



# **CODE OF CONDUCT**

## INTRODUCTION

Launching our new brand identity was a major milestone for our business. I am proud of what our brand stands for – a commitment to helping customers accelerate the pace of innovation. Our business has always been associated with the world's leading innovators. These organizations place great trust in us; they rely on our content and services for mission critical decisions.

It is imperative that we live up to our clients' expectations and earn that trust. Each one of us has the opportunity – and responsibility – to ensure that our customers associate our brand with excellence, integrity and great customer service. Following the guidelines and policies created by our Compliance team will enable us to build our reputation amongst our customers, partners and fellow colleagues, which in turn is a foundation for our future success.

Steady growth and strong financial performance go hand in hand with ethics and compliance. By holding ourselves to the highest ethical standards, we will create the type of workplace environment that attracts the best people, and we will establish Clarivate Analytics as the type of company that everyone wants to do business with.

I have every confidence that our employees want to do the right thing. This Code of Conduct ensures that we all have a common understanding of what the right thing is. Please take time to read our Code and don't hesitate to ask if you have any questions.

Thank you for your commitment.

Jay Nadler  
Chief Executive Officer

## INTRODUCTION

**Who this applies to** The Code applies to all officers, directors and employees of Clarivate Analytics. Outside consultants, contractors and temporary employees are also required to abide by the policies, principles and values set out in this Code.

**What you need to do** You should read this Code and any supplemental policies posted on [our intranet page](#) and complete any related online training courses. Employees engaging third parties acting on behalf of Clarivate Analytics should also ensure that such third parties are aware of their obligations under this Code.

**Questions** If you have any questions about this Code, please contact [compliance@clarivate.com](mailto:compliance@clarivate.com). Alternatively, you can also call our Compliance team at 203-539-8706.

**Hotline** If you believe there has been a violation of this Code, you should report it immediately via the Hotline using the toll-free number for your country or through the online reporting system accessible through our intranet. Please refer to [our intranet page](#) for further details on reporting any possible Code violations, including how to do so anonymously where permissible and for further details on our policy of non-retaliation and how investigations will be handled.

**Acknowledgement** You are required to acknowledge on an annual basis that you have read the then-current version of this Code, and to take mandatory training courses associated with the Code. Please note that you will be expected to comply with this Code regardless of whether you acknowledge receipt, and that Clarivate Analytics reserves the right to interpret this Code and related policies at its sole discretion. This Code is not exhaustive and no statement of principles and procedures can offer a complete guide to cover all possible situations. Clarivate employees are expected to observe both the spirit and the letter of this Code, and to consult this Code or an appropriate representative of Clarivate when faced with an ethical issue. This Code is not intended to alter your terms of employment.

### Contact details

For general questions regarding the Code, please visit [our intranet page](#) or contact our Compliance team at [compliance@clarivate.com](mailto:compliance@clarivate.com).

The Code also references other Clarivate teams that should be consulted for various matters. For your convenience, here are their contact details:

HR: [Email your HR contact as listed on your profile on the Lens](#)

Legal: [legal@clarivate.com](mailto:legal@clarivate.com)

Sourcing: [clarivate.sourcing@clarivate.com](mailto:clarivate.sourcing@clarivate.com)

Contract Administration: [contract.admin@clarivate.com](mailto:contract.admin@clarivate.com)

## PROPER USE OF ASSETS

### Clarivate assets are to be used for your job

**Use of company assets** You should use Clarivate assets only for authorized business purposes, and you should only access systems and information that you are authorized to access. Clarivate assets should be secured. Clarivate assets must never be used for illegal activities.

We are realistic about our work/life habits and permit limited and occasional personal use of our e-mail, messaging, internet and phones provided that such use is not excessive, does not interfere with your work responsibilities and does not violate this Code. You should not assume or expect privacy when using communications and technology infrastructure owned or supplied by Clarivate. Where permitted by applicable law, we reserve the right to monitor and record your use of communications and technology infrastructure owned or supplied by Clarivate.

**Use of computer systems** Computers and communication devices are provided to help us work more productively, but keep in mind the following:

- **Use Good Judgment** If Clarivate becomes involved in litigation or an investigation, your communications may have to be turned over to third parties including regulators and the court. Avoid careless, exaggerated or inaccurate statements that could be misunderstood or used against you or us in a legal proceeding. **Before you hit “send,” think and re-read.**
- **Inappropriate Content** Don't access, send or download inappropriate content that could be offensive, insulting, derogatory or harassing to another person, such as sexually-explicit messages, jokes or ethnic or racial slurs.
- **Confidential Information** Don't forward internal communications or send confidential materials outside of Clarivate unless you are explicitly authorized to do so.
- **Collaboration Tools** Use of collaboration tools on your work computer, such as instant messaging, is only permitted if you're using an approved tool provided by Clarivate.
- **Passwords** Manage and keep confidential your computer user IDs, passwords and authentication devices;
- **IT Security** Follow guidance from our IT Security team regarding security (e.g., exercise caution when opening files attached to e-mail, be careful of people outside of Clarivate asking for financial, customer or corporate information through e-mail or phone scams). **Please report any suspected computer security exposures or incidents to our IT department immediately.**
- **Personal Devices** In some instances, you may be allowed to use personal smartphones or other devices for business purposes. If you have approval from your manager to use a personally-owned device for business, your phone will be subject to the same security and data management practices as a company-owned device.

**Returning assets** When you leave the company or are requested to do so, you must stop using and return any and all Clarivate assets in your possession.

If you become aware of loss, theft, misuse, damage or waste of our assets, or you have any questions about your proper use of them, you should contact our Compliance team or report it through the Hotline.

# CONFIDENTIALITY, INTELLECTUAL PROPERTY AND DATA PRIVACY

## You must protect our confidential information, and not misuse any personal data or intellectual property belonging to third parties

**Safeguarding confidential information** You should not share confidential information belonging to Clarivate, or our customers, vendors or partners with anyone, including colleagues, unless there is a legitimate “need-to-know” and you are authorized to do so. Improper disclosure of confidential information could put us at a competitive disadvantage, or could hurt or embarrass us or other stakeholders.

Your obligation to safeguard our confidential information applies to you even after you leave Clarivate for as long as the information remains confidential.

**Data privacy** Many countries have data protection and privacy laws that govern the collection, use, retention and transfer of personal information. You should consult with our Legal team before making any new or different uses of information about individuals, especially if it involves sensitive information, such as credit card numbers or medical or healthcare related information.

**Intellectual property** As a global leader in the provision of IP solutions, it is essential that we both protect our own intellectual property and respect the intellectual property rights of others. You should get written permission before making use of a third party’s copyright-protected materials, patents, brands or other intellectual property. If you want to use intellectual property that belongs to someone else, we may need to obtain a license or purchase outright ownership of the property. If we already have a license from the third party owner, you should check that your intended use is permitted before making such use or consult with our Legal team.

Downloading, duplicating or redistributing copyrighted material, including music, movies, images or software, may violate the law in many countries and can result in disciplinary or legal action. Do not engage in these activities unless you are legally permitted to do so.

Any intellectual property generated in the course of your employment or using Clarivate assets belongs to Clarivate.

## MEDIA AND PUBLIC INQUIRIES

### Don't speak on behalf of Clarivate unless you are authorised to do so

**External requests for information** Only an authorized spokesperson may engage in discussions about Clarivate with third parties. No other individual is authorized to speak on behalf of the company. Anyone contacted by a third party must refer the third party to a member of the Communications Team.

**Public speaking and publications** Before publishing, making a speech or giving an interview in your capacity as a Clarivate employee – or if a publication, speech or interview might in any way be connected to your position at Clarivate – you should obtain approval from our Communications Team.

**Social media** Exercise good judgment when posting or sharing information relating to Clarivate. Do not disclose any confidential or sensitive information. Avoid using statements, photos, video or audio that could be construed as malicious, obscene or threatening, or that disparages our business, co-workers, customers or business partners. Be transparent about your relationship to Clarivate if you are writing about our industry, or Clarivate products or services.

# HEALTH AND SAFETY, SECURITY AND ENVIRONMENT

## We are committed to ensuring the health and safety of our employees

We endeavor to provide a healthy and safe work environment for our employees as well as be a good corporate citizen in the communities where we do business. In this regard, you must:

- Conduct our operations in a manner that complies applicable occupational health and safety laws, environmental laws, and the public policies that they represent.
- Follow policies and guidelines, and take training to ensure safety, pollution prevention, resource efficiency and responsible sourcing.

**Drugs and alcohol** Clarivate will not tolerate the abuse/misuse of alcohol and illegal and prescription drugs, while conducting Clarivate business on or off our premises.

Employees who violate this policy will be subject to disciplinary action. As involvement with certain drugs is illegal, violations of this policy could also subject you to arrest and prosecution by law enforcement agencies.

**Workplace violence and hostility** Clarivate has zero tolerance for acts or threats of violence, intimidation and hostility towards another employee, a customer or a member of the public. If you feel that you or another person is being threatened or subjected to violence, or if you encounter suspicious activity, you must make this known immediately to the Compliance team or HR.

No person may possess a weapon of any kind, or other dangerous or hazardous device or substance on Clarivate premises, at Clarivate-sponsored functions or otherwise on company business.

In the event of a life-threatening emergency, immediately call local police or an ambulance and then line-management. Domestic and personal issues that may apply to or affect the workplace (i.e., orders of protection, restraining orders) should be reported to the Compliance team or HR.

# FAIR COMPETITION, ANTITRUST AND COMPETITIVE INTELLIGENCE

## We comply with applicable laws and compete fairly

[Interacting with competitors](#) We believe in fair and open competition. You should always comply with applicable antitrust and competition laws wherever we do business. It is against our policy to:

- fix prices (formally or informally) with competitors or non-related parties, whether directly or indirectly
- share pricing or other commercially sensitive information with competitors
- allocate customers, territories or product markets between Clarivate and our competitors
- unfairly disparage or misrepresent competitors or their products
- induce another party to breach a contract in order to enter into a transaction with Clarivate
- deal unfairly with customers or suppliers

If you are involved in marketing, sales or sourcing, or regularly in contact with our competitors, make sure you understand the applicable antitrust laws and internal policies.

[Gathering competitive intelligence](#) Legitimate intelligence gathering is an important part of doing business and understanding our market. However, you should not obtain information about our competitors through illegal practices. For instance, you should not misrepresent your identity or relationship with our business to gain access to a competitor's product. If you have been given access to a competitor's product, you must comply with any relevant terms and conditions when making use of such product. More details about appropriate competitive intelligence gathering can be found on the Compliance Intranet page.

Any questions about antitrust or competitive intelligence should be directed to the Compliance team.

## GIVING OR RECEIVING PAYMENTS, BENEFITS OR GIFTS

### Use your best judgment in giving and receiving gifts; don't directly or indirectly make unauthorised payments to company or government representatives

Although giving and receiving gifts, meals, services or entertainment could be considered a customary business practice, they can also potentially affect objectivity and judgment, and may breach anti-bribery and corruption laws and regulations in extreme cases.

Acceptable gifts, meals, services and entertainment Gifts, meals, services and entertainment are acceptable and comply with this Code if they:

- are relatively infrequent and not excessive in value
- comply with applicable laws and regulations, and are consistent with customary business practices or courtesies
- will not place the recipient under any obligation to the person who gave the gift
- do not include cash or cash equivalents
- would not embarrass Clarivate, the person receiving the gift, or the person giving the gift, if publicly disclosed
- comply with any additional guidelines posted on the Compliance Intranet page

Because it's not possible to define "not excessive" in a way that covers all possible cases, we rely on your good faith judgment in these situations. If you have any doubts, you should consult with the Compliance team.

In all cases, you should keep in mind that our customers often have their own policies and guidelines, and you should not offer gifts, meals, services or entertainment which you know or suspect would violate those policies or guidelines.

Bribes, improper payments and gifts Our policies, as well as the laws and regulations of most countries where we do business, forbid you from making payments designed to improperly influence the decisions of an individual, company or governmental official. Similarly, you cannot solicit, encourage or actually receive any payment, gift or favour that could influence your decision or cloud your independent judgment. While what's viewed as a bribe in one country may be acceptable in another, you're expected to comply with this Code.

Facilitation payments "Facilitation payments" (small payments made to government officials or affiliated persons to secure routine actions such as processing visas or other government papers, obtaining non-discretionary permits, providing phone or power service, and similar activities) are prohibited under Clarivate policy even if local laws permit it. If you are faced with a request for such a payment, you should refuse.

## CONTRACTING FOR CLARIVATE ANALYTICS

### Do not sign a contract on behalf of Clarivate unless you are authorised

**Commercial contracting** Clarivate enters into many contracts that govern our business relationships, so we have policies and procedures in place to ensure that any contract entered into on behalf of Clarivate has the appropriate level of review and approval.

Before you enter into any contracts on behalf of Clarivate, you should have proper authorization. All third party vendor and supplier agreements should be negotiated by our Sourcing team. All customer agreements, partner agreements and other non-vendor commercial agreements should be negotiated by our Contract Administration team or Legal team. Do not sign a contract unless it has gone through the appropriate channels.

You may not enter into “side letters” with customers, vendors or suppliers. Side letters are undisclosed and unapproved documents, emails or verbal assurances that allow customers, vendors or suppliers to deviate from our standard contract terms. All terms relevant to our dealings with these parties should be contained in the formal contract.

**Government contracting** In addition to the rules and procedures outlined above, if you engage with governments, it is vitally important that you follow the rules which govern public procurement, comply with applicable laws, policies and standards, and consult with our Legal team whenever there is a question about any of the above.

## POLITICAL AND CHARITABLE CONDUCT AND CONTRIBUTIONS

### **Political contributions made on behalf of Clarivate are not permitted. Charitable contributions made on behalf of Clarivate always require approval**

**Political conduct and contributions** Clarivate does not give support – directly or indirectly – to any political party, candidate, group or religion, nor does it take sides in national or international conflicts or disputes. In keeping with this policy, you should make it clear that you are acting or speaking on your own behalf, and not on behalf of Clarivate, when you are involved in political activities or expressing your opinion on political or public issues. You must not identify the name of Clarivate (or any of our brands) with any political party or group or any one side in such conflicts or disputes.

You must notify our Compliance team if you plan to campaign for, or serve in, public office, and avoid conflicts of interest by excusing yourself from any political matters involving Clarivate if you do so.

**Charitable conduct and contributions** We encourage you to contribute your personal time and resources to charities and non-profit organizations. However, if you are affiliated with a charity or non-profit organization that seeks to do business with, or receive donations, assets or services from Clarivate, you should disclose this to our Compliance team and obtain appropriate approval.

## CONFLICTS OF INTEREST

### Avoid actual and potential conflicts of interest in performing your duties for Clarivate and do not advance personal interests at the expense of Clarivate

We expect that you will act in the best interests of Clarivate and avoid conflicts of interest by making reasoned and impartial decisions. A conflict of interest may arise whenever a personal interest interferes with - or even appears to interfere with - the interests of Clarivate. A conflict of interest can also arise when you take a position or have an interest that makes it difficult for you to perform your work objectively and effectively.

**Identify and pre-clear conflicts** It is your responsibility to identify potential conflicts as soon as they arise and to contact our Compliance team if you are unsure whether a relationship or transaction poses a conflict before engaging in the conduct. Full disclosure allows us to resolve unclear situations. Some conflicts are permissible if they are disclosed and approved by the General Counsel. We rely on you to exercise sound judgment and to seek advice when appropriate.

**Examples of conflicts** The following are examples of conflicts of interest that could arise, and are prohibited unless they have been pre-cleared or resolved in advance:

- **Improper Benefits** You or someone in a close relationship with you receives improper personal benefits (such as cash, gifts, entertainment, services, discounts, etc.) as a result of your position at Clarivate.
- **Interference** Your work as an officer, director, employee or consultant to another company interferes with your ability to do your job at Clarivate, or the other company competes with Clarivate.
- **Other opportunities** You take for yourself a business opportunity which you discovered through your position at Clarivate without first offering it to Clarivate.
- **Personal Gain** You use Clarivate property or information, or your position at Clarivate for personal gain.
- **Relationship** Someone in a close relationship with you is directly reporting to you, or you have the ability to supervise, review or influence the job evaluation, hiring, pay or benefits of someone in a close relationship with you who also works at Clarivate.
- **Improper Influence** You allow any investments held by you or someone in a close relationship with you to influence you in your work for Clarivate.

In addition, if someone in a close relationship with you works for a competitor, customer or supplier of Clarivate, both of you should take special care to comply with the duties that each of you owe to your employer.

**Other positions** Working outside of Clarivate or serving as a director of another organization may create a conflict of interest, whether or not the position is compensated.

Before agreeing to work outside of Clarivate or joining the board of another organization, you should assess whether such action could result in a potential conflict of interest. If there is a potential for conflict, you must receive written approval from the General Counsel prior to accepting the job or appointment. In addition, you may not serve as a director of a publicly traded company unless you've received approval from the General Counsel.

If you hold a position with another organization and if you speak publicly for such organization, you should ensure that you are seen as speaking on behalf of that organization, and not on behalf of Clarivate.

If you're permitted to work outside of Clarivate or join another organization's board, you may not divulge any confidential or strategic information about our business, and you must not vote on any board issues that are related to dealings with Clarivate.

Any permitted outside work/positions should not be done on Clarivate time or using Clarivate equipment, property, information or supplies. Your outside work/position should not interfere with or prevent you from devoting the time and effort needed to fulfill your primary duties and obligations to Clarivate.

## ACCOUNTING, AUDITING OR DISCLOSURE CONCERNS AND FRAUD REPORTING

### Promptly report any accounting, auditing or disclosure concerns that you may have. Keep accurate and reliable records

We have a responsibility to keep accurate financial records in line with our company's accounting standards and policies and in compliance with applicable laws, and to submit good faith questions and concerns regarding questionable accounting, auditing or disclosure practices.

**Examples of accounting and auditing issues to report** You should promptly report any concerns relating to accounting, internal controls or auditing matters, which may include actions involving:

- fraud or deliberate errors in the preparation, maintenance, review or audit of any financial statement or financial record of Clarivate
- deficiencies in, or noncompliance with, the Clarivate internal accounting controls
- misrepresentation or false statements to or by a senior officer or accountant regarding a matter contained in the financial records, financial reports or audit reports of Clarivate
- deviations from full and fair reporting of the Clarivate financial condition

**Examples of fraud to report** You should also report any other types of fraudulent or dishonest activity that you become aware of, or have good faith suspicions about. Examples include:

- questionable transactions with customers or business partners not in accordance with Clarivate policies
- forgeries or other alterations of documents
- billings made higher or lower than normal prices for products or services at a customer's or vendor's request
- payments made for any reason other than as described in the relevant contract, or payments made to an individual account rather than the account of a company with which we are doing business
- payments made through intermediaries that deviate from ordinary business transactions
- embezzlement, theft or misappropriation of Clarivate assets or customer assets that we have been entrusted with

**Proper financial and accounting recordkeeping** Our financial and accounting records are used to produce reports for Clarivate management, directors, governmental and regulatory authorities and others. We have appropriate control systems in place to ensure these records are complete and accurate. You can help us by doing the following:

- All of your books, records and accounts – including time sheets, sales records, invoices, bills and expense reports – must be complete, accurate and reliable.
- Unrecorded, undisclosed or "off-the-books" funds or assets should not be kept for any purpose.
- Never falsify any document or distort the facts relating to a particular transaction.
- Transactions should be recorded in a timely manner and supported by appropriate documentation.
- You should not incur or pay the cost of anything using Clarivate funds if the incurrence or payment is not authorized under company policy.

You should report fraudulent activities by current or former employees, officers, directors, contractors or third parties with which we do business to the Compliance team.

## **EQUAL EMPLOYMENT OPPORTUNITIES AND HARASSMENT**

### **We provide a workplace that offers equal employment opportunities and is free from harassment and inappropriate conduct**

We are committed to providing equal employment opportunities for all persons with respect to hiring, compensation, promotion, training and other terms, conditions and privileges of employment. We comply with applicable laws and regulations governing non-discrimination in all locations. All employees should treat each other with courtesy, dignity and respect. We have zero tolerance for harassment or other inappropriate conduct, whether committed by an employee, supervisor, customer, vendor or any other person on our premises or conducting business on our behalf.

Any form of discrimination or harassment is a violation of this policy and will be treated as a disciplinary matter. You should contact HR or the Compliance team regarding any discrimination or harassment issues.

## RECORDS MANAGEMENT

### **Comply with records management policies applicable to you and don't destroy or falsify documents or e-mails if you learn of litigation or investigations**

Our information and records are valuable corporate assets that must be carefully maintained. We must comply with legal and regulatory requirements that relate to document and record retention and disposal. You should manage our records and information in a manner that ensures:

- consistently organized filing, storage and retrieval of recorded information
- record maintenance in whatever media satisfies legal, fiscal, regulatory and operational requirements
- protection of records (including backups)
- needed documentation in the event of litigation
- proper and timely disposal of records no longer of value, both in paper and electronic format

If you are informed about pending or threatened litigation or a governmental investigation, you may not destroy any records (including e-mails) unless you have been authorized to do so by the Legal team. It may be a criminal offense to destroy or falsify documents or e-mails that are subject to a subpoena or other legal process. Any employee who fails to comply with this policy, as well as applicable laws and regulations, is subject to disciplinary action, up to, and including, termination and may also face criminal or civil prosecution, with possible fines and prison terms.

You should contact the Legal team if you have a question about records retention.

# EMBARGOES, SANCTIONS AND EXPORT CONTROLS

## Comply with applicable sanctions and export control laws

As a global business, we need to ensure that we don't breach any of the laws, rules or regulations that apply to trade embargoes, sanctions and export controls.

**Sanctions** Sanctions restrict our ability to do business with particular countries, entities or individuals.

There are wide-ranging sanctions or "embargoes" that apply to different countries or regions. These sanctions are politically motivated and may change over time – you can find a current list of sanctioned markets on the Compliance Intranet page.

Additionally, governments and inter-governmental bodies (e.g., the United Nations) may issue lists of entities and individuals that are sanctioned. We systematically screen our prospects and customers against these lists.

You must not do business with any person or entity that is a sanctioned party or in a sanctioned market, or owned, controlled or acting on behalf of a sanctioned party or a party in a sanctioned market. One of the key ways that you can support our sanctions compliance efforts is to **know your clients and business partners** - who owns or controls them, what their reputation is, what business they do and where they do it.

To find out more about rules on doing business with sanctioned countries and parties, please visit the Compliance Intranet page.

**Export controls** Export control imposes restrictions on what you can export, from where, to where, to whom and for what purpose. You must follow any processes and guidelines implemented by our business for compliance with export controls.

If you have any questions about sanctions or export controls, please contact our Compliance team.