December 2019

Strategic Communications Rules of Practice

LAST MODIFIED FEBRUARY 2021

Note: Links provided are to internal FTI content only.

Purpose of Policy

FTI Consulting's Strategic Communications segment ("Strategic Communications") is committed to conducting its work in an ethical manner. The various practice teams within Strategic Communications all operate at the frontline of complex and high-profile client matters. Because clients often seek our assistance when their business is in crises or under stress (e.g., they face detractors, are under some form of investigation, or have experienced a scandal or other negative event), our work is often subject to a higher level of public scrutiny. It is therefore important that all Strategic Communications personnel conduct their work in a manner that meets industry standards, does not cause embarrassment to Strategic Communications or our clients and, above all, meets our high ethical standards. The following Policy sets out basic rules and standards of behavior designed to achieve these goals, which will apply to all Strategic Communications offices across the globe.

Scope and Relationship to Other Policies and our Ethics and Compliance Infrastructure

This Policy applies to all Strategic Communications employees and contractors. It supplements FTI Consulting's Global Code of Ethics and Business Conduct and is designed to address issues that may have particular relevance to the Strategic Communications business. This Policy is not intended to be exhaustive and will be amended and enhanced over time.

FTI Consulting has an established set of values against which all employees are expected to operate. This Policy requires and assumes our professionals will act in accordance with FTI Consulting's values at all times. A few basic principles from FTI Consulting's policies and practices bear repeating here given their direct application to Strategic Communications work:

- FTI Consulting maintains a Social Media Policy and Acceptable Use Policy that must be followed at all times. These policies may affect personal use of social media channels and company-provided IT equipment.
- Many of the obligations set out in FTI Consulting policies, including those related to maintaining company and client confidentiality, continue to apply even after leaving FTI Consulting.
- Strategic Communications employees will not be required to work on an engagement if they find the nature of the work objectionable. Such a decision will be respected, without penalty or reprisal.
- If a Strategic Communications employee has a concern or would like to report possible improper behavior or violations of our Code of Ethics and Business Conduct, our other policies or applicable law, they should use the FTI Consulting Integrity Helpline, speak with their coach, an SMD in the practice or with Mark McCall.
- Colleagues will undertake required regular trainings and adhere to guidance provided at either the FTI corporate level or within our segment.

Adherence to Laws, Values and Best Practices

All work for Strategic Communications must meet the following requirements:

- We will undertake our work in compliance with applicable laws and regulations. This includes, but is not limited to, laws addressing data privacy (e.g., the European Union's General Data Protection Regulation (GDPR) and similar laws around the globe), insider trading, lobbying, defamation and fair competition.

- We will adhere to, and follow, industry codes of ethics for our relevant regions of operation. In the U.S., this includes the PRSA Code of Ethics, found here and in the UK, the PRCA Professional Charter and Codes of Conduct, found here. In EMEA more broadly, we follow the code of conduct set out by the European Public Affairs Consultancies' Association (EPACA), found here.
- Strategic Communications professionals will remain abreast of industry trends and issues as they relate to ethical standards and best practices.
- Beyond merely complying with legal and professional standards, we will constantly evaluate the reputational impacts of the work we do and ask ourselves "Is this work in the best interest of the reputation of, and consistent with the values, of FTI Consulting?"
- We will conduct our work with the highest level of integrity, and we will always follow the principles of careful communications. We will not include unnecessary commentary in our written communications and, where possible given the nature of the assignment, we will avoid including personal data or information or opinions about third-parties. All of our engagements merit this type of careful approach, and some, including those that involve active litigation, are particularly sensitive.

How We Work

The following rules apply to how we conduct ourselves when performing client work (this includes tasks performed directly by Strategic Communications employees and situations where we manage third-party/freelance activity).

- *Mistruths and Misrepresentation.* We will not misrepresent our identity when performing work assignments nor will we instruct others to do so. We will not impersonate other people online, employ social media profiles designed to impersonate another person or group, or pseudonyms or other methods defined as 'astroturfing' in connection with our work. The content we develop will never make claims designed to appear as fact, without being able to provide evidence to back them up.
- *Website Development/Registration and Launch. A*ll websites developed by Strategic Communications will have a clear sponsor (considered as a named client or body to which they belong) that is transparent to the visitor. The sponsor should not be an FTI Consulting employee or contractor. Strategic Communications will not take ownership of any third-party privacy policies or terms of use for websites -- the privacy policy must be owned by the company, coalition, etc. sponsoring the site.
- *Social media accounts.* All social media accounts created or managed by Strategic Communications will have a clear sponsor (e.g. client entity) that is transparent to the visitor. Our use of these platforms must adhere to the site's policies.
- *Work for Coalitions, Committees or Organizations.* For entities that claim to be a coalition, committee or organization, we will only create public-facing content (e.g., creative, digital, advertising campaigns) if the entity is (a) a legally registered organization in the jurisdiction in which it operates, or (b) an organization or coalition that consists of two or more participating members.
- *Paid Advertising/Social Media Marketing.* Wherever required by advertising or social media platforms, paid advertising campaigns will have a clear sponsor and Strategic Communications will follow relevant transparency guidelines.

- *Use of Data Providers & Advertising Vendors.* We will only work with data/digital/advertising vendors and partners that follow information security best practices, post clear privacy policies, post opt-out guidelines, are members of or follow industry member best practice bodies (such as the Network Advertising Initiative or the Digital Advertising Alliance) with respect to data collection, data security, data storage, and data use.
- *Content.* We will not produce content containing images or text designed to exclude, "redline" (engage in marketing designed to exclude racial or ethnic groups from financial services products), inflame, incite, or confuse individuals, communities or groups of common interest.
- *Wikipedia.* When acting on behalf of Strategic Communications, we will not under any circumstances edit Wikipedia directly. The platform has clear guidance on best practice (found here) that relates to clients wishing to see content changed or updated.
- *Syndicated Advertising (e.g., Outbrain, Taboola).* Strategic Communications may undertake syndicated advertising activity in support of client engagements, but in doing so we will only point to existing credible and legitimate news sites or content already in the public domain, and activity will contain appropriate disclosure and sponsorship when required by the platform.
- *Targeting (e.g. via Paid Content).* When deploying targeting techniques in support of client engagements, we will exercise caution around protected characteristics (e.g. gender, ethnicity), and will act in compliance with applicable law (e.g. fair housing guidelines). Moreover, no audience fewer than 50 individuals should be targeted via digital means.
- *Community Management*. We will not manage client communities via our personal social media accounts. At the client's request, we can develop content and post via client's accounts as representatives.
- *Grassroots campaigns.* We will seek only to represent grassroots campaigns in support of when a genuine group or individuals are, or can be, motivated to speak or act on their point of view – and that point of view itself must not be in contravention of FTI's policies, i.e. climate denial, de-stabilizing communities.
- *Miscellaneous Search Engine Optimization Black Hat Tactics.* We will not engage in any other "black hat" tactics such as key word stuffing, cloaking, spam comments, and invisible text. The use of tools, such as botnets or click farms, is prohibited.

Collection, Use and Storage of Data

FTI Consulting maintains several policies and procedures related to the proper processing and protection of data. The collection, use and storage of personal data, in particular, is subject to a number of legal requirements and generates heightened risks. In the US, regulated data tends to be defined as Personally Identifiable Information (PII) and consists of first name, last name, address, social security number, personal health information, personal financial information, or information that could be linked directly or indirectly with a particular consumer or household. In the EU, Brazil, and elsewhere, however, the definition of Personal Data is broader and can include simply a person's name.

The processing or storing of significant amounts of PII or Personal Data should only be conducted if specified by the client in the statement of work. If you will be collecting, processing, transferring, analyzing or storing PII or Personal Data in the course of your work, you should familiarize yourself with FTI Consulting's applicable policies. Strategic Communications employees and contractors should also comply with the following rules:

- If you do not need Personal Data or PII to complete your work, do not collect or store it. Politely advise clients not to send it to you. In the alternative, some tasks can be completed using "de-identified" information – that is information that has the personal elements stripped out so that the individual cannot be identified. Where possible, the de-identification of the data should be undertaken by the client or other supplier of the data so that Strategic Communications does not come into possession of the Personal Data/PII.

- Only those employees/contractors who have a need to have access to Personal Data/PII should receive such data or be given access to it.

- For those matters that will involve the use of some Personal Data or PII, consider using a secure transfer method to transfer the data to and from Strategic Communications. For large data sets this will generally involve using a secure File Transfer Protocol and ITG can assist with this process. Large data sets should not be communicated via e-mail. In other cases, involving smaller amounts of information, it may be appropriate to use Voltage, FTI Consulting's e-mail encryption tool.

- Certain laws limit the transfer of Personal Data across jurisdictions. If you are not sure whether a cross-border transfer is permissible, contact FTI Consulting's Chief Risk & Compliance Officer or the EU Data Protection Officer. Notably, transfers of data between FTI Consulting offices is generally permissible.

- While some documents must be retained for legal reasons or because they remain useful, over-retention of data creates risk. Accordingly, we are encouraged to agree with clients on specific record retention/destruction periods and include those terms in letters of engagement. We must then take action with respect to destruction/return of data at the appropriate time.

- Any Strategic Communications engagements that will involve the collection, use or storage of Protected Health Information (PHI) (i.e., information related to an individual's health, healthcare, health related billings, etc.) should be brought to the attention of FTI Consulting's Chief Risk & Compliance Officer immediately.

- Where possible, avoid including in written work product the names, personal information, or opinions about specific individuals who are not public figures, unless this information is necessary to properly complete the assigned task.

Rules Applicable to Digital Advisory Practice Teams

The following rules apply specifically to Strategic Communications Digital Advisory Practice teams:

- In general, given differences in privacy law and data usage across national jurisdictions, data should be stored, processed, analyzed and reported in the same jurisdiction of the client brief. For "matters conducted under privilege or at the direction of counsel," this must be followed.

- Similarly, we will not produce content containing images or text meant to feature private individuals who are not public figures.

Where to Get Help

General questions about this Policy should be directed to Mark McCall or the applicable Regional Strategic Communications Head. Questions related to the Digital Practice should be directed to Brent McGoldrick or Ant Moore.