

Code of Conduct

September 2026

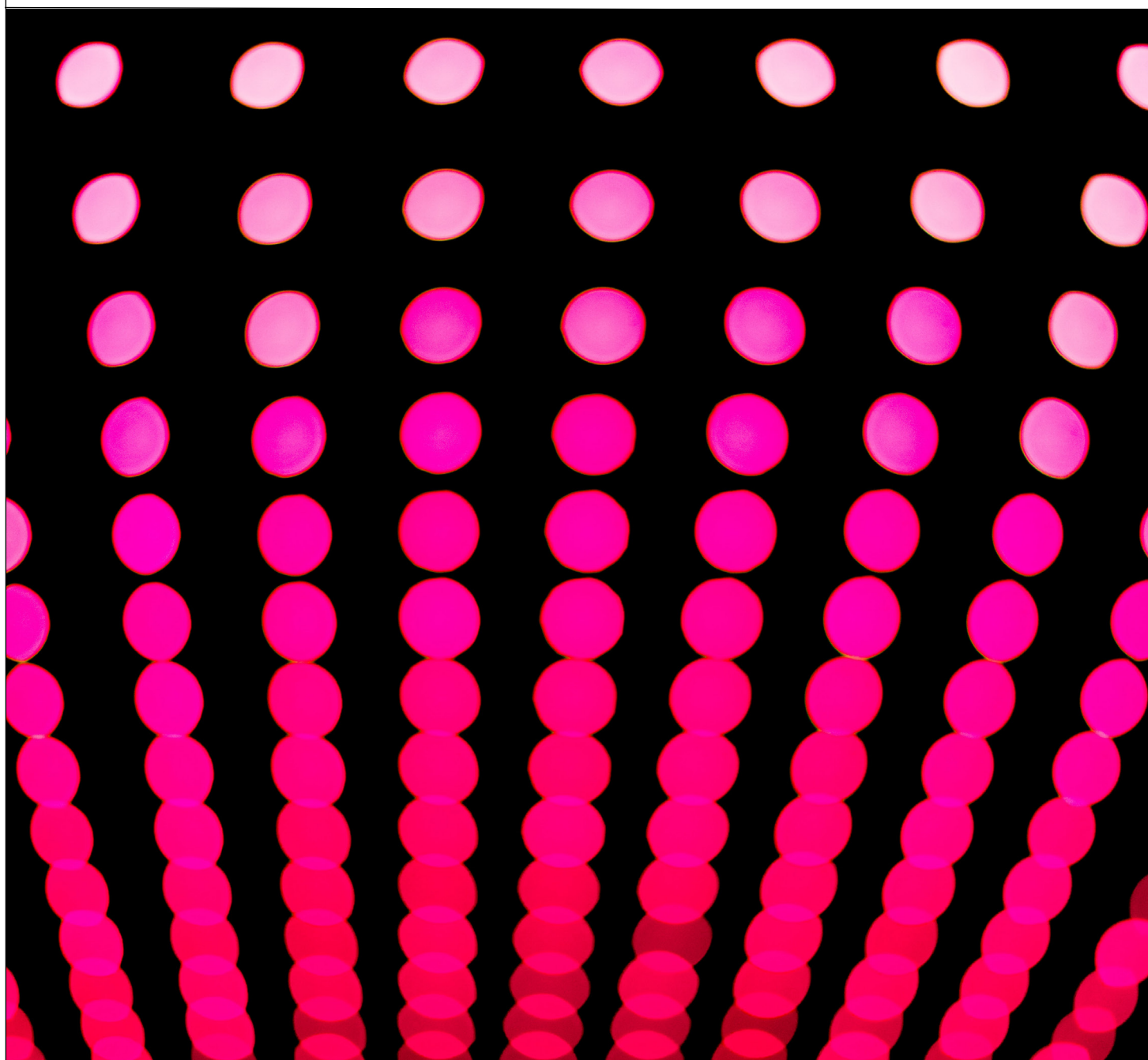


Table of contents

Letter from our Co-CEOs	1
Understanding our code of conduct	
Purpose of the Code	2
Application of the Code	2
Acting with integrity	
Our behaviours	3
Equal opportunity employer	3
Disciplinary and Grievance	3
Diversity and inclusion	4
Human rights	4
Modern Slavery and Human Trafficking	5
Safety and security in the workplace	6
Conflicts of interest	7
Sustainability and Corporate Responsibility	9
Gifts and Entertainment	10
Travel and Expenses	10
Representing OSTTRA	11
Communications with regulators and government agencies	11
Treating customers fairly	12
Compliance with laws, rules and regulations	
Anti-bribery and corruption	13
Money laundering and terrorist financing	14
Sanctions	16
Market abuse	16
Fraud	17
Confidentiality and data protection	18
Records and information management	19
FCA obligations / fit and proper (SMCR)	19
Other Regulatory Requirements	20
Communication channels	20
Keeping the company and our employees safe	
Information security	22
Use of AI	23
Right to monitor	23
Reporting Misconduct and Whistleblowing	
Non-retaliation	24
What to report	24
Reporting misconduct	25
Good faith reporting	25

Letter from our Co-CEOs

Team OSTTRA,

We have extraordinary people, partnerships, networks, and trust. That trust has been earned over many years - and we must each play our part in retaining it.

Our Code of Conduct ('the Code') is an essential component of our commitment to delivering excellence, ethically. It sets out clear expectations and high standards - so that all of us operate with integrity, honesty, and respect.

The code is a promise we make to our customers, shareholders, and one another that we will always do what we say we'll do, encourage others to do the same, and raise the bar even higher.

We are a global team of experts and owners - this code further empowers us to put the right behaviours at the heart of our decisions. Please read it thoroughly and apply it in your work.

Thank you for your dedication to strengthening our position of trust and for creating our distinct culture, as we build the future of post-trade, together.

Guy and John,

Co-CEOs



John Stewart and Guy Rowcliffe

Understanding our code of conduct

Purpose of the Code

This Code of Conduct (Code) outlines what we stand for, our ethical standards and how we conduct business.

Our Code cannot cover every situation. For this reason, we have separate corporate policies, procedures and guidelines for our business practices that provide more detail and information. Even then, we cannot predict or plan for every scenario – so take a responsible and cautious approach, and where something seems wrong, even if it is not directly prohibited by a policy, please escalate, or refrain from acting.

Please refer to these additional materials, which we reference throughout the Code, to better understand our expectations and requirements. Abiding by legal requirements, ethical standards and this Code is critically important for all of us. Failure to do so could subject individuals and the company to fines and criminal penalties and could cause OSTTRA to lose its ability to conduct business around the world. It could also cause serious damage to our reputation. Keep in mind that there may be times when laws differ significantly from region-to-region.

If you find yourself in a situation where local law or custom conflicts with our Code or other company policies, please escalate this to our compliance team, compliance@osttra.com to get further advice.

Application of the Code

Our Code applies to all employees, officers, and board members in all locations where we conduct business. We also expect our suppliers, and other business partners to comply with the law and ethical standards described in our Code, as well as the [third party vendor policies](#).

Failure to comply with the Code of Conduct and other company policies may result in disciplinary action, up to and including termination.

Acting with integrity

Our behaviours

- Our distinct culture is underpinned by a set of behaviours that define how we do things at OSTTRA.

They are:

- **Bold** - challenge yourself and others to think and act differently; unafraid to try, fail, and learn
- **Curious** - look for ways to improve our systems, processes or how we do things; connect the dots; share what we learn
- **Accountable**: strive for continued operational excellence; raise the bar even higher
- **Collaborative**: share knowledge; seek and strengthen relationships; forge collaboration.

Equal opportunity employer

We have policies and processes in place to ensure we are an equal opportunity employer. This means our processes ensure equal employment opportunities without regard to race, colour, religion, sex, sexual orientation, gender identity or expression, national origin, age, disability, pregnancy, veteran status, genetic information, citizenship status or any other basis prohibited by applicable law.

We are committed to equal employment opportunities at all levels of our organisation.

This applies to all employment practices, including but not limited to, recruitment, hiring, employment, assignment, training, compensation, benefits, demotion or transfer, promotions, disciplinary action and terminations.

Disciplinary and Grievance

OSTTRA is committed to maintaining a transparent, fair, and supportive work environment grounded in mutual trust and psychological safety. The Disciplinary and Grievance framework highlights OSTTRA's approach to dealing with instances of employee misconduct and/or complaints. We encourage open dialogue and provide clear guardrails to ensure that all employees are treated equitably, rights are protected, and conduct standards are consistently met.

Formal matters undergo independent fact-finding, objective reviews, and structured hearings. All proceedings, investigations, and records are handled with strict discretion to protect the privacy and safety of all participants.

Employees can raise concerns or participate in investigations in good faith without fear of reprisal, victimisation, or detriment. Where appropriate, minor conduct or performance issues are addressed informally through manager coaching and mutual support before formal escalation.

Where conduct falls below required standards we apply a structured outcome framework. Depending on the nature, frequency, and severity of the issue potential outcomes include: Informal advice, coaching, formal warnings, final written warnings and termination of employment.

For further details on the disciplinary and grievance processes, please refer to the Disciplinary and Grievance framework

Diversity and inclusion

Diversity is reflected in our commitment to an inclusive workplace that values each individual and their unique contributions.

Our people are our most valuable asset. Their diverse characteristics, perspectives, ideas, and backgrounds give us a vital competitive edge.

We have high expectations for our people, which is to be:

- Respectful to each other
- A team that works together and embrace each other's diverse perspectives and backgrounds
- Aware and cognisant of our approach to work-life balance such as flexible work arrangements
- A work environment free from discrimination and harassment

Any inappropriate conduct or behaviour against others will not be tolerated. Any employee found to be acting in an inappropriate manner may be subject to disciplinary action, up to and including termination of employment.

Human rights

We are committed to responsible and transparent operations that demonstrate respect and support for all human rights.

This means:

- We will always treat our people and members of the communities where we do business with dignity and respect
- We will always conduct business in a legal, ethical and responsible manner
- We believe it is important to work with vendors who operate with the same high standards we set for ourselves

Modern Slavery and Human Trafficking

OSTTRA maintains a zero-tolerance policy towards modern slavery and human trafficking across its organisation and supply chain, operating with a commitment to high ethical standards and compliance with relevant laws like the UK Modern Slavery Act. As a provider of post-trade financial services with a supply chain primarily focused on professional services and IT, OSTTRA identifies its business model as low-risk for such abuses. However, due diligence is carried out on vendors, clients and other suppliers to ensure that OSTTRA does not unwittingly breach the requirements.

If potential violations of the [Slavery or Human Trafficking statement](#) are identified, employees are reminded of their duty to make confidential reports or request guidance on such ethical issues by contacting Compliance or HR, submitting a confidential report through [EthicsPoint](#) or reporting to the appropriate criminal agency.



Safety and security in the workplace

We are committed to providing a safe and healthy workplace built on a foundation of strong and uncompromising ethics and integrity.

We all play an important role in creating that environment.

- We strive to create an environment where you can work in safety and comfort
- We maintain the security of our premises by safeguarding our people, physical assets, intellectual property, and other confidential, sensitive, and proprietary information
- We maintain a workplace safe and free from violence by prohibiting the possession or use of unauthorised dangerous weapons on company property

More information can be found in our [Physical and Environmental Security](#) and [Health and Safety Policies](#)

Conflicts of Interest

For any industry in which trust is a central feature, the need to have demonstrable standards of practice and the means to enforce them is a key requirement. We are committed to the highest level of integrity and complying with policies and controls relating to conflicts of interest.

A conflict of interest can be described as a situation in which someone in a position of trust has competing professional and/or personal interests that makes it difficult to fulfil their duties fairly.

While working at OSTTRA, you have an obligation to always do what is best for the company and its customers, above what would benefit you the most.

Conflicts of interest can arise between:

- OSTTRA and the interests of one or more customers
- Customers with competing interests
- Entities or individual functions or business divisions within OSTTRA
- You and the interests of one or more customers

There may be circumstances in which your personal interests could result in:

- A financial gain, or the avoidance of a financial loss, at the expense of a customer
- You have an interest in the outcome of a service provided to the customer in a transaction carried out on behalf of the customer, which is distinct from the customer's interest in that outcome
- You have a financial or other incentive to favour the interest of another customer or group of customers over the interest of the customer or potential customer
- You pursue or engage in the same kind of business as the customer or potential customer
- You receive (or expect to receive) inducements from a third party in relation to a service provided to the customer, in the form of monetary or non-monetary benefits or services

The list above is not exhaustive, and you have a responsibility to ensure that you adhere to our [Conflicts of Interest policy](#).

The main question when assessing if such a conflict of interest exists is whether the customer may be put or perceived to be put in an unfavourable position.

You must avoid any type of conflict and identify any situations that create, or appear to create, a conflict between your personal interests, OSTTRA's interests and any customer's interests.

All potential conflicts of interest should be disclosed, via the OSTTRA Compliance platform, ACA Compliance. It will be for your manager and our compliance team to decide if there is an actual conflict, and what, if any, adjustments need to be taken to remove the conflict.



Sustainability and corporate responsibility

OSTTRA is committed to operating responsibly, transparently, and with the highest standards of governance and risk management. Our commitment to driving progress begins within our own operations and extends across our value chain.

We actively fulfill our Environmental, Social, and Governance (ESG) responsibilities by:

- **Fostering Diversity & Inclusion:** Creating a safe, inclusive, and equitable workplace where all employees can thrive.
- **Establishing Our Environmental Footprint:** Measuring, monitoring, and managing our energy consumption and carbon emissions across global operations to establish a verified baseline for future performance
- **Upholding Strong Governance:** Maintaining effective executive management and Board oversight to ensure compliance, data security, and ethical decision-making.

Engaging Our Supply Chain: Partnering with suppliers who share our commitment to ethical labor practices and environmental responsibility.

ESG considerations inform our corporate governance mechanisms for effective Board oversight as well as how we manage our company to fulfill our strategic priorities and carry out our corporate purpose to accelerate progress for stakeholders and communities across the world.



Gifts and Entertainment

Developing relationships with our customers, vendors and other stakeholders is an important part of our business. Any giving or receiving of gifts, entertainment or other hospitality must be appropriate and reasonable, as well as in compliance with any legal requirements. In this way we will protect our reputation.

Gifts and entertainment should only be provided to strengthen business relationships and never with the aim to improperly influence the actions or decisions of another party. Improper gifts, entertainment, meals, or travel may create the appearance of a conflict – and where they are excessive, this may even risk appearing like a bribe.



Our [Gifts and Entertainment Policy](#) provides guidance on when it is appropriate to give or receive gifts or entertainment or other related hospitality, including the rules relating to government officials. Before accepting or providing any gift or entertainment, ensure you are familiar with the requirements of this policy. This also sets out limits that we see as reasonable, and not give a false perception of favouritism, bribery, or corruption.

Travel and Expenses

Expenses should be reasonable, directly related to company business and supported by appropriate documentation. If you travel or incur business-related expenses, you must be familiar with the requirements of the [Travel and Expense Policy](#).

When submitting expenses, please make sure you have included the required documentation, you have clearly described the business reason for the expense, you have included the names and affiliations for all those who attended and have appropriately categorised the expense type.

If you are uncertain about whether something would be an appropriate expense, please contact your manager.

Managers are responsible for all money spent and expenses incurred by their direct reports and must carefully review all expenditures before providing their approval.

Representing OSTTRA

To build our brand recognition, our experts around the world participate in media interviews and share commentary via social media platforms on a wide range of topics.

Our experts offer insight and analysis on news or thematic expertise pertaining to our industry. These interactions project the voice of OSTTRA, build our presence, promote recognition of our expertise and bolster our business and position in the marketplace.

Only those who have been granted permission to do so will be able to present the views of OSTTRA. If approached by the media, or if you have a view that you would like expressed with the media please seek permission before answering or expressing the view.

This is to ensure that we give a consistent view across all aspects of the business. One view that is out of kilter with the rest of our media presence could jeopardise an important opportunity elsewhere.

Colleagues are expected to act with integrity and be respectful to companies, shareholders and individuals.

For more information please refer to our [Global Media Policy](#).

Communications with regulators and government agencies

If there is a possible violation of law, then nothing in this Code or any other OSTTRA policy prevents you from communicating directly with or providing non-privileged documents or other information to a regulator or government agency. You may do so without disclosure to us and we may not retaliate against anyone for any of these actions.

In the course of your employment, it is unlikely that you will be contacted by or need to contact a regulator, policy maker, central bank, politician or government agency. Notwithstanding the above provision (concerning possible violations of law), you should consult with our compliance team and/or with the head of legal, risk, compliance and government and regulatory affairs in the event of any such contact, either as soon as it has been received, or before you intend to reach out.

Treating customers fairly

As part of operating with the highest levels of integrity, we will treat our customers in an objective, even-handed and professional manner, taking care to avoid preferential treatment of one or more customers.

Any concerns or complaints raised by customers will be treated promptly, effectively and with respect. Communications with customers will be clear and in plain language that is easy to understand.

An issue will be classified as a complaint if there has been an oral or written expression of dissatisfaction, whether justified or not, about the provision of an OSTTRA service.



Compliance with laws, rules and regulations

Anti-bribery and corruption

Bribery can be either active (offering, promising, or giving a bribe) or passive (requesting, agreeing to receive, or accepting a bribe). It makes no difference whether the person involved is a private person, a corporate entity, or a public official – what is relevant is whether there is an attempt, or a perception that there was an attempt to influence them with the intention of obtaining or retaining business.

Common indicators of bribery include:

- Payments for abnormal amounts or purposes
- Payments made in an unusual way
- Decisions are taken for which there is no clear rationale
- Records are incomplete or missing

We are committed to compliance with anti-bribery laws and regulations and will not give or receive illegal or improper payments, regardless of local business practices.

Decisions and actions concerning our businesses, and our relationships with third parties, will always be taken on objective grounds and without allowing any undue or improper influence.

We will follow our guiding principles and internal rules in the giving and receiving of gifts and entertainment.

Bribery and corruption are criminal offences and could result in direct action against you and OSTTRA. We expect our vendors and other third-party relations to honour the same level of integrity and to exercise zero tolerance for bribery and corruption.



Money laundering and terrorist financing

We will not tolerate our services being used in connection with money laundering or terrorist financing and will take all reasonable steps to ensure that we do not receive or otherwise handle any funds that are the proceeds of a crime.

The methods by which money may be laundered are varied and can range in sophistication. Any involvement in a transaction or service that is designed to conceal or disguise the nature, location, source, ownership, or control of proceeds may constitute money laundering

Money laundering is usually understood to be a three-stage process:

1. Placement - this means getting 'dirty' money into the financial system
2. Layering - this means mixing the 'dirty' money into the system so that it gradually 'disappears'
3. Integration - this is the result of placement and layering – the 'dirty' money is now indistinguishable from clean money and may be used.

The following activities are prohibited by law and may additionally incur criminal sentencing, including up to 14 years imprisonment:

- Becoming involved in a money laundering scheme
- Failing to report a suspicion that a customer or a third party is engaged in money laundering
- “Tipping off” a person suspected of money laundering
- Destroying or disposing of documents related to an investigation
- Failing to produce information or providing misleading information in response to request for such information in an investigation of suspected money laundering

Comprehensive anti-money laundering procedures are in place to ensure that our customers are fully identified and that business purposes are properly understood.

This is known as ‘Know Your Customer’ (KYC) checks. All customers are subject to KYC and cannot be onboarded without up-to-date KYC. Red flags or other suspicions are escalated internally and are examined in order to determine the proper course of action, including external reporting where necessary.

If you have any reason to suspect that a customer or other third party has engaged in money laundering or terrorist financing, you must immediately notify the relevant designated Anti-Money Laundering Reporting Officer (MLRO).

Training is also provided to ensure sound awareness of internal anti-money laundering procedures as well as money laundering risks and typologies.



Sanctions

We comply with all applicable sanctions regimes including those that prohibit business or financial relationships with certain entities, industries, or regions. Customers are also routinely screened to ensure that necessary actions are taken in the event of any new or updated sanctions.

For more information, please see the [OSTTRA Anti-Financial Crime Policy](#).

Market abuse

The financial services industry is highly regulated and there are widespread laws and prohibitions against insider trading and other forms of market abuse.

Rules to be aware of include:

- Insider dealing and unlawful disclosure: The insider dealing rule prohibits persons in possession of inside information from using that knowledge to deal or attempt to deal in financial instruments or to recommend or induce another person to transact on the basis of inside information. Unlawful disclosure of inside information is where a person possesses inside information and discloses that information to any other person, except where the disclosure is made in the normal exercise of employment, a profession, or duties.
- Market Manipulation: entering into a transaction, placing an order to carry out an execution or any other behaviour which gives or is likely to give false or misleading signals.

You have an ethical and legal obligation to maintain the confidentiality of information about OSTTRA and the companies with which we do business.

For more information on your obligations regarding market abuse and personal trading, please refer to our [Market Abuse Policy](#) and our [Personal Account Dealing Policy](#).

Fraud

OSTTRA is committed to fostering a culture with the highest ethical standards to uphold our company behaviours. As part of this commitment, we will follow the [OSTTRA Anti-Fraud Policy](#) to further enforce this message and provide guidance concerning any and all issues related to fraud and fraud related misconduct.

Fraud is defined as an act of deception intended to result in a financial or personal gain.

Examples of fraud include:

- Submitting false or misleading expense reports
- Unauthorised use of company assets;
- Reporting revenue that has not been earned or does not exist
- Submitting false or misleading financial statements
- Misappropriation of physical assets such as a company issued laptop or intellectual property or
- Using company funds to buy equipment or supplies for personal use or gain.



Fraudulent activities can be directed internally or externally within corporate organisations. An employee may engage in fraudulent activities that result in direct losses for OSTTRA, or alternatively, partake in such activities that could benefit the Company.

If you become aware, or have suspicions, of fraudulent activities or other dishonest behaviour, you are required to report the suspected activity immediately to your manager, our HR team or our compliance team.

See also the “Reporting misconduct” section below which also gives a method to report suspicions anonymously.

Confidentiality and data protection

Protecting the privacy of personal information is critical to ensure regulatory requirements, employee and client trust. We have a company-wide privacy compliance programme designed to protect the privacy of personal information under our control.

This is built on the core principles that we:

- Process personal information fairly and lawfully
- Collect personal information only for specified, explicit and legitimate purposes
- Process personal information only to an extent that is adequate, relevant, and not excessive
- Retain personal information only for as long as is necessary for the purpose for which it was collected
- Deploy technical and organisational safeguards to protect personal information
- Build Privacy into our business by design and default

Personal information is defined as any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier (e.g., employee ID number, email address, home address, date of birth, etc.).

We have comprehensive policies, procedures, and systems for protecting privacy that every employee, contractor and vendor is responsible for understanding and enforcing.

We communicate our commitment to privacy and data protection to our customers, prospects, vendors, and other stakeholders through our Privacy policy.

Vendor Risk Management also assesses and monitors vendors to ensure that they process personal information in compliance with our requirements, contractual obligations, and applicable privacy laws..

We must ensure our customers, prospects, and other stakeholders trust us with their personal information and we remain committed to meeting the highest standards of confidentiality and privacy.

To demonstrate our commitment to the protection of our employees' privacy, our [Global](#) and [US Privacy Policies](#) is tailored to jurisdictions and guides how we collect, process, transfer and store your personal data.

Records and information management

It is the responsibility of all of us to manage our information. The [Information Governance Policy](#) and related standards define information creation, identification, management, disposition, privacy and security.

All records, data, tools, and information created, received, or maintained during normal business activities or employment with OSTTRA remain the exclusive property of OSTTRA. Employees do not hold personal or proprietary rights over any OSTTRA information.

The Records and Information governance framework supports employees meeting our regulatory and client requirements.

FCA obligations / fit and proper (SMCR)

The UK FCA regulates some of our services, and as such the [FCA's Conduct Rules](#) apply to certain people working in those businesses.

However, at OSTTRA, we believe that we should all follow the principles set by the regulator. These are known as the "[Conduct Rules](#)" and they will help set the culture and standard that we use and want to be known for.

The Conduct Rules also now incorporates Non-Financial Misconduct (NFM), which includes bullying and intimidation, harassment, and violence. The FCA views NFM as a fundamental regulatory concern which directly breaches the Conduct Rules and can impact an individual's Fit and Proper assessment.

First tier – all employees

1. You must act with integrity
2. You must act with due care, skill and diligence
3. You must be open and cooperative with regulators
4. You must pay due regard to the interests of customers and treat them fairly
5. You must observe proper standards of market conduct.

The Second tier – these apply to Senior Managers (as approved by the FCA)

1. You must take reasonable steps to ensure that the business of the firm for which you are responsible is controlled effectively.
2. You must take reasonable steps to ensure that the business of the firm for which you are responsible complies with the relevant requirements and standards of the regulatory system.
3. You must take reasonable steps to ensure that any delegation of your responsibilities is to an appropriate person and that you oversee the discharge of the delegated responsibility effectively.
4. You must disclose appropriately any information of which the regulator should reasonably expect notice.

Other Regulatory Requirements

There are additional regulatory requirements in the United States that apply to TriOptima AB and OSTTRA SEF Limited. Specifically, additional National Futures Association (“NFA”) rules apply to TriOptima AB, in its capacity as an Introducing Broker, and Commodity Futures Trading Commission (“CFTC”) rules apply to OSTTRA SEF Limited in its capacity as a trading venue, and are outlined in the TriOptima AB Compliance Procedures Manual for US and the OSTTRA SEF Compliance Manual, respectively. Those OSTTRA employees whose work responsibilities include coverage of either of these entities will be expected to review and attest to the respective Compliance Manuals.

Communication channels

OSTTRA must ensure business communication remains secure and appropriate for a number of reasons including; data privacy, cybersecurity, accurate business records and finally - because there is a regulatory requirement to record and monitor communications to ensure that there is no inappropriate behaviour like market abuse and financial crime.

For this reason, interaction with clients of Optimisation services and OSTTRA SEF is captured, recorded, maintained and reviewed by the Compliance team to ensure that regulatory obligations are met.

Work related communication outside of OSTTRA platforms and contracted partners cannot be captured and monitored by OSTTRA and would be considered “off-channel” and should not be used. This includes but is not limited to unrecorded phone lines, personal email accounts and messaging apps such as iMessage, SnapChat, Signal and Telegram.

Monitored communications are adjusted depending on the role of the employee within OSTTRA. These communications include Google Mail, Google Chat, Google Meet, Bloomberg Chat, WhatsApp (limited to staff who have been informed), Teams, Zoom. There is a lot of regulatory scrutiny and as such, communications monitoring is industry-wide.

All OSTTRA employees must follow these rules:

- If business related, keep communication on OSTTRA system
- Consider content - as once on record, it is always on record.
- Any accidental use of unapproved communication methods should be escalated to Compliance immediately.
- Employees should never attempt to delete communications sent, especially those sent accidentally via off-channel communications.

Employees should be aware that their communications may be reviewed and monitored on a regular basis, as part of OSTTRA's compliance obligations. Violations can be subject to disciplinary actions up to termination of employment. See also the "Right to monitor" section below.

Keeping the company and our employees safe

Information security

An employee must not:

- Disclose any confidential information about OSTTRA or its activities
- Disclose any confidential information about OSTTRA's customers, clients or third parties
- Copy or disseminate internal communications, whether or not marked confidential, to third parties, unless authorised by the company.

Some general rules:

- You should use OSTTRA's systems and property only for OSTTRA's business
- Always lock your computer when leaving your desk or you are away from your computer
- Store confidential information in a secure area. It must not be left out on desks or in areas with unrestricted access
- Apply software updates in a timely manner when prompted.
- Be aware of your surroundings especially when conducting sensitive business conversations or working on privileged, confidential, or proprietary information
- Don't use public, unprotected Wi-Fi to conduct work without a secure Virtual Private Network (VPN)
- Never reuse passwords from OSTTRA for external systems and websites including personal use
- Never access systems that are not reasonably related to your responsibilities
- Never view inappropriate content or repeatedly open or click on suspicious emails that exhibit "Phishing" attributes, such as unfamiliar email sources, embedded links to unknown Internet sites, requests for payments, requests for passwords and/or other confidential information
- Never store company data on non-approved cloud storage platforms (e.g., Dropbox, and public GitHub)
- All mandatory security training must be completed by the specified deadline.
- Promptly report all suspected or confirmed security incidents, vulnerabilities, or policy violations to the Information Security team.
- Do not attempt to bypass or disable security controls e.g., antivirus software.

Use of AI

Generative AI can be used for the benefit of OSTTRA, however it presents novel and potentially serious legal risks which must be removed or mitigated.

These include but are not limited to:

- The risk of data breaches
- Infringement of third-party intellectual property
- Ambiguity around ownership of AI output
- Accidental use of open-source code.

As a partner of Google, OSTTRA is offered some intellectual property indemnities and data protection mechanisms to users of “Trusted Google Platforms” covering some of the risks set out above. For more details on these platforms and additional guidelines on the safe use of AI within OSTTRA please refer to the [OSTTRA Generative AI – Legal Use Policy](#).

Right to monitor

We have implemented several policies and procedures consistent with applicable law to protect the confidentiality, integrity, and availability of our information assets. To support these efforts, we reserve the right to take possession, access, review, monitor, intercept, or conduct surveillance on any content or materials located on any OSTTRA information resource or facility.

The OSTTRA information assets you use or to which you have access are the property of OSTTRA and are provided for official business use. Our information resources should only be used for business-related purposes. Personal use of our assets should be limited to incidental use. Any communication conducted on our assets and systems is not your personal or private property, and we reserve the right to view that communication at any time. In addition, we may disclose these communications to designated OSTTRA officials, law enforcement officials or other persons when appropriate. Use of our information resources for conducting any outside business activities is strictly prohibited.

There may be times when you will access or monitor workspaces – including information stored on and usage of your company computer – for the safety of others or when otherwise deemed appropriate in the judgement of management.

All security incidents must be reported to our Technical Operations Centre (TOC) via email at DL-TOC-Incident-Notification@osttra.com as soon as possible. Security incidents include any possible or actual violations of our security practices, such as losing a piece of confidential information or leaving a laptop unlocked and unattended in public.

Reporting misconduct and Whistleblowing

Non-retaliation

We understand that you may be apprehensive about reporting misconduct. However, you should know that we will provide support when you raise concerns in good faith, even if your concern turns out to be mistaken. All internal investigations will be conducted confidentially and as discreetly as possible given the facts and circumstances of the situation.

We are prohibited from threatening or retaliating in any way against people who report misconduct in good faith. Any employee, officer or director found to have engaged in threats or retaliation will be subject to disciplinary action, up to and including termination.

If you believe you have suffered any detrimental treatment as a result of reporting misconduct in good faith, please inform our Head of HR or Legal immediately.

What to report

You have an obligation to speak up and report any conduct or wrongdoing that violates our Code or any applicable law, rule, or regulation, regardless of whether it is about to occur or has already occurred.

You must be alert and sensitive to situations that could result in misconduct. Situations that may involve a violation of our Code or applicable laws, rules or regulations may not always be clear and may require making difficult decisions and exercising careful judgement.

Always raise concerns or questions about the propriety of a course of action or decision with a manager or a member of the compliance department.

Any concerns or questions you may have about possible wrongdoing should be raised using the procedures below

Reporting misconduct

Whether you are raising a concern about a potential violation, or seeking advice, we have multiple resources to help guide you.

1. You can share your concern with your manager
2. Contact any member of the OSTTRA HR team who can provide further guidance
3. You can report a concern, anonymously if you choose, online or by phone to [Ethics Point](#). When calling the hotline, you can speak to someone who can guide you through the process
4. Contact a member of Legal or Compliance for guidance on any situation involving the Code or any other laws, policies, standards, or procedures.

Good faith reporting

The effectiveness of our Code and the policies summarised in it rely on your judgement. We take concerns of misconduct very seriously and expect that any employee, officer, or contractor who reports misconduct does so in good faith.

Bad faith reporting or misuse of the reporting system is a violation of our Code and can be very damaging to us and your fellow colleagues.



For more information, please email compliance@osttra.com

osttra.com

OSTTRA

The Global Post-Trade Network