



Ethics & Business Behavior

We think ...

“Even with the best policies, protocols and systems in place, a culture of integrity is ultimately about behaviors – therefore we link up closely with Human Resources when delivering our program of ethics training.”

Lauren Aste, Chief Legal Officer & General Counsel



We act with ethics and integrity



At CWT, we pride ourselves on our reputation as a world-class company operating with the highest standards of ethical conduct. We have built a culture that earns trust and protects the relationships we have with our stakeholders, including our clients and suppliers, by acting in an open and honest way at all times.

Through our internal ethics and compliance program, as well as external alignment to internationally-recognized standards, we seek to conduct business in the right way. Business ethics and compliance, responsible purchasing as well as data privacy and information security, represent key priorities of our program. Our process starts with implementing ethical business conduct through a robust governance structure – supported by dedicated policies and hands-on training.

Ethics and Compliance governance

Ethics and Compliance is overseen at the highest levels of the company. Our Compliance Committee includes our President and CEO and other members of the Executive Leadership Team. Supporting the Committee is a team of global lawyers and support staff who oversee implementation, and report progress to the Vice President of Global Compliance.

The Global Compliance team is responsible for the deployment and updating of various policies and procedures and also responsible for promoting and ensuring compliance with our Code of Business Ethics and Conduct (the Code). The Code outlines the ethical standards expected of our teams and contractors everywhere we do business. We promote our standards through annual awareness training for all our staff, topics include anti-bribery, anti-corruption, non-retaliation, gifts and entertainment, Human Rights and ethical behavior. We also run a dedicated sustainability assessments for our key non-trade* suppliers.

Code of Business Ethics and Conduct

Our Code of Business Ethics and Conduct helps to inform our day-to-day decision-making. It is the foundation of all CWT policies and encourages discussions on Ethics and Compliance among our people to empower us to handle any ethical dilemmas we may encounter. Fundamentally, it helps us maintain the trust we have built with our employees, clients and suppliers.

The Code applies to every individual and contractor who works for CWT or represents us worldwide. It outlines how we comply with applicable laws, treaties and regulations relevant to business conduct. It also includes guidance around workplace conduct and reinforces our values clearly and comprehensively.

In 2017, we carried out a detailed review of the Code to reflect the latest industry best practices and legislative trends. The process involved refreshing and updating the content from key internal groups (including Human Resources, Internal Audit, Information Security, Responsible Business, Legal and Compliance and Communications) as a first step. Beyond this, we also worked to simplify the language of the Code to make it more engaging and readable for our stakeholders. Our fully revised Code of Business Ethics and Conduct was launched on January 1, 2018, is in the public domain and can be downloaded [here](#).

* Non-trade suppliers are those that are not directly related to CWT's core businesses. Examples of non-trade suppliers include IT and services companies.



Compliance Policy Manual

With the aim of updating, clarifying and summarizing our compliance standards, we consolidated our numerous compliance policies into a single, easy-to-use Compliance Policy Manual in 2017.

The Compliance Policy Manual will help reduce the complexity of our processes by clearly articulating what is expected of our employees. It will also help us in our mission to empower individuals to make smart, informed decisions easily and to maintain accountability, all while supporting our Digital Difference strategy in a way that meets Ethical and Compliance standards.

Each of our employees, contractors and any other individual working for and representing CWT is expected to follow the policies contained within the Manual. The Manual was launched on January 1, 2018 and contains the following policies*:

1. Protection of Personal Data

We understand the importance of holding the personal information provided by our travelers, employees, travel managers, clients and prospective clients carefully and securely. This policy explains how any employee or other individual representing CWT who processes personal information must protect and safeguard it in line with our data privacy policy.

2. International Trade Compliance Policy

We operate in numerous countries around the world and must comply with all applicable international trade laws such as trade embargos, sanction screening and product export controls. Our International Trade Compliance Policy sets out our processes and controls around how we deliver this.

3. Anti-Corruption

We do not allow payment of bribes or the facilitation of corrupt behavior under any circumstances. Unfair business practices, such as kickbacks, facilitation payments, and use of third parties to channel bribes are also strictly prohibited. Our Anti-Corruption Policy outlines our zero-tolerance stance on bribery and corruption, and our adherence to legislation such as the US Foreign Corrupt Practice Act and the UK Bribery Act to ensure we meet global requirements.

4. Competitive Information Policy

Many of the countries where we do business have competition, or antitrust laws. These laws aim to ensure fair competition, which allows our clients and the public to buy goods and services at fair market prices. Competition laws prohibit agreements, practices and conduct which have a damaging effect on competition, such as improper agreements between competitors or abuse of market power.

5. Conflicts of Interest Policy (including gifts and entertainment)

Our formal Conflict of Interest Policy seeks to make all employees aware of CWT's rules about situations that could create a potential, real or perceived conflict between CWT's interest and CWT employees. Anyone acting on CWT's behalf must be free from conflicts of interest and/or appearance of conflicts of interest that could adversely influence their judgment, objectivity or loyalty to CWT.

6. Anti-money laundering

The laws and regulations of many countries where CWT operates prohibit money laundering in any form. Under no circumstances may any CWT personnel or agent (independent sales representatives, distributors, consultants or agents) participate in or allow the commencement of any transaction involving CWT that involves any funds that the employee knows or suspects were illegally obtained.

Additional existing key policies and processes include:

– Fraud

Our formal internal fraud procedure seeks to outline the procedures to follow when a case of fraud has been identified or suspected and to establish the process to report, investigate, manage and share information about fraud with key CWT stakeholders and shareholders.

– Fair marketing

We compete for client commitments, but never by sacrificing honesty and fairness. This is especially vital in all of our sales, marketing and advertising pursuits. All advertising and marketing claims must be substantiated and must include all information and disclosures necessary to make them accurate.

The CWT Compliance Team has in place an appropriate due diligence process allowing the business to be aligned with the expectations set out under this Manual. There is also a comprehensive compliance risk assessment process related to all compliance policies.

* The wording used to describe these policies has been taken from the Compliance Policy Manual.



Training on the Code

Our Compliance program is designed to detect and prevent violations of the law, respond to potential issues and proactively deter problematic behaviors and actions.

Preventive measures implemented include mandatory training and awareness programs driven by the Global Compliance team. Each year, we run mandatory training on the Code and its policies, both for new recruits and current staff – we achieved a 99% completion rate in 2017. We also run Responsible Purchasing training for those working with our suppliers (see [page 20](#)).

Employees can access training sessions wherever and whenever as part of our online Learning Management System. Our Compliance team has access to metrics on how employees are performing on each compliance topic, and benchmarking data that shows how we are performing as a business against our peers. We use this insight to determine if additional training is required.

We live ...

... to uphold ethical behavior through the Ethics Helpline

Our policies and tools ensure that any instances of non-compliance are dealt with discreetly and fairly. This includes our confidential Ethics Helpline.

Available 24/7, our confidential Ethics Helpline connects callers (employees, clients and other third parties) to an experienced, independent operator who speaks their language. Concerns are logged by phone and/or through an online tool where they are addressed promptly. We also make use of a third-party provider to verify adherence to local privacy laws and reporting requirements.

The Compliance team reviews all cases and assigns an internal investigator based on the nature of the issue. In 2017, the Compliance team created an investigation manual, identified and trained a group of internal investigators to further build skills internally and to standardize the conduct of investigations. CWT treats the reported information in a confidential manner to the extent reasonably possible and allowed by law and has a strict non-retaliation policy.

The Compliance team develops metrics on cases submitted through the Ethics Helpline, such as the nature of the concern, what countries cases are reported in, and tracks how the cases are resolved. This information is then reviewed quarterly with the Compliance Committee, which oversees Compliance at CWT.

Ethics Helpline information is posted on our corporate website and is made accessible not only for our employees, but also for our clients, travelers, third-party vendors and partners to use as well.

 [More information can be found here.](#)

Fighting bribery and corruption

As stated in our Code of Business Ethics and Conduct, we abide by all applicable laws, treaties, and regulations that forbid bribery and corruption. As part of our commitment to conducting our business the right way, we maintain a zero-tolerance stance on bribery and corruption. This means that we will never bribe or receive bribes from any public or private third party, either directly or indirectly (such as through an agent) – even if this means we will lose business as a result.

Our Corporate Audit function monitors existing and emerging risks around bribery and corruption. We perform a full risk assessment and risk ranking on an annual basis which allows us to identify any ethical issues that may arise in the company and to take the appropriate action. As part of our methodology, we evaluate and rank how our countries are performing across criteria linked to the operations, context of the country and local control actions (audit, compliance, etc.)

In line with our anti-corruption commitment, the head of audit reports directly to the Audit Committee which is a sub-committee of the Board and its members are all Board members.

We take a risk-based approach to due diligence of subcontractors and suppliers. The level of diligence is based on a number of factors, such as industry, location, services provided and beyond. As an example, our visa and passport providers are required to complete a third-party due diligence process and follow our visa and passport procedures document.

In addition to due diligence requirements, our supplier agreements obligate the supplier to abide by all laws, rules and regulations, including those related to anti-bribery and corruption. They must also adhere to CWT standards.



We act to build a responsible supply chain

Our clients and stakeholders tell us how important it is to them that we work with suppliers who share our commitment to Responsible Business. We value ethical conduct, and because of this, we expect our partners in the supply chain to uphold the same rigorous standards that we do.

At CWT, business opportunities will never take priority over our reputation, our Code and the law. That's why we launched our Responsible Purchasing Program in 2014. The program helps us to mitigate ethical, social and environmental risks in our supply chain.

It has two main areas of focus: the CWT Responsible Supplier Code, which defines standards we ask our non-trade suppliers* to meet and an annual Supplier Corporate Social Responsibility (CSR) Assessment Campaign for key non-trade suppliers.

Our Responsible Purchasing Program demonstrates our commitment to the United Nations Global Compact (UNGC) and to the ILO principles and rights.

Our Responsible Supplier Code

To ensure that our non-trade suppliers observe CWT's high standards of ethical conduct, we expect our suppliers to adhere to the principles set out in our Responsible Supplier Code. The Responsible Supplier Code forms part of our Global Non-Trade Procurement Policy, which sets out the rules and procedures

that must be followed when making non-trade purchases (those not directly related to CWT's core business).

Available in six languages, CWT's Responsible Supplier Code clarifies the minimum requirements CWT expects from non-trade suppliers in terms of ethics, compliance, Human Rights, social, and environmental standards. We expect all our suppliers to operate in full compliance with the laws, rules and regulations to which they are subject, and our Responsible Supplier Code goes further, drawing upon internationally recognized standards to advance social and environmental responsibility.

CWT's Responsible Supplier Code covers the following broad topics:

- Compliance and Ethics;
- Human Rights, including anti-human trafficking and the fight against modern slavery;
- working conditions; and
- protection of the environment.

In 2017, a review of the Responsible Supplier Code was initiated to align it with industry-best practices and legislative trends. In accordance with CWT's commitment to the fight against human trafficking, and in line with the UK Modern Slavery Act, we reviewed the Responsible Supplier Code to reinforce our commitment towards preventing the use of any forms of modern slavery in our supply chains. The updated version of the Responsible Supplier Code will be published in 2018.

* Non-trade suppliers are those that are not directly related to CWT's core businesses. Examples of non-trade suppliers include IT and services companies.

We live ...

... to provide training and awareness on the Responsible Supplier Code

To ensure effective application of the Responsible Supplier Code, a video training module is available on our internal learning platform. This module was rolled-out in 2016 to all of CWT's senior management, representing most potential buyers of non-trade products and services. Internal guidelines on how to apply the Responsible Supplier Code are also available for all employees on our social intranet.

Supplier sustainability assessments

Ensuring that we keep up-to-speed with our supplier's performance is a fundamental part of our Responsible Purchasing Program. Our key non-trade suppliers are independently evaluated by the rating organization EcoVadis on 21 sustainability criteria relating to:

- labor practices (including Human Rights);
- environment;
- sustainable procurement; and
- fair business practices (including business ethics).

Started in 2014, the annual supplier assessment campaign is organized by our Global Responsible Business and Global Sourcing teams, who work closely with EcoVadis to coordinate the campaign and explain its importance to suppliers.



We act ...

... to protect customers and their information

As a world-class travel management partner, we provide state-of-the-art travel services to our clients. We do this within a comprehensive information security program which gives clients assurance around the security of their traveler's information as well as their own.

Not only are we transparent about how we are using our customers' data, we've also put in place effective policies and technical controls to safeguard our customers' information, whoever and wherever they are.

Our Information Security program embeds information security within our culture and is closely aligned to numerous industry standards (such as ISO, NIST, PCI DSS, etc.). We put significant investment into best-in-class tools, processes and people to ensure that we are up-to-speed with the latest regulatory and best-practice requirements.

Information Security and Data Privacy governance

Our Chief Information Security Officer is responsible for our Information Security program and is supported by a global information security team who report directly to our Chief Risk Officer. Beyond this, a Global Security Steering Committee, comprised of members from the CWT Executive Leadership Team, provides governance and oversight to facilitate the highest level of alignment, support and co-operation with global CWT security initiatives.

For data privacy, our Global Privacy Officer is responsible for the Data Privacy program. The Global Data Privacy Officer reports to the Vice President of Global Compliance and are supported by compliance and data privacy professionals located worldwide. Our CEO, executives, the Compliance Committee and Board of Directors receive regular updates and briefings on our performance in this area.

Our robust governance framework is supported by CWT's incident response system ([see iRespond on page 22](#)), which operates 24 hours a day, seven days a week. Our Business Resiliency program also tests and monitors for rapid response in case of business disruption, ensuring traveler data is protected and secured around the clock.

Our policies and standards

Our policies and standards form a robust framework by which CWT addresses physical and technical protection that ensure the confidentiality, integrity and availability of information.

We review and update our policies and standards annually (or as often as materially necessary) in response to changes in technology, infrastructure, regulatory and regional requirements as well as potential threats and security incidents.

CWT Information Security policies and standards cover data protection, comprehensive access controls, physical and environmental security, network and perimeter security, business resiliency, security assessments, security education and awareness. These also adhere to international regulations and standards such as the UK Data Protection Act, the EU Directive and General Data Protection Regulation (GDPR) and ISO 27001, among others.

We perform periodic internal and external audits on our products and services. These audits review compliance with information security and privacy policies, the National Institute of Standards and Technology (NIST), and the Payment Card Industry Data Security Standard (PCI DSS) requirements.



We live ...

... to prevent data security incidents

We take all the precautions necessary to prevent data security incidents. However, if an incident does occur, we must minimize the impact to our business and our stakeholders. In line with our Risk Management and Business Continuity Planning (BCP) processes, iRespond is our digital tool for reporting suspected information security incidents and fraud within the company. Employees can anonymously report an incident and initiate necessary processes. Our 24/7 incident response system supports this robust governance framework, while a Business Resiliency program tests and monitors for rapid response in case of business disruption to ensure that traveler data is protected and secured around the clock.

2017 Highlights

The General Data Protection Regulation (GDPR) takes effect on 25 May 2018. GDPR outlines a new set of rules designed to give EU citizens full control over their personal data. It aims to harmonize and simplify the regulatory environment for business so both citizens and businesses can fully benefit from the digital economy. CWT has been preparing for GDPR since the regulation was first announced in 2016. The company has been updating its Global Privacy program to meet GDPR standards and is well-positioned to achieve compliance with GDPR when it goes into effect and becomes enforceable.

Following the creation of a new EMEA data center in Madrid in 2016, responsible for hosting master traveler records, we expanded the data center's compliance to PCI requirements. We also received a clean opinion on the Services Organization Controls Accreditations (SOC) 2 type 2 Security Principle Report on Commercial services. These reports were completed by an American Institute of Certified Public Accountants firm on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy.

Raising awareness – inside and outside CWT

Our Information Security program includes regular training in data privacy, and the administrative, technical and physical safeguards that provide guidance to users for securing their information. All users are required to complete this training on an annual basis.

At any time, employees can access our global Information Security policies, which are readily available on our social intranet site. We also publish regular communications on security topics throughout the year to keep our employees up-to-speed and conscious of information security requirements and best practices.

To raise awareness, we held an annual Cyber Security Awareness Week in 2017 with the theme of 'Cyber Security is Everyone's Business'. The objective of the event was to provide tips and tricks for protecting business and personal information both at work and at home. Topics covered included everything from password protection to social engineering attacks and top tips on device security.

As well as keeping our teams engaged on these complex and ever-changing risks, our Compliance and Data Privacy team share best practices with other businesses, governments and expert organizations. In 2017, this included participating in the Global Business Travel Association's symposium on challenges specific to travel management in the energy, resources, and marine industries, the annual conference of the Society of Corporate Compliance and Ethics, and summits of the Privacy & Data Protection Officers, and Chief Financial Officers.



We said ...

2020 objectives

Further engage all employees and CWT partners through a global multi-year ethics training and communication program.

Deploy a robust external information campaign about our global policies and our best-practice approach to ethics and compliance, as well as our Responsible Purchasing program.

Continue protecting employee and client data through leading edge data privacy and information security policies and practices, while continually developing expertise throughout the organization.



We did ...

2017 performance

We achieved a 99% completion rate for our Code of Conduct training.

We shared best practices with businesses, governments, and expert organizations by participating in symposiums and conferences on ethics, compliance and data privacy.

We updated the Responsible Supplier Code to reinforce our commitment towards preventing any forms of modern slavery in our supply chain.

We redesigned our program on data privacy, including updates to our policy in line with General Data Protection Regulation (GDPR). We also received System and Organization Control (SOC) accreditation and Payment Card Industry (PCI) compliance for our EMEA data center in Madrid.



We will ...

2018 goals

Conduct regional compliance training at leadership conferences and develop subject-specific compliance training based on exposure to risk.

Further extend the scope and application of the Responsible Supplier Code to include more suppliers.

Maturing the Information Security program by maintaining our PCI and SOC compliance. PCI expansion to various key service centers along with aligning the program to meet regulatory requirements such as GDPR.

