS”) laws, regulations and Company EHS policies.
- Create and maintain a safe working environment and prevent workplace injuries.
- Assess EHS impact and issues before starting a new activity or project.
- Eliminate unreasonable EHS risks from Company facilities and activities.
- Ensure that waste handling, disposal and recycling processes for electronic equipment, light bulbs, batteries, and other materials that, after use, may be subject to waste regulations comply with all hazardous waste laws.
- As much as practicable, reduce toxic and hazardous materials; prevent pollution; and conserve, recover and recycle waste materials, water and energy.
- Continue to improve our EHS systems and performance as an integral part of Company operational strategy.
- Promptly alert your supervisor or EHS lead to unlawful or unsafe conditions, workplace injuries and third party injury or damage, including "near misses."
- Conduct appropriate due diligence in advance of completing any proposed purchase, sale or lease of real estate.
WHAT TO WATCH OUT FOR

- Unsafe activities and conditions.
- Failure to comply with health, safety or environmental regulations or procedures.
- EHS complaints from employees, customers, guests, suppliers, contractors or neighbors.
- Unreported environmental, health or safety hazards or accidents.
- Failure to respond promptly to concerns about possible product safety issues.
- Risks and liabilities associated with new acquisitions, activities and projects.
- Failure to follow Company policies for the management, shipping, transportation, import/export or disposal of hazardous materials and chemicals.

ADDITIONAL RESOURCES IN THE INTEGRITY SECTION OF YOUR BUSINESS UNIT’S INTRANET

- Frequently Asked Questions
- Safety policy in your business unit’s Employee Handbook

Privacy

INTRODUCTION

Protecting and respecting the privacy rights of our employees and parties with whom we do business, such as customers, suppliers and contractors, is critical to our success. Each employee must be aware of and follow all applicable policies regarding the responsible use of customer, employee and others’ personal information.

WHAT TO KNOW

- In the United States, a number of laws regulate customer and employee “personal data” (e.g., name, home and office contact information, medical and other data), and a growing number of countries are more stringently regulating the collection and use of personal data.
- In addition, many countries regulate personal data of employees and other personnel in business-to-business transactions. A few countries even regulate the privacy of information relating to corporations.
- We are committed to handling personal data responsibly and in compliance with applicable privacy laws worldwide.
- Every employee is responsible for safeguarding personal data within the Company’s control.

Every employee is responsible for safeguarding personal data within the Company’s control.
WHAT TO DO

• Ask about and comply with all of the following as they apply to personal data, including:
  – applicable laws and regulations of locations from which the personal data is collected and in which it is processed or used;
  – the internal and customer-facing privacy policies of the Company; and
  – any applicable contractual obligations.
• Be aware of personal data that is subject to specific laws, such as customer financial information, cable subscriber personally identifiable information, customer proprietary network information ("CPNI"), health data and children’s information, and consult with the law department of your business unit for any questions.
• Collect, process and use only the personal data you need for legitimate business purposes.
• Retain personal data in accordance with your business unit's document retention guidelines and ensure it is disposed of securely.
• Use “anonymous” data (names and other personal information removed and not identifiable) or “aggregated” data (summarized so as not to be identifiable to an individual) instead of personal data where appropriate or required.
• Limit access to personal data to individuals who need it for a legitimate business purpose, and, if third parties are involved, carry out a third party risk assessment as appropriate and ensure that there is a written agreement in place that has been reviewed by a Company lawyer.
• Use care to prevent unauthorized access in processing of personal data or accidental loss or destruction of personal data.

• If you learn that personal data has been used in violation of this policy, or if you learn that the security of any system, device or document containing personal data has been compromised (e.g., emails sent to the wrong person, papers left on a train, a Company website hacked), immediately notify your supervisor and a Company lawyer.

WHAT TO WATCH OUT FOR

• Inadequate access or security controls for personal data, such as:
  – e-mailing or otherwise distributing personal data to a larger group than legitimately needs it;
  – using your personal email account for work purposes instead of using a Company remote working solution;
  – leaving printouts with personal data at a printer, copy machine or fax machine where others may see them, or not locking them away at the end of the day;
  – not following local procedures for the secure disposal of confidential waste (including IT equipment); or
  – storing personal data in unsecured files or on unsecured devices (e.g., unencrypted USB devices), or not transferring information in a secure manner.
• Sharing of personal data with third parties, such as suppliers or contractors, who lack appropriate security safeguards or restrictions on information use.
• Transfers of personal data between countries without considering applicable legal requirements. If you have collected personal data in a country regulated by a “data protection” law (such as most countries in Europe), consult with the law department of your business unit as to the restrictions on using or sharing that information.

• When you record information about people, it’s important to remember that in many countries individuals have rights of access to the information we hold about them.

• Consult with a Company lawyer in relation to any new business initiative that may capture or use personal data.

ADDITIONAL RESOURCES IN THE INTEGRITY SECTION OF YOUR BUSINESS UNIT’S INTRANET

• Frequently Asked Questions

• Confidentiality policy in your business unit’s Employee Handbook

OTHER APPLICABLE CODE POLICIES

• Supplier Relationships
Our Commitment to Our Company

We must keep in mind our obligation of loyalty and ethical duty to the Company. We are entrusted with Company assets, both tangible and intangible, including intellectual property, confidential information, time, funds and equipment. We are each responsible for using Company assets only for legitimate business purposes and for protecting them from damage, loss, theft or misuse. Below are several areas that focus on this commitment to the Company and the conduct expected from each of us.

- Intellectual Property
- Security and Crisis Management
- Conflicts of Interest
- Gifts and Business Entertainment

Intellectual Property

INTRODUCTION

Intellectual property is among our most valuable assets. Protecting, maintaining and defending our rights, and respecting the intellectual property rights of others, is critical to the success of our Company. Each employee must be aware of and follow our policies regarding the responsible use of intellectual property and content protection.

WHAT TO KNOW

- “Intellectual property” primarily refers to copyrights, trademarks, trade names, patents and trade secrets. Comcast’s intellectual property is embodied in a variety of things: software; hardware and network-based technology; inventions and innovations; entertainment content; confidential business processes; customer lists; and other confidential business ideas and information. The protection of intellectual property—such as motion pictures, television shows, website content, digital and mobile applications, logos, brands, inventions and innovations—is critical to the success and vitality of the business.

- Every employee is responsible for safeguarding our intellectual property.

Every employee is responsible for safeguarding our intellectual property.
• We must respect the valid intellectual property rights of others. The unauthorized use of others’ intellectual property can expose the Company, and employees, to lawsuits and even criminal penalties.

• If you have a question about procedures regarding the protection or use of intellectual property or about any of the topics addressed in this policy, contact the law department of your business unit.

WHAT TO DO

• Follow your business unit’s applicable policies and guidelines regarding the handling and security of intellectual property. Be alert to business practices that may result in the unauthorized distribution or other unauthorized use of Company intellectual property.

• Take care in everyday matters by, for example, not leaving papers in conference rooms or other open work areas, not leaving notes on blackboards or whiteboards in conference rooms, and not sharing passwords or employee ID badges.

• Secure all physical and electronic proprietary content when not in use. When discarding confidential documents, place them in secure onsite shred containers for destruction. Contact your business unit’s records management department for assistance.

• Use caution in discussing Company business in common areas and public places, such as elevators, trains and airplanes.

• Consult with the law department of your business unit to determine whether licenses or approvals to use the intellectual property of others are necessary, and how to obtain them.

• Understand your responsibilities to the Company regarding creative works, ideas, inventions and innovations that you develop that relate to the Company’s business.

• Follow the requirements of your business unit in handling unsolicited ideas from third parties and unsolicited employee submissions.

• Comply with applicable guidelines for use of the Company’s trademarks and trade names.

WHAT TO WATCH OUT FOR

• Distributing intellectual property to third parties, or disclosing nonpublic intellectual property to third parties, without an appropriate written agreement in place or in an unapproved, insecure manner.

• Discussing with or otherwise disclosing to a third party information that is confidential or proprietary to your business (including, without limitation, any creative, technical or business ideas) without an appropriate written agreement in place.

• Hiring or engaging an outside company or person to develop intellectual property without having put a written agreement in place. Such an agreement must be reviewed by the law department of your business unit and must cover rights in the developed intellectual property as well as in other results of the work.

• Unauthorized copying or use of copyrighted works of others (including unauthorized downloading or distribution of newspaper and magazine articles, website articles, computer software, music, movies, pictures and graphics).

Be alert to business practices that may result in the unauthorized distribution or other unauthorized use of Company intellectual property.
• Receiving from anyone, or communicating to others within the Company, a suggestion for a film, television show or new business idea without following your business unit’s unsolicited idea procedures.

• Consult with the law department of your business unit where appropriate before:
  
  – Producing or distributing content, in order to confirm it does not infringe on the intellectual property rights of others.
  
  – Launching a new service or product, in order to determine if any intellectual property clearance work should be performed.
  
  – Introducing (or providing information about) a potentially patentable new product or service to a third party.
  
  – Communicating with any third party about the scope or validity of the Company’s intellectual property (including any belief that someone may be infringing such property) or taking action against a suspected infringer.
  
  – Hiring a new employee, especially a person who previously worked for a competitor, without putting in place safeguards to prevent the person from inadvertently disclosing or using the proprietary information of the previous employer.
  
  – Accepting confidential or proprietary information from a third party.

ADDITIONAL RESOURCES IN THE INTEGRITY SECTION OF YOUR BUSINESS UNIT’S INTRANET

• Frequently Asked Questions

• Confidentiality policy in your business unit’s Employee Handbook

Security and Crisis Management

INTRODUCTION

The safety of our people and operations is critically important at Comcast. We are committed to protecting employees through vigilant security regarding our property, technology and business operations. We have implemented procedures that address the prevention of criminal acts and ensure that employees understand potential threats to our people, operations and facilities. We have created emergency response and business continuity plans to ensure key business functions will continue to operate effectively in the event of an emergency. It is the responsibility of every employee to follow the steps below to help ensure the safety of our team and operations.

WHAT TO KNOW

• We seek to provide a workplace that is safe and secure.

• Security threats can include threats to our property, personnel and computer systems.

• All users of our facilities, including employees, must be properly authorized to gain entry.

• User identification must be displayed at all times in all of our facilities.

• The removal of Company property and equipment from our premises is prohibited without proper authorization.
WHAT TO DO

• Protect Company assets against damage, loss, theft or other misuse.

• Learn and follow the portions of the security procedures and business continuity plans for your business unit that are applicable to you.

• Know your security leaders and how to contact them.

• Understand life safety guidelines, including evacuation and shelter-in-place procedures.

• Understand and follow your business unit’s emergency response protocol, including the communications strategy.

• Be alert to data or computer system security threats.

• Be aware of your surroundings; if you see or observe suspicious activity, notify Security immediately.

• Be alert to and report—to your supervisor, Human Resources or Security—any concern about workplace violence.

• Properly secure your workspace and computer work stations at the end of each work day.

• Comply with global immigration rules and travel policies, including how to obtain appropriate pre-clearances and authorizations for travel to high-risk destinations.

• Understand the proper procedures for handling suspicious mail and packages.

WHAT TO WATCH OUT FOR

• Visitors to a Company facility who do not display an employee ID badge or authorized visitor pass.

• Security concerns about your physical surroundings.

• Potential physical or computer system security breaches in any of our facilities.

• Unattended or unsecured equipment or property, including laptops, packages, knapsacks, bags and luggage.

• Efforts or offers to circumvent travel safety policies or country entry requirements.

ADDITIONAL RESOURCES IN THE INTEGRITY SECTION OF YOUR BUSINESS UNIT’S INTRANET

• Frequently Asked Questions

• Physical and Environmental Security policy in your business unit’s Employee Handbook

Be aware of your surroundings; if you see or observe suspicious activity, notify Security immediately.
Conflicts of Interest

INTRODUCTION
On the job or in your free time, nothing you do should conflict with your responsibilities or duty of loyalty to the Company. Even when nothing wrong is intended, the appearance of a conflict can have negative effects. It is crucial to consider how your actions may appear, and to avoid the perception of a conflict of interest. This policy requires employees to disclose and receive approval, as needed, for all outside work, financial interests and other personal activities or relationships that may create, or appear to create, a conflict of interest. Conflicts of interest may also involve the offer or acceptance of gifts or business entertainment. Because of the importance of this area, we have created a separate Gifts and Business Entertainment Policy.

WHAT TO KNOW
• A conflict of interest may exist when you are involved in activities that might interfere, or appear to interfere, with the performance of your duties and responsibilities, or that could reflect negatively on the reputation of the Company.

• Owning a financial interest in an outside business that has a current or potential business relationship with the Company, such as a supplier, contractor, customer, competitor, potential competitor or company in which the Company has an investment may be a conflict of interest if you have the ability to influence the success of that business or affect the Company’s relationship with that outside business. The term “outside business” means a company or other for-profit business organization, including a family-owned business.

• A potential conflict of interest could arise if you have the ability to influence Company decisions relating to employment or business transactions that affect a family member or close personal relationship.

• The Company encourages you to participate in civic and charitable activities. Participation in a civic or charitable organization on your own time requires prior approval by an Authorized Approver only if such participation might present a conflict of interest or the appearance of a conflict of interest, or harm the Company’s reputation or business relationships.

Business decisions made by Company employees should be made solely on the basis of competitive factors.

WHAT TO DO
General Principles
• Avoid personal activities or relationships that may cause actual or potential conflicts or create the appearance of a conflict with your job or the Company’s interests. For example, do not:
  – direct Company business to, or make Company decisions regarding, an outside business owned or managed by you, a family member or a close personal relationship; or
  – make any employment decisions regarding a family member or close personal relationship (including hiring, promoting or directly supervising).

• Devote your best efforts to the Company’s interests while at work.

• Notify your supervisor or contact another resource (e.g., Comcast Listens, NBCUniversal Integrity Helpline or a Company lawyer) if you know of a possible conflict of interest involving another employee or anyone else representing the Company.
Outside Activities and Financial Interests

- Do not use Company information, resources, influence, time, intellectual property or facilities for personal benefit or to promote an outside business or activity of yours, a family member or a close personal relationship. This includes the use of Company office equipment, e-mail and computer applications (e.g., to print or distribute flyers to promote a family member’s business or invitations to a personal social event).
- Do not take for yourself personally opportunities in which the Company may have an interest. Do not pursue opportunities for your own benefit that you learned of through your Company position or access to Company information.
- Get approvals from your supervisor and an Authorized Approver before:
  - Working as an employee, consultant or officer or being a director of an outside business while you are a Company employee.
  - Participating in outside writing, blogging, lecturing or other activities that draw on proprietary or confidential information of the Company gained as part of your employment with the Company. For example, seek approval of any activities that may inadvertently disclose proprietary or confidential information about technology trials, product development, scripts or show outcomes.
  - Participating in civic or charitable activities while on Company time or using Company resources or assets.
- Get approval from an Authorized Approver before:
  - Soliciting charitable contributions from current or potential suppliers, contractors, customers or other outside businesses using the Company’s name or your position at the Company.
  - Owning (either directly or indirectly through an entity, family member, close personal relationship or other person) stock or any other financial interest in any outside business that has a current or potential business relationship with the Company or is a competitor or potential competitor of the Company. You do not need approval to own such an interest if:
    » the company is a public company and you purchase stock in the open market (i.e., through a stockbroker and not directly from the company);
    » you own less than one percent of a class of the company’s stock; and
    » you do not perform any business function, provide any advice, or have any ability to influence the policies or activities of the company.
  - Soliciting or accepting any offer (even unsolicited) to acquire securities (including by having securities reserved for you in an IPO) of any outside business if either the outside business or the person (or third party) making the opportunity available to you on behalf of the outside business has current or potential business relationships with the Company or is a competitor or potential competitor of the Company. This restriction applies even if you are paying market price for the securities.
- Get approval from your business unit’s General Counsel before running for election or accepting appointment to a national, state or local public office. The term “public office” is interpreted broadly, and includes, but is not limited to, school boards, local government councils and all governmental offices and positions.
WHAT TO WATCH OUT FOR

• Personal discounts or other benefits from Company suppliers, contractors, customers or other third parties that may not be available to the public or your peers at the Company.

• Personal relationships that may conflict with your job responsibilities or compromise Company interests.

ADDITIONAL RESOURCES IN THE INTEGRITY SECTION OF YOUR BUSINESS UNIT’S INTRANET

• Frequently Asked Questions
• List of Authorized Approvers
• Outside Employment policy in your business unit’s Employee Handbook
• Employment of Relatives policy in your business unit’s Employee Handbook
• Social Media policy in your business unit’s Employee Handbook

OTHER APPLICABLE CODE POLICIES

• Gifts and Business Entertainment
• Anti-Corruption Laws
• Interacting with Governments and Political Activities
• Supplier Relationships

Gifts and Business Entertainment

INTRODUCTION

We believe business decisions should be based on competitive factors. The offer or acceptance of gifts or business entertainment (as defined below) can create the appearance that business decisions are being influenced by other factors. Gifts or business entertainment should never be offered or accepted in order to influence a business or official decision or obtain an improper advantage. This policy requires employees to obtain approval in certain circumstances when offering or accepting gifts or business entertainment.

NOTE: All gifts and business entertainment involving a Government Official require prior approval from a Senior Attorney and must comply with the Interacting with Governments and Political Activities Policy and the Anti-Corruption Laws Policy.

WHAT TO KNOW

• A “gift” is anything of tangible or intangible value, including cash, gift certificates or gift cards, transportation, lodging, discounts, promotional items, contributions to a charity or other non-profit organization, and the recipient’s use of the donor’s time, equipment or facilities. A “gift” also includes the following if not attended by the donor: meals, entertainment, participation in recreational activities or events, and tickets, passes or other access to cultural or sporting events.

• “Business entertainment” includes the following if attended by the donor and during which business matters are discussed: meals, entertainment, participation in recreational activities or events, and tickets, passes or other access to cultural or sporting events. (Note that if business is not discussed, it is considered a gift.)
• The term “Authorized Gift and Business Entertainment Approver” means:
  – the President (or other business unit head) of your business unit (for example, a Division President in Comcast’s Cable Division, or a President of a Universal Pictures division);
  – the Chief Financial Officer of your business unit;
  – a Senior Attorney; or
  – a Senior HR Professional.

Click here for a current list of Authorized Gift and Business Entertainment Approvers. This information can also be found in the Integrity Section of your business unit’s intranet.

• Business decisions made by Company employees should be made solely on the basis of quality, service, price and other competitive factors.

• Employees in a position to deal with persons or outside businesses that have a current or potential business relationship with the Company must be particularly sensitive to the potential conflict of interest that may arise in the offer or acceptance of gifts or business entertainment.

WHAT TO DO

• Offer or Acceptance of Gifts:
  – For all gifts relating to a Government Official, obtain the prior approval of a Senior Attorney.
  – For all gifts not relating to a Government Official, obtain the prior approval of an Authorized Gift and Business Entertainment Approver before offering or accepting a gift or gifts valued above $250 in total per calendar year per each supplier, contractor or other outside business receiving or offering the gift.

  – Never offer or accept a gift of cash, regardless of the amount, except with prior approval by an Authorized Gift and Business Entertainment Approver in situations where cash gifts are required out of respect for local custom (e.g., funerals in some Asian countries).

  – Nominal gift certificates or gift cards may be offered or accepted, such as gift cards to a coffee house or doughnut shop. However, other cash equivalents should never be offered or accepted without the prior approval of an Authorized Gift and Business Entertainment Approver.

  – All gifts, regardless of the amount, must be:
    » consistent with the Company’s business interests;
    » prudent and reasonable by local or industry standards;
    » infrequent in occurrence;
    » consistent with customary business practices;
    » given or accepted without an expectation of reciprocity; and
    » compliant with all laws and regulations.

  Obtain the prior approval of an Authorized Gift and Business Entertainment Approvers before offering or accepting a gift valued above $250.

• Offer or Acceptance of Business Entertainment:
  – For all business entertainment relating to a Government Official, obtain the prior approval of a Senior Attorney.

  – Business entertainment not relating to a Government Official may be offered or accepted without prior approval as long as it:
    » is consistent with the Company’s business interests;
    » is prudent and reasonable by local or industry standards;
    » is infrequent in occurrence;
    » is consistent with customary business practices;
    » is given or accepted without an expectation of reciprocity; and
    » complies with all laws and regulations; and

Speak up! ComcastListens Talk with your supervisor or visit www.ComcastListens.com to learn more about how to raise a concern.
» complies with any dollar limit or other guidelines established by your business unit (for example, the Corporate and Cable Divisions of Comcast have each established a $250 dollar limit).

Click here for a link to various business units’ Gift and Business Entertainment Guidelines.

- Obtain the prior approval of an Authorized Gift and Business Entertainment Approver before offering or accepting travel or accommodations connected to business entertainment above $250 per trip.
- Obtain the prior approval of an Authorized Gift and Business Entertainment Approver before offering or accepting business entertainment for a family member or personal guest above $250 in total per calendar year per each supplier, contractor or other outside business receiving or offering the business entertainment.

Appropriate business entertainment does not include adult entertainment or any other entertainment or event that could negatively affect the reputation of the Company or individuals involved.

- Gifts or business entertainment should never be offered or accepted where:
  - there is no real business purpose;
  - the donor’s purpose is to motivate the recipient to take (or fail to take) an action that could be a violation of law, regulation, policy or contract; or
  - public disclosure would harm the reputation of the Company, the donor or the recipient.

Make sure you understand and comply with your business unit’s business entertainment and dollar limits.

WHAT TO WATCH OUT FOR

- Offering or accepting multiple gifts to or from the same vendor within the same calendar year.
- Offering or accepting business entertainment that exceeds the dollar limits or other guidelines established by your business unit.
- Accepting tips or gratuities (cash or otherwise) from customers. Excellent customer service should be provided at all times, and accepting gratuities sends the message that better customer service is given to those customers that provide a tip.

ADDITIONAL RESOURCES IN THE INTEGRITY SECTION OF YOUR BUSINESS UNIT’S INTRANET

- Frequently Asked Questions
- List of Authorized Gift and Business Entertainment Approvers
- Business Unit Gift and Business Entertainment Guidelines

OTHER APPLICABLE CODE POLICIES

- Conflicts of Interest
- Anti-Corruption Laws
- Interacting with Governments and Political Activities
- Supplier Relationships
Our Commitment to Our Shareholders

We are committed to delivering value to our shareholders while conducting business in an ethical manner. In our day-to-day decisions, we should never take actions to secure short-term goals at the expense of long-term shareholder value. We take responsibility for our actions as individuals and as an organization by reporting information honestly, timely and accurately, maintaining transparent Company records and prohibiting trading on material, nonpublic Company information.

- Financial Responsibility
- Insider Trading and Stock Tipping

Financial Responsibility

INTRODUCTION

Financial responsibility principles require us to protect the Company through integrity in record keeping, financial reporting and public disclosures. We have a responsibility to maintain our books and records, prepare our financial statements, and make public disclosures in compliance with the law and accounting standards.

WHAT TO KNOW

- Financial responsibility encompasses:
  - Honest, fair and accurate financial reporting.
  - Making full, accurate, timely and understandable public disclosures to government agencies, such as the Securities and Exchange Commission, and the public.
  - Complying with our system of internal controls.

- Corrections to our financial records and reports that are timely identified, reported in accordance with our system of internal controls and appropriately corrected within our internal controls system are not deemed violations of this policy.

- If you are a professional employee in the areas of accounting, internal audit, finance, financial planning and analysis, investor relations, risk management, tax or treasury, you should review our Obligations of Financial Professionals Policy for additional obligations applicable to you.

We should never take actions to secure short-term goals at the expense of long-term shareholder value.
WHAT TO DO

• Ensure that all books and records:
  – are maintained in accordance with applicable law;
  – fairly and accurately reflect, in reasonable detail, the transactions or occurrences to which they relate; and
  – fairly and accurately reflect, in reasonable detail, our assets, liabilities, revenues and expenses.

• Make sure that our books and records do not contain any false or misleading statements or entries.

• Never intentionally misclassify any transaction as to accounts, departments or accounting periods.

• Do not change accounting or business practices or policies for the sole purpose of enhancing near-term financial performance at the expense of long-term shareholder value, such as by “smoothing” or otherwise managing quarterly or annual results.

• Maintain accurate, appropriate and reasonably detailed documentation to support all transactions.

• Provide all relevant information to, and never conceal information from, our internal auditors or our independent auditors.

• Prepare all external reports and disclosures that are based on our books and records in accordance with generally accepted accounting principles (“GAAP”) and securities laws.

• Preserve documents (including email) in accordance with your business unit’s records and information management policies.

WHAT TO WATCH OUT FOR

• Financial records or subscriber statistics that appear inaccurate or are not transparent.

• Inaccurate financial reports or statements, such as overstated travel and entertainment expenses or erroneous invoices or timesheets.

• A request to document a transaction in a way that does not accurately reflect its substance.

• Financial results that seem inconsistent with underlying performance.

• Statements or communications that don’t make business sense or are inaccurate.

• An actual or apparent conflict of interest that affects any employee with financial reporting, accounting or internal controls responsibilities.

• Circumvention of proper review and approval processes.

• Inadequate routines and controls to preserve financial records.

ADDITIONAL RESOURCES IN THE INTEGRITY SECTION OF YOUR BUSINESS UNIT’S INTRANET

• Frequently Asked Questions

• Obligations of Financial Professionals Policy
Insider Trading and Stock Tipping

INTRODUCTION

In the course of your service with Comcast, you may learn of material information about Comcast, our subsidiaries or other companies before it is made public. What is “material” information? It is information that an investor may consider important in deciding whether to buy, sell or hold securities.

You may learn about material information by simply overhearing a hallway conversation or coming across a memo left at a copy machine. You may not buy or sell securities of Comcast, any of our subsidiaries or any other company while aware of material information before that information is made public (doing so is known as “insider trading”) or convey material information to others who might trade on the basis of that information before it is made public (doing so is known as “tipping”).

WHAT TO KNOW

- Material information includes earnings announcements, earnings forecasts and significant financial developments (including dividend or share repurchase actions; possible acquisitions, divestitures, investments, or financings; loss of or entry into a significant contract; important product, technology or strategy developments; changes in key personnel; and major litigation developments and governmental investigations.

- These prohibitions against insider trading and tipping apply not only to Comcast’s securities, but also to the securities of any of the Company’s subsidiaries that are registered with the Securities and Exchange Commission or are listed on any securities exchange (such as the NASDAQ or New York Stock Exchange). In addition, these prohibitions against insider trading and tipping apply to the securities of any company about which you have material, nonpublic information.

- “Securities” are defined broadly to include more than stock. Put and call options, debt securities (such as bonds and notes) and any other similar equity or debt or instruments are deemed securities. Also, certain forms of hedging or monetization transactions and other complex transactions can present unique insider trading risks.

- Consequences of insider trading and tipping can be severe. Insider trading and tipping is against the law and can subject you to potential penalties that include imprisonment, disgorgement of profits, substantial fines and monetary damages. Similar penalties may be imposed on people who knew, or recklessly disregarded, that an employee was engaging in insider trading and failed to take appropriate steps to prevent it. The Company also could suffer serious business and reputational damage from improper disclosure of information or an insider trading investigation.

WHAT TO DO

- Do not buy or sell, either directly or indirectly through entities, family members or other persons, the securities of Comcast, any of our subsidiaries or any other company while you are in possession of material, nonpublic information. You should assume that any nonpublic information about a company that would influence your own decision about whether to buy or sell

Speak up! ComcastListens Talk with your supervisor or visit www.ComcastListens.com to learn more about how to raise a concern.
that company’s securities is material, nonpublic information, and you should not, until after the information has become public:

- buy or sell the security; or
- recommend that anyone else buy or sell the security. If you are unsure whether information could be deemed “material,” contact the law department in your business unit.

- Do not disclose to any person any material information about Comcast, our subsidiaries or any other company that you learn in connection with your service with the Company until that information is generally available to the public. This includes not disclosing this information to analysts, shareholders or other securities market professionals.

- Treat decisions relating to investments in Comcast stock through your 401(k) plan or the employee stock purchase plan the same way you would treat decisions involving a direct purchase or sale of securities. Accordingly, you should not switch into or out of Comcast stock in your 401(k) plan or change your payroll deduction in the employee stock purchase plan if you are aware of material, nonpublic information about Comcast.

- Maintain the confidentiality of proprietary or other important or sensitive information about the Company and do not convey information to anyone outside of Comcast unless necessary for your business activities. You also should maintain the confidentiality of information that you learn in the course of your service about suppliers, contractors, customers, companies in which the Company has an investment and other third parties.

- If the nature of your business activities and your position in the business subject you to additional requirements relating to buying and selling securities (such as the preclearance of personal trades or being subject to a blackout policy), learn and follow all of those requirements, and review the Comcast Blackout Period and Pre-Clearance Policy. In addition, CNBC employees and employees in the various news divisions of NBCUniversal are subject to additional policies and guidelines.

- If questions arise, consult a Senior Attorney before trading in the relevant security or disclosing the types of information described above.

WHAT TO WATCH OUT FOR

- Buying or selling a security because you learn information that you think will make the price go up or down once it is publicly announced. Even after the information is released to the public, there must be adequate time for the market to become fully aware of the information before it is considered to be public information.

- Buying or selling a security before a significant Company announcement.

- Talking to people (both inside and outside the Company) who do not have a need to know information about what you have been working on, where you have been traveling on Company business, or who has visited the office.

ADDITIONAL RESOURCES IN THE INTEGRITY SECTION OF YOUR BUSINESS UNIT’S INTRANET

- Frequently Asked Questions
- Blackout Period and Pre-Clearance Policy
- Fair Disclosure Policy
Supplier Relationships

INTRODUCTION

Our relationships with suppliers are based on lawful, efficient and fair practices. We expect our suppliers to obey the law, including laws that require them to treat workers fairly, provide a safe and healthy work environment and protect environmental quality. Following these guidelines helps ensure that our supplier relationships will not damage our reputation.

WHAT TO KNOW

• We strive to do business only with suppliers who comply with applicable laws and standards governing labor, health and safety.

• We provide competitive opportunities, where practical, to all suppliers, whether they are large or small, local, national or international, or internal or external.

• Employees must strictly follow Company policies restricting the acceptance of gifts and business entertainment from suppliers.

WHAT TO DO

• Conduct business only with suppliers that comply with national, local and other applicable legal requirements and Company guidelines relating to labor, the environment, health and safety. Unacceptable supplier practices include:

  – employing workers younger than the required minimum age or the age of 16, whichever is higher
  – using forced, prison or indentured labor, or workers subject to any form of compulsion or coercion
  – failure to observe applicable environmental laws and regulations
– failure to observe applicable laws and regulations governing wage and hour, days of service and overtime payment
– failure to provide workers with a workplace that meets applicable health and safety standards
– failure to maintain and enforce policies requiring adherence to lawful business practices, including a prohibition against bribery

• Provide a competitive opportunity for suppliers to earn a share of the Company’s purchasing volume, including small businesses and businesses owned by minorities and women.

• Select suppliers in accordance with your business unit’s procurement or sourcing procedures (including concerning competitive bidding).

• Safeguard our confidential and proprietary information (including that of our customers) provided to suppliers and safeguard any supplier-provided information.

• Maintain open, honest dialogue with suppliers, consistent with good business practices.

• Evaluate all supplier offerings on the basis of quality, reliability, performance, price, service and technical requirements.

• Follow government acquisition regulations when purchasing materials and services for fulfilling government contracts.

• Disclose any potential conflicts of interest regarding suppliers or potential suppliers to your supervisor or to an Authorized Approver.

WHAT TO WATCH OUT FOR

• Potential conflicts of interest in supplier selection, such as offers of gifts or other items of value.

• Doing business with a supplier owned or managed by an employee’s family member or a close personal relationship.

• Unsafe conditions in supplier facilities.

• Supplier employees who appear to be underage or subject to coercion.

• Apparent disregard of environmental standards in supplier facilities.

• Entrusting personal data or confidential information to suppliers without ensuring that they have appropriate technical, physical and organizational measures to prevent unauthorized access or use. Follow applicable business unit supplier risk assessment procedures, especially when a third party will have access to our systems or data.

• Solicitation, receipt or use of a supplier’s proprietary data other than as authorized by such supplier.

ADDITIONAL RESOURCES IN THE INTEGRITY SECTION OF YOUR BUSINESS UNIT’S INTRANET

• Frequently Asked Questions

OTHER APPLICABLE CODE POLICIES

• Anti-Corruption Laws

• Conflicts of Interest

• Gifts and Business Entertainment

• Interacting with Governments and Political Activities

• International Trade Controls

• Money Laundering Prevention

• Privacy
Interacting with Governments and Political Activities

INTRODUCTION

We conduct business with national, state and local governments and government-owned enterprises. In the course of our business activities, we frequently interact with Government Officials. In every instance, employees must adhere to the highest ethical standards and comply with all applicable laws and regulations, including special requirements associated with government contracts. In addition, we comply with national, state and local restrictions and reporting requirements addressing political contributions, lobbying activities and gifts and business entertainment to Government Officials (defined below).

When interacting with a Government Official, employees must also comply with the Anti-Corruption Laws Policy.

WHAT TO KNOW

- There are various national, state, local and international laws that prohibit or otherwise restrict the provision of gifts, cash, business entertainment or anything else of value to Government Officials. These laws may also forbid or restrict one’s ability to provide anything of value to another person or entity (such as a charity) at the request of a Government Official. Therefore, any gifts or business entertainment involving a Government Official must be pre-approved by a Senior Attorney, regardless of value.

- “Government Official” is defined as any official (elected or appointed), officer, employee (regardless of rank), or other person acting as a representative of:
  - a U.S. or non-U.S., federal, national, state, provincial or local government, including any department, agency, instrumentality, state-owned or state-controlled company, public international organization (such as the United Nations or World Bank), or political party, party official or any candidate for political office; or
  - an entity that is financed in large measure through public appropriations, is widely perceived to be performing government functions, provides services to all inhabitants of a jurisdiction, or has its key officers and directors appointed by a government. Examples include, but are not limited to, a public school, library, hospital, university, authority or commission.

- The government contracting process can be complex and may impose a variety of legal obligations, not only on the business unit proposing the contract, but also on the Company as a whole. Violating the terms of a government contract or laws regulating such contracts can potentially lead to severe criminal, civil and reputational damage for the Company and individual employees. Violations can also lead to temporary or permanent loss of the ability to do business with the government entity.

- Government contracts include agreements with any country, regional, state, municipal or local agency or entity. They also include deals with “quasi-government” entities, such as state-owned or state-run broadcasters, hospitals, universities, port authorities and convention centers and arenas. Our government business may include:
  - providing cable, internet, phone or other services to government entities, including public schools, libraries, hospitals, universities, authorities or commissions;

- licensing content to government entities;
- production–related agreements (including participating in tax credit programs or trade-outs with local tourism agencies);
may be used in connection with federal fundraising activities under certain limited circumstances. We are also subject to similar state and local limitations on political contributions to candidates for state and local office, which may vary widely.

WHAT TO DO
• Obtain pre-approval of a Senior Attorney before offering any gift, business entertainment or anything else of value, regardless of value, to any Government Official.
• Do not offer to employ, or retain as a consultant, a Government Official or a member of a Government Official’s immediate family without the pre-approval of your business unit’s General Counsel.
• Abide by all applicable laws and regulations relating to working with governments, particularly special requirements associated with government contracts and transactions.
• Be truthful and accurate when dealing with Government Officials and agencies.
• Adopt processes that ensure that reports, certifications, statements and proposals are current, accurate and complete and that contract requirements are communicated to, complied with and documented by the responsible parties.
• Obtain required approvals from your business unit’s law department before bidding for, entering into or renewing any government contract.
• To ensure that the Company and our employees are in compliance with applicable lobbying laws, do not engage in, or retain an outside person to engage in, any government lobbying activities (as described above) on behalf of the Company without the prior approval of your business unit’s General Counsel.

Abide by all applicable laws and regulations relating to working with governments, particularly special requirements associated with government contracts and transactions.
• Never use Company funds or other Company assets to make a political contribution, whether at the national, federal, state or local level, without the prior approval of your business unit’s General Counsel and the Comcast Corporation Political Affairs department. A “political contribution” means any benefit provided to a national, federal, state or local candidate, candidate campaign, political party, political committee (e.g., a political action committee (“PAC”), inaugural or ballot measure committee), political convention, any entity exempt from federal income taxes under Section 527 of the U.S. Internal Revenue Code, or a 501(c)(4) social welfare organization. This includes monetary contributions (e.g., a corporate check or purchase of tickets to a political fundraiser) as well as “in-kind” contributions (e.g., the use of corporate personnel or facilities, or the donation of free airtime to a candidate).

• In order to prevent an illegal in-kind corporate political contribution, do not use Company facilities, office space or personnel in connection with volunteer activity (such as fundraising) for a political campaign, or perform volunteer activity for a political campaign during work hours, without the prior approval of your business unit’s General Counsel, and the Comcast Corporation Political Affairs Department.

• Employees are permitted and encouraged to participate in their personal capacity in federal, state and local political activities in compliance with applicable laws. However, do not engage in overt, visible or partisan political activity that gives the appearance that you are expressing the views of the Company, or use the Company’s name in connection with such activities, without the prior approval of your business unit’s General Counsel and the Comcast Corporation Political Affairs Department.

• Do not engage in political activities other than on your own time or make personal political contributions, other than from personal funds as a private citizen. When making or soliciting personal political contributions, comply with applicable state and local “pay-to-play” laws that may trigger an automatic ban on the Company’s ability to enter into contracts with those government entities. We provide employees, officers and directors covered under these laws with appropriate additional information, including pre-clearance requirements where applicable.

• Do not request reimbursement or other compensation for personal political contributions. Under no circumstance will the Company reimburse, or otherwise compensate, any employee for a political contribution.

WHAT TO WATCH OUT FOR
• Special requirements that apply to transactions with governments, including contractual certifications and representations requiring compliance with specific laws and regulations.

• Submission of inaccurate or incomplete cost, pricing or other data to the government.

• Donations to non-profits that have relationships with, or are solicited by, a public official or government employee. For example, we must comply with U.S. lobbying rules that require the reporting of donations to organizations with certain relationships with a U.S. federal official, as well as expenses related to events that honor or recognize a U.S. federal official. We have established separate procedures to capture information relating to these payments in order to comply with these reporting requirements.

• Collecting or forwarding political contribution checks from other people to a federal, state or local candidate, political party or political committee. Any such “bundling” may be illegal and requires the prior approval of your business unit’s General Counsel.
ADDITIONAL RESOURCES IN THE INTEGRITY SECTION OF YOUR BUSINESS UNIT’S INTRANET

- Frequently Asked Questions
- List of Authorized Gift and Business Entertainment Approvers

OTHER APPLICABLE CODE POLICIES

- Anti-Corruption Laws
- Conflicts of Interest
- Gifts and Business Entertainment
- Supplier Relationships
Our Commitment to the Law

A fundamental obligation that we owe to the nations and communities in which we do business is to obey the law. We adhere to all applicable laws everywhere we do business. **There is no business reason, no management pressure, no unwritten understanding that ever justifies violating the law.** If you feel pressured to violate a law, immediately contact a Company lawyer or Comcast Listens. While this commitment refers to all applicable laws, a few areas are of particular significance and applicability.

- Complying with Competition Laws
- Anti-Corruption Laws
- Money Laundering Prevention
- International Trade Controls

Complying with Competition Laws

**INTRODUCTION**

Antitrust laws in the United States, known as competition laws in most other countries, are designed to ensure open and vigorous competition in the marketplace. Agreements or understandings among competitors that limit or restrict competition are, in most circumstances, unlawful. Unilateral actions that injure or prevent competition can also be illegal if undertaken by a company with significant market power. The Company and our employees shall abide by the antitrust laws and all other laws governing fair competition applicable to our businesses. Competition laws are complex and their application is fact specific. Consult a Company lawyer early when questions arise under this policy.

**WHAT TO KNOW**

- Antitrust laws prohibit agreements (expressed or implied, formal or informal, written or oral) that unreasonably restrain trade or reduce competition. These may include, for example, agreements between or among competitors to fix prices or other competitive terms and agreements to allocate sales, customers or service territories.

- Unilateral efforts to injure or prevent competition by companies with significant market power may also violate antitrust laws.

- It is possible for an entity to be both a valued partner for some purposes and a competitor for others.
In certain situations, it may be improper for a Company employee to share information with an employee of a different business unit if it could be used in a way that injures competition.

Government agencies can review proposed transactions and investigate Company activities that they believe may be anticompetitive.

The Company is subject to several consent decree agreements with the Government relating to the Antitrust laws, which impose additional obligations on the Company.

Violating competition laws or the consent decrees can have severe consequences, including criminal prosecution, criminal and civil fines and large damage awards.

Detailed guidance regarding compliance with competition laws can be found in the Comcast Compliance Guide to the Antitrust and Competition Laws.

WHAT TO DO

Understand and follow the Compliance Guide to the Antitrust and Competition Laws and any specific guidelines your business unit has regarding complying with competition laws or consent decrees.

Don’t assume you’re an expert. While the basic requirements of the competition laws—to refrain from monopolizing or restraining trade—are simple, the application of these principles to everyday circumstances often is not.

Proceed with caution and seek guidance when you’re not sure. Because application of competition laws to any situation is highly dependent on the particular circumstances, it is essential that you understand and avoid situations that could result in violation of the law, even unintentionally, and that you consult immediately with the law department of your business unit regarding any dealings that you suspect implicate competition laws.

WHAT TO WATCH OUT FOR

The following guidelines, while not a summary of the Compliance Guide to the Antitrust and Competition Laws, illustrate its principles. Unless you have received specific guidance from the law department of your business unit, you should not:

- Seek price information from a competitor.
- Discuss the Company’s current or future plans or pricing with a competitor.
- Share confidential Company information with a competitor.
- Agree with one or more competitors on any decision or course of action.
- Price any product or service below cost.
- Seek or require exclusivity in business arrangements.
- Seek to raise a competitor’s cost of doing business, such as preventing suppliers or contractors from dealing with a competitor, or agreeing to costly contractual requirements on the condition that a competitor meets the same obligations.
- Seek to restrain a competitor from doing business.

ADDITIONAL RESOURCES IN THE INTEGRITY SECTION OF YOUR BUSINESS UNIT’S INTRANET

- Frequently Asked Questions
- Compliance Guide to the Antitrust and Competition Laws
- Confidentiality policy in your business unit’s Employee Handbook
Anti-Corruption Laws

INTRODUCTION
Bribery is illegal, and we prohibit bribery of any kind. Making a payment or providing anything else of value to influence any act or decision of a Government Official or otherwise to gain an improper advantage in any situation is never acceptable and exposes you and the Company to criminal sanctions and/or civil liability pursuant to national, state and local anti-bribery laws, including the U.S. Foreign Corrupt Practices Act, the U.K. Bribery Act and similar anti-corruption laws of other countries. We expressly prohibit improper payments in all business dealings, with governments or in the private sector, in every country in the world.

When interacting with a Government Official, employees must also comply with the Gifts and Business Entertainment Policy and the Interacting with Governments and Political Activities Policy.

WHAT TO KNOW
• Anti-corruption laws prohibit offering, promising, giving or authorizing the offering, promising or giving of anything of value (such as money in any form, gifts, business entertainment, discounts, meals, travel, goods, services, jobs for relatives or charitable contributions), directly or indirectly (e.g., through an agent) to any Government Official, or to an employee of a supplier, contractor or other business partner, in order to influence a business or official decision or obtain or retain an improper advantage.

• The Company and its employees may, under some circumstances, be held responsible for the actions of independent third parties, including agents, intermediaries, consultants, distributors, business partners and other representatives (collectively, “agents”) who interact with a Government Official on behalf of the Company even where employees may not have actual knowledge that the agent has paid others. Therefore, the Company must conduct appropriate due diligence, in accordance with Company procedures, as to any potential agent’s reputation and experience prior to deciding to retain the agent, in order to protect against bribes or other improper payments being given to Government Officials indirectly. Employees must also monitor agent activities and escalate to a Company lawyer any red flags indicating a risk that any improper payment may be made by the agent.

WHAT TO DO
• Do not offer, promise or give, or authorize the offering, promising or giving, of anything of value, directly or indirectly, including a bribe, to any Government Official or any third party in order to influence a business or official decision or obtain or retain an improper business advantage.

• Pursuant to the Gifts and Business Entertainment Policy, obtain the pre-approval of a Senior Attorney before offering any gift, business entertainment or anything else of value, regardless of the amount, to any Government Official.

• Follow Company due diligence, approval and contractual requirements when selecting agents to represent the Company to ensure that they are reputable and qualified, and that they agree to comply with applicable law and policy related to governmental and commercial anti-corruption. You must receive approval from the law department of your business unit before entering into an agreement with an agent who will have contact with a Government Official on behalf of the Company.
• Make sure that records of gifts, business entertainment, gratuities or any other thing of value provided to a Government Official or any third party are fully and accurately maintained and reflect the true nature of the transaction.

• Contact a Company lawyer immediately if anyone offers you an improper payment or other thing of value, or if you are concerned that such a payment or thing of value has been or will be offered to any non-U.S. Government Official or to anyone else in the Company, whether directly or indirectly (e.g., by an agent).

• If you are asked for a gratuity or other payment by a non-U.S. Government Official to expedite a routine, non-discretionary administrative action, you must consult with and obtain prior approval from a Senior Attorney before making any such payments. “Facilitating payments” to expedite a routine administrative action to which a person is otherwise entitled (such as processing visas, permits or other routine government papers, or providing mail pick up or delivery, phone services or power and water supply) may be allowed in certain limited circumstances, but also may be prohibited under local law. If approved, all such facilitating payments must be clearly and accurately recorded in the Company’s financial books and records.

WHAT TO WATCH OUT FOR

• Background information about existing or potential agents that indicates:
  – allegations of improper business practices
  – reputation for bribes
  – family or other relationships that could influence the decision of a Government Official

• Any request for a suspicious payment, such as a commission payment before the finalization of a transaction or announcement of an award decision, for poorly defined, last-minute or unanticipated expenses, or for payments against suspicious invoices.

• Any suggestion to direct Company business through a specific representative or partner due to a “special relationship.”

• Any request to make a payment in cash, or any request to make a payment in a country or to an individual not involved in or related to the transaction.

• Compensation that is disproportionate to the services provided, or not consistent with reasonable business practices.

• Business partners who are unwilling to sign a contract provision agreeing to compliance with applicable anti-corruption laws.

ADDITIONAL RESOURCES IN THE INTEGRITY SECTION OF YOUR BUSINESS UNIT’S INTRANET

• Frequently Asked Questions
• List of Authorized Gift and Business Entertainment Approvers

OTHER APPLICABLE CODE POLICIES

• Conflicts of Interest
• Gifts and Business Entertainment
• Interacting with Governments and Political Activities
• Supplier Relationships
Money Laundering Prevention

INTRODUCTION

People involved in criminal activity (e.g., bribery, narcotics, fraud or terrorism) may try to “launder” the proceeds of their crimes to make it appear that they came from a legitimate source. Money laundering schemes may involve disguising the origin of funds, or transferring funds through third parties (such as a supplier) or through financial institutions. Many countries around the world (including the United States) have laws against money laundering. We are committed to complying with all applicable anti-money laundering laws, conducting business only with reputable partners, and receiving funds only from legitimate sources.

WHAT TO KNOW

• In order to protect the Company against attempts to launder money through our Company, we take reasonable steps, based on the level of risk, to detect and prevent unacceptable and suspicious forms of payment and to perform reasonable due diligence on our suppliers, contractors, customers and business partners.

WHAT TO DO

• Follow your business unit’s due diligence procedures for all suppliers, contractors, customers and business partners, including, when appropriate, checking that they do not appear on any government “watch lists” and ensuring that the financial institutions they use to process transactions meet Company standards.

• Follow your business unit’s guidelines for acceptable forms of payment. Routine customer cash payments for regular services, retail transactions or other traditional cash transactions with individual consumers would not likely require review. Large cash payments in business-to-business transactions may be prohibited or require additional due diligence.

• Consult with the law department or accounting department of your business unit if you encounter suspicious activity or have any questions about appropriate due diligence steps or concerns before proceeding further with the transaction.

WHAT TO WATCH OUT FOR

• A supplier, contractor, customer or business partner who hesitates or refuses to provide requested background information.

• Requests for transactions to go through more than one bank or through a third-party account.

• Requests to make payments to, or receive payments from, any supplier, contractor, customer or business partner that is not the party to the transaction.

• Requests from a supplier, contractor, customer or business partner to conduct transactions with unknown financial institutions or financial institutions outside the country where the transaction is occurring or where the business partner has operations.

• Overpayments with requests for refunds.

• Transactions that occur in regions known for drug trafficking, terrorist or other criminal activities.

• Out-of-the-ordinary transactions for a supplier, contractor, customer or business partner.

• Large cash payments or business-to-business payments made in cash.

ADDITIONAL RESOURCES IN THE INTEGRITY SECTION OF YOUR BUSINESS UNIT’S INTRANET

• Frequently Asked Questions

OTHER APPLICABLE CODE POLICIES

• Supplier Relationships
International Trade Controls

INTRODUCTION

International trade control ("ITC") laws regulate the movement of goods, services and technology across country borders and the conduct of business with certain countries, individuals and entities. ITC laws include customs, trade restrictions (such as economic sanctions) and other import/export regulations, and are often based on national security and foreign policy concerns. In order to do business in today’s global environment, we need to understand and follow applicable ITC laws and regulations, both in the United States and in other locations where we do business.

WHAT TO KNOW

• ITC laws may apply to various aspects of our operations, such as shipping, e-mailing or otherwise transferring products or other items between countries (e.g., DVDs, marketing materials, technical documentation and software), sending equipment to other countries for international filming and production, and newsgathering in countries that are subject to legal embargoes and restrictions.

• A government license may be required before certain regulated items are sent into or out of a particular country or to a foreign national wherever located. For example, certain types of equipment used in filming, production and newsgathering (such as night vision lenses, special cameras, and body armor) are restricted under U.S. trade control laws and cannot be exported without a government-issued license. Employees working abroad or engaging in financial transactions outside the U.S. may confront similar trade controls as well.

• U.S. ITC laws restrict business activities with certain countries, such as Burma (Myanmar), Cuba, Iran, Sudan, Syria and North Korea. Transactions involving sanctioned governments and their controlled entities are of particular concern to U.S. authorities, as are those involving organizations and individuals suspected of supporting terrorism, perpetrating human rights violations, participating in transnational criminal organizations, exploiting conflict minerals, engaging in drug trafficking, or aiding the proliferation of weapons of mass destruction. Consult a Company lawyer for a current list of sanctioned countries, organizations, and individuals.

• U.S. regulations provide limited exemptions for the export of "informational materials" to countries under trade restrictions. These materials may include publications, films and other content. Consult a Company lawyer for further information regarding applicable exemptions or to determine if pre-clearance is required prior to export.

• U.S. restrictions on international trade apply to the Company, our U.S.-incorporated subsidiaries and affiliates, and their respective employees. All Comcast employees, wherever located and regardless of citizenship or nationality, must comply with this policy and with applicable U.S. restrictions on international trade.

• U.S. law prohibits U.S. companies and their affiliates from participating in foreign boycotts that are not supported by the United States (e.g., the Arab League boycott of Israel). Requests to comply with such foreign boycotts must be reported to the U.S. government. Consult a Company lawyer if you believe a proposed transaction may involve a foreign boycott.

Consult a Company lawyer before exporting equipment or other goods, or sending technology to a recipient in another country.
WHAT TO DO

• Follow relevant ITC laws and regulations of all countries in which your business unit operates, as well as your business unit’s ITC procedures as they relate to cross-border shipments, communications and transactions.

• Consult a Company lawyer before exporting equipment or other goods, or sending, transmitting via e-mail, or otherwise transferring technology — including software or technical documentation — to a recipient in another country or to a non-U.S. foreign national located in the U.S.

• Provide complete and accurate information when completing customs forms and other required documents.

• Do not retain a customs broker, shipper or other third party to handle customs matters or other cross-border shipments without performing due diligence and obtaining approvals required by your business unit. These processes should include screening potential service providers against government “watch lists.”

• Do not cooperate with any restrictive trade practice or boycott that is prohibited or penalized under U.S. or other applicable laws. Consult a Company lawyer if you receive a request to comply with a foreign boycott, including a request to supply boycott-related information, such as a request to furnish information about the race, religion, sex, national origin or nationality of U.S. persons working on a Company project in a boycotting country.

• Conduct screening against government “watch lists” when and as required by your business unit. Consult a Company lawyer if any proposed business activity (e.g., licensing content or newsgathering) relates to a sanctioned country, a citizen or representative of a sanctioned country, or an individual or organization possibly subject to government sanctions.

WHAT TO WATCH OUT FOR

• Any shipment, transmission, communication, financial transaction, or other business activity involving an organization or individual affiliated with a sanctioned country, such as Burma (Myanmar), Cuba, Iran, Sudan, Syria or North Korea.

• Business activities involving the international transfer of especially sophisticated equipment, software or technical documentation.

• Documents, including contracts, requests to bid, letters of credit, purchase orders, shipping and customs documents, certificates of origin and questionnaires that include words such as “boycott,” “blacklist,” “whitelist” or similar terms.

• An invoice for imported or exported goods in which the price shown does not reflect its actual value, the description of the goods is incomplete, the goods are improperly classified, or the country of origin is not correctly identified.

• Any payment to an importer or exporter, or any payment benefiting an importer or exporter that is not included in the invoice price or otherwise reported.

ADDITIONAL RESOURCES IN THE INTEGRITY SECTION OF YOUR BUSINESS UNIT’S INTRANET

• Frequently Asked Questions

OTHER APPLICABLE CODE POLICIES

• Supplier Relationships

• Anti-Corruption Laws

• Interacting with Governments and Political Activities

• Complying with Competition Laws