
Code of Conduct
Living our Values of Integrity, Ownership and Caring
Win. The Right Way.
Together.
UniCredit

Index



A message from our CEO and the Group Executive Committee 3

Our Culture 4 - 6

General Principles of Conduct 7 - 12

Social Media and External Communications 13 - 14

Client Interest Protection 15 - 16

Antitrust 17 - 18

Market Integrity 19 - 20

Anti-Money Laundering, Counter-Terrorist Financing and Financial Sanctions 21 - 23

Anti-bribery and Anti-corruption 24 - 25

Data Protection 26 - 28

Glossary 29

A message from our CEO

and the Group Executive Committee

Dear Colleagues,

When I joined UniCredit, I stated that we have an ambition that goes beyond the basic role of providing financial support to our society. We want to act as the engine of social progress and **be the Bank for Europe's future.**

To achieve this goal, our Group has a critical role to play, always striving for success: for our clients, for our investors and for ourselves. This begins with our people and the Culture that we create together.

Our mindset is to **Win. The Right Way. Together**. This is what will enable us to deliver sustainable long-term success and create a **Culture that each of us is part of and can be proud of.** A Culture that puts our Values of **Integrity, Ownership and Caring** at the heart of our decision-making and everything we do.

Our Culture and these Values are more than just words. They embody what we stand for, determine how we act, and shape the decisions that we take every day.

And this is where our **Code of Conduct** comes into play. It outlines how we bring our Culture to life in our everyday behaviours and how we treat all our stakeholders.

It guides all our actions and behaviours.
It ensures their coherence with our new set of Values.
It guarantees the highest standard of professional conduct from all UniCredit's employees and other external experts involved in any activity on behalf of our Bank.
It sets us apart from being simply a good company and positions us as a great company.

Our Code of Conduct isn't a nice to have, it is a critical tool in the success of our business. We will be judged on our adherence to this Code, and it defines how we will all be held accountable.

I urge you to comply not only with the letter of what is set out in this Code, but also with the spirit. Each and every one of us has a responsibility to hold ourselves to the highest standard, and to hold others to that same standard.

Let's embrace our Code of Conduct as we take **another step forward in our transformation journey.**

Let's make it our mission to further cement it in the way we do business. Doing so will ensure we stay on the path we are forging: a path to achieve our goals and **Win. The Right Way. Together.**



Our Culture



Our Culture is the blueprint for how our bank will operate, with our Values, Purpose, and Ambition working in synergy to deliver for all stakeholders. It informs every aspect of how we do business, as detailed in our Code of Conduct.

Andrea Orcel

As UniCredit, we have a choice to make.

We can fulfil the basic role of banks and provide the financial support and infrastructure necessary for society to function.

Or, we can return to our fundamental role within society: to act as the engine of social progress, to help Europe and its people to become stronger than ever.

We choose the latter. And we ask that you do too. Because if

we are to succeed, we will succeed together.

As one team working to a shared Culture.

Our Values are more than just words. They are Actions.

Mandates. Pledges.

Our Values are more than just words. They are Actions. Mandates. Pledges.

Our Culture

We ask you to sign up to the UniCredit Culture, to the belief that our Group can go further and do better – for our people, our clients, our investors, and for Europe.
Our Culture starts and ends with our people – with giving you what you need to succeed. It starts with our Culture.
At UniCredit, we work with a shared mindset and Values. We ask that you subscribe to these.

Our mindset is to **Win. The Right Way. Together.**

We are not afraid of ambition. We want to win: for our clients, for our investors and for ourselves.
We want to win in the right way – putting our Values at the heart of our decision-making and everything we do.
And we will do it together, as one team acting as true partners to our different stakeholders.

We encourage everyone to embody this mindset. We will never punish you for trying to win, as long as you do so in the right way.
If mistakes are made, but your reaction is right and in line with our Values – owning up to them and working together to put them right – we will always support you.

Integrity

- We act in the best interests of our customers.
- We are honest, straightforward, and transparent.
- We do the right thing – even when no-one is watching.

Ownership

- We deliver on our promises and take accountability for our actions and commitments.
- We are empowered to make decisions and learn from failure.
- We speak up – to express an idea, an opinion or when we see something wrong.

Caring

- We care about our customers, communities, and each other.
- We are eager to help one another and for our people to thrive.
- We treat each other with respect and value our differences.

When we all commit to these shared Values, we will deliver for our clients. And delivering for our clients – in any way, large or small – is how we fulfil our Purpose.
If we all pull together, we can achieve concrete results for our clients and Win. The right way. Together.
And we will achieve our Purpose: to provide the communities we serve with levers for progress.
Only in this way can we be the bank for Europe‘s future.

Our Values are more than just words. They are Actions. Mandates. Pledges.

Our Purpose

When we offer someone a mortgage, we are giving a family a new home.

When we provide a loan, we enable young entrepreneurs to fulfil their ambition of becoming business owners.

When we open a bank account, we are setting someone up with the tools to build a secure and stable life.

All those small but significant moments are why we exist. And together, they amount to something greater than the sum of their parts. They amount to our Purpose: **empowering communities to progress**, to unlock the potential of individuals, communities and businesses across Europe.

Our Ambition

Working to deliver this Purpose every single day will give us financial strength to achieve our ambition and be the **bank for Europe's future**.

It's no secret that we must be financially strong and resilient, able to withstand inevitable economic changes and market shocks that will upset those challengers with less experience, local knowledge, and trust of its clients than we have.

More than that, we must grow. We do not shy away from this aspiration or see it as independent of our Purpose or Culture. In fact, we embrace it.

Because it is this financial success which will enable us to serve more clients and to serve them better, building trust with them and their communities – a trust which will enable us to continue succeeding and growing over the long-term.

Working in synergy

So, you see, in our Culture, our ambition for financial success is inseparable from fulfilling our social Purpose, both of which are powered by our team working with a shared Culture.

We cannot have any one of these without the others. And we should not want to.

General principles of conduct



This Code of Conduct has been written in line with our Group's Values – Integrity, Ownership and Caring – that guide all our actions and behaviours. Such Values are driven by our Purpose to deliver outstanding performance and have a positive impact on our customers, shareholders, communities and people.

How we work

UniCredit expects a **high standard** of professional conduct from its employees and other professionals involved in activities related to the Bank's operations or on behalf of UniCredit. Everything we do should comply with all applicable laws and regulations, our internal rules, and the professional standards of our industry, in line with our Diversity, Equity and Inclusion principles as strategic assets for our business, growth, innovation and performance, which also are integral parts of our corporate Culture.

In practice, this translates into recognising and mitigating unconscious bias, promoting inclusive and fair decision making, and supporting equal access to opportunities, development and visibility for all employees, regardless of role, background or personal characteristics.

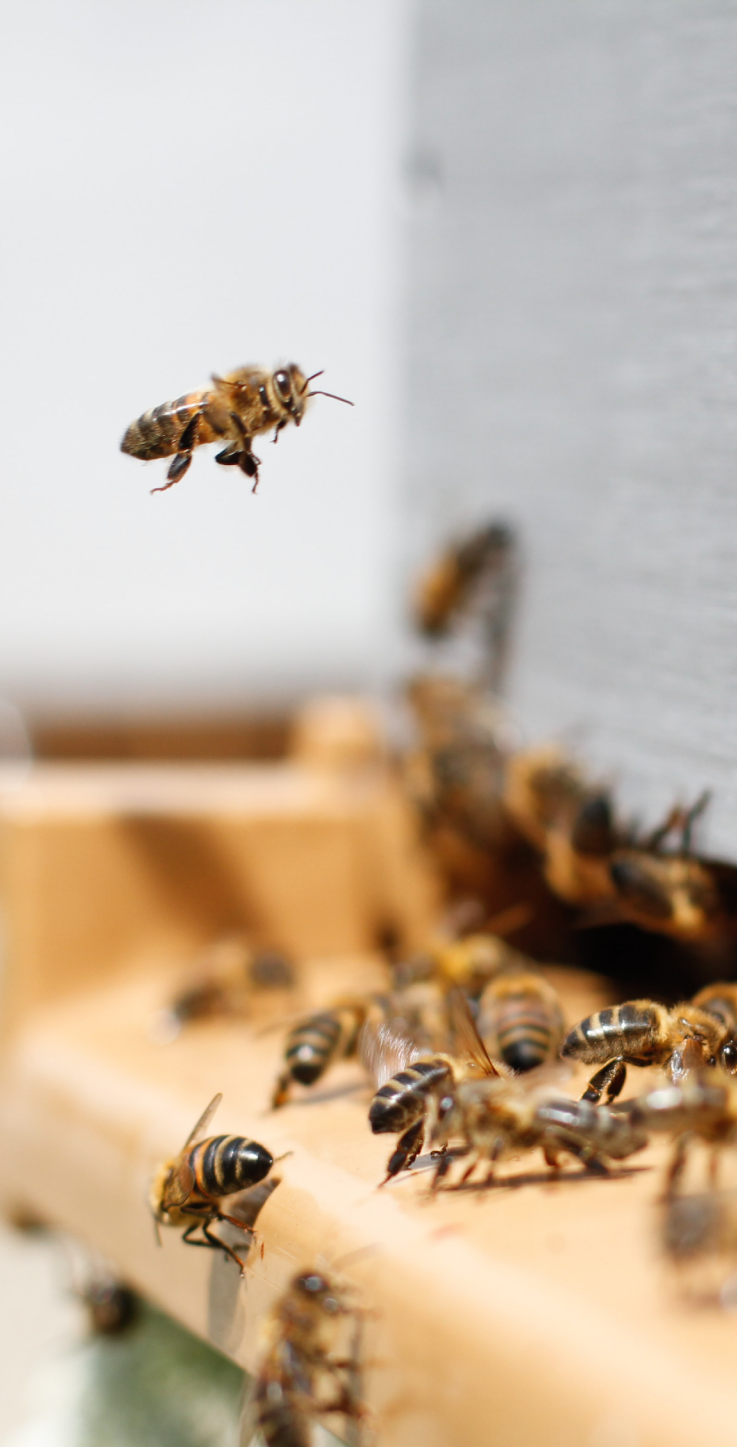
Managers play a key role in embedding these principles by leading through their conduct, encouraging ethical, inclusive and fair decision-making, ensuring awareness and understanding of the Code of Conduct, and fostering an open environment in which employees feel comfortable asking questions, expressing constructive challenge, raising concerns and escalating issues.





The UniCredit Group, its employees and third parties (when acting on behalf of UniCredit), **are prohibited** from facilitating attempts by clients, counterparties, or employees to defraud, deceive or otherwise mislead any authority, including the tax authorities. This prohibition applies irrespective of where the conduct occurs and includes any behaviour that could expose UniCredit to liability under applicable laws in any jurisdiction in which UniCredit operates, including through its branches.

Two of the Group's most important assets are its **reputation and business sustainability**. That is why we are clear about our roles and responsibilities within the Group. This is also why we have mandatory training programmes and expect our people to master the skills required by their jobs in order to do their work with efficiency, care and an appropriate sense of personal and ethical responsibility, and constantly improve their knowledge of products, services and internal processes and procedures.



How we support the environment and society

At UniCredit, **ESG** (Environmental, Social and Governance – hereinafter "ESG") considerations are fundamental to every decision we make and every action we take. They are a central part of how we do business. We know that fulfilling our Purpose of empowering communities to progress would not be possible without meeting the highest ESG standards across the Bank.

Our business is governed by ESG principles because it is the right thing to do, and it will help us fulfil our Purpose in the long term since we believe that the ESG transformation has been the greatest business opportunity in decades.

ESG has great potential and poses many challenges. We will constantly be required to assess **the trade-off** between environmental impact and social repercussions. These are equally important for UniCredit: we are realistic about their interaction and we know that we can **create value** through finding the right balance between them.

Compromises will be necessary if we are committed to achieving our goals in both these areas, but we will make these with our ultimate Purpose in mind, focusing our energies on where we can have the greatest impact.

In recent years, thanks to a clear multistakeholder approach, we have made significant efforts to integrate all ESG factors into our Bank's governance, business, risk and credit management, metrics and operations.

Banks have an important social function which goes far beyond lending. We have a significant responsibility to support customers in their own business transformation and guide financing in the right direction. Our role is to help our clients and communities make meaningful progress towards a more sustainable, inclusive and equitable society over the long term.

At UniCredit, we recognize that respect for human rights is fundamental to sustainable business and to the trust placed in us by our stakeholders. We are committed to conducting our activities in a manner consistent with internationally recognized human rights standards, including the prohibition of child labour, and expect the same commitment from our business partners.

We will continue to play our part by **boosting stakeholders' trust**, supporting impactful social initiatives, and consistently measuring our results to ensure that we are all held accountable. This will help ensure that ESG considerations remain embedded across our business and operations as we build a Bank ready to thrive over the long term.

A bank for Europe's future.



How we empower our employees

It is always extremely important for colleagues to feel free to voice their concerns about questionable conduct they may become aware of. Managers have the responsibility to create a safe environment where team members feel comfortable and are encouraged to raise their concerns or report any misconduct (i.e., the so-called **"whistleblowing"**). Every employee is encouraged to speak up when they become aware of potential misconduct. Good faith reporting is in fact always encouraged and protected, even when concerns are ultimately found to be unfounded. Managers are also expected to monitor the conduct of employees under their supervision, ensure that our Code of Conduct is applied consistently, and guarantee that whistleblowers are not retaliated against in any way. At UniCredit, empowerment is also rooted in psychological safety, whereby people can ask questions, share ideas, challenge decisions respectfully and acknowledge mistakes without fear of negative consequences, consistently with our Values and Culture.

To this end, the Group guarantees the confidentiality of any information that is provided by whistleblowers and will treat it with the utmost care.



How we ensure a fair workplace

UniCredit requires its employees to contribute to creating and **maintaining a non-discriminatory working environment** that is respectful, safe, and inclusive, where differences in gender identity, age, race, ethnicity, sexual orientation, ability, background, religious or ethical Values and political beliefs or any other category protected by law in the local jurisdiction are embraced and valued. Managers at all levels play a key role in upholding this commitment and are expected to actively prevent, recognise and address behaviours or practices that could lead to discrimination, exclusion or inequitable outcomes, even where unintentional.

We must treat others with dignity and respect with **zero tolerance** for mobbing and **bullying.**

During recruitment, assessment, promotion, or other people-related processes, it is also our responsibility to act without any prejudice encompassing the criteria of objectivity, competence, professionalism, and equal opportunities, without practicing favouritism. In this way, we can ensure that those with the best available expertise, the highest levels of professional integrity and fit to our Values are selected.





Ethics and Responsibility in Artificial Intelligence

Artificial Intelligence (AI) offers significant opportunities to improve the way we serve customers, support colleagues, and conduct business. At UniCredit, we are committed to using AI responsibly, ethically, and in a manner that upholds our values. UniCredit employees are therefore expected to use AI in a way that is fair, transparent, accountable, and respectful of the rights and interests of customers, colleagues, and other stakeholders. Human judgement and responsibility must remain central to important decisions, particularly where individuals may be significantly affected.

When using AI, employees must:

- exercise appropriate professional judgement and not rely solely on AI-generated outputs;
- verify the accuracy and suitability of information produced by AI systems before using it for business purposes;
- respect confidentiality, privacy, intellectual property, and data protection requirements;
- avoid uses of AI that may result in bias, discrimination, unfair treatment, or harm to individuals or groups;
- use AI tools responsibly and only for legitimate business purposes.

Employees should promptly raise concerns about AI systems or uses of AI that may create ethical, legal, regulatory, security, or reputational risks.

By embracing innovation while acting responsibly, UniCredit seeks to ensure that AI is used in a manner that benefits our customers, colleagues, communities, and society as a whole, and ensures ethical data processing and the informed use of both AI Systems (AIS) and General Purpose Artificial Intelligence (GPAI) Models.



How we protect our Group

We are also expected to consider the broad environmental and human consequences of the business decisions we make. As a banking Group, the financing we provide to the real economy can significantly affect the communities we serve, and it is part of our job to make sure that our impact is overwhelmingly positive.

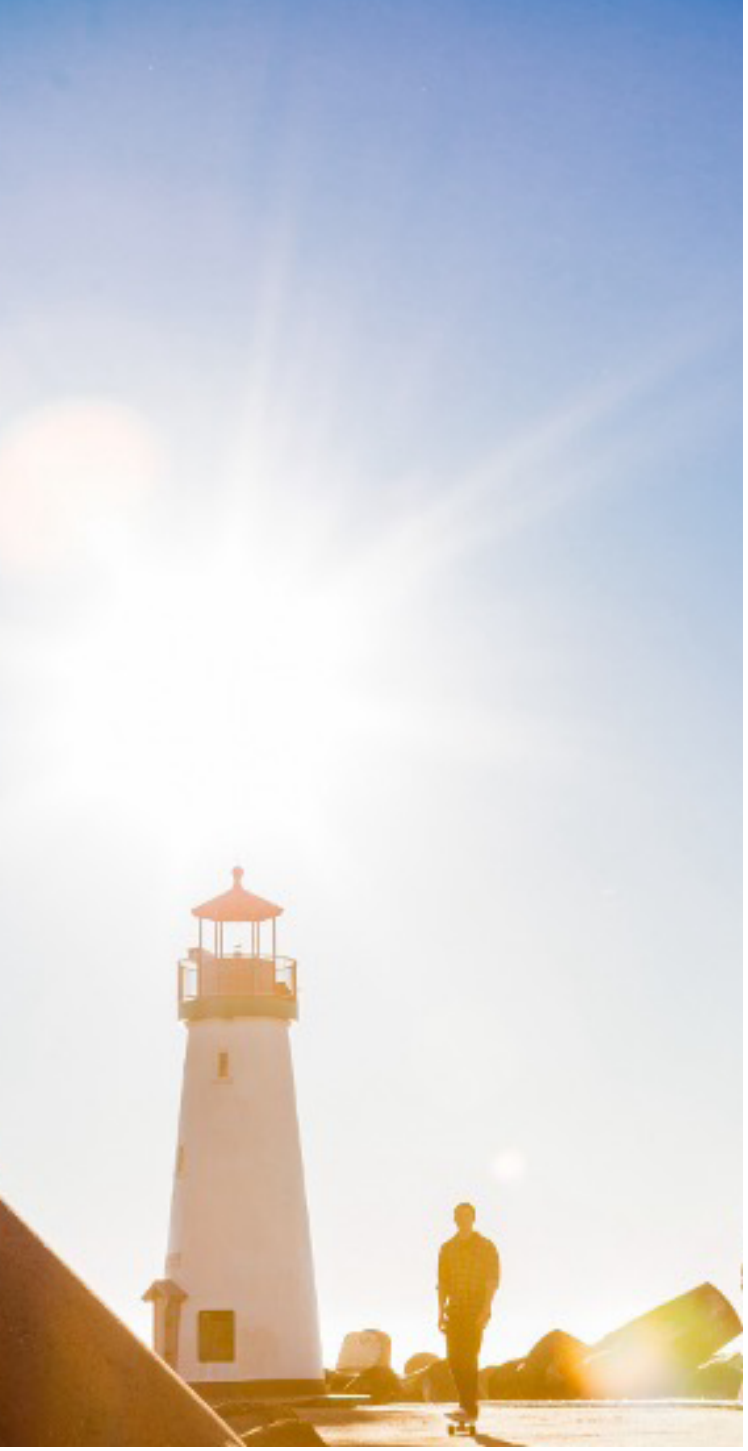
In addition, we are expected to **safeguard and protect the assets owned by the Group** itself. From capital and clients' information to facilities and email accounts, all Group's assets must be used only for legitimate business purposes.
Data and information must not be shared via tools which are not authorized by the Group. As employees, we have been entrusted with the proper use of these assets, and we should always treat them with respect even if, or when, our relationship with the Group comes to an end. This requirement pertains to physical assets, as well as to confidential information and intellectual property.

Cybersecurity is everyone's responsibility. Employees are expected to protect the confidentiality, integrity, and availability of UniCredit's information, systems, and customer data by complying with applicable security policies, standards, and procedures. Employees must remain vigilant against phishing, social engineering, malware, fraud attempts, and other cyber threats. They are expected to use only authorized systems and tools, safeguard passwords and credentials, secure devices and information, and handle confidential, sensitive, and personal data responsibly.
Any suspected or actual security incident, vulnerability, unauthorized access, data loss, suspicious activity, or breach of security requirements must be reported promptly through designated reporting channels. Employees are expected to cooperate fully with investigations and remediation activities related to cybersecurity incidents.

UniCredit operates on a strict "need-to-know" basis to protect internal, confidential, sensitive and inside information. Employees only have access to information to the extent that it is necessary for the normal exercise of their employment and duties, and always actively consider if there is a legitimate business "need-to-know" before sharing any information, keeping the number of people privy to information to the minimum necessary and carefully assessing the potential impact of tools used for processing, communicating and storing of information (e.g. chat applications, file sharing platforms, web-based AI and GenAI tools).

Only authorised personnel can speak on behalf of the Group. We shall use UniCredit's name and brand images in line with the internal brand policies and guidelines in place, always in good faith. All communications issued on behalf of UniCredit should always be accurate and comply with all applicable regulations. The same can be said of our interactions with all governmental authorities. Making false or misleading statements, concealing key data, or intentionally providing inaccurate information is strictly forbidden.

All Group Legal Entities and all employees have to comply with tax legislation by carrying out only activities that are supported by actual business purposes and economic substance; it is forbidden to carry out transactions aimed at circumventing **tax legislation** or obtaining undue tax reductions and/or benefits.



When acting on behalf of UniCredit Group, employees are prohibited from undertaking operations and other initiatives or propose investments and products to Customers with the intent to evade and/or elude taxes, or to obtain undue tax advantages in violation of the law.

Employees are required to promptly provide complete, accurate, reliable and transparent information to all tax authorities and tax obligations must be carried out correctly and within the deadlines established by law.

Improper handling of personal finances (borrowing, gambling, activities on prediction markets, certain kinds of investments), communications and other personal activities, may generate reputational risk for the employee and for the Group; for this reason, employees should always make sure that any behavior, inside or outside our premises, will be following the ethical rules mentioned in the Code and must not prejudice, even indirectly or potentially, the trust that Group and the Customers put in the employees of the Bank.

The Group faces potential legal, regulatory and reputational risks in the area of **financial crime**. Assisting money launderers and terrorist financiers or sanction evaders is prohibited and can have serious legal and reputational consequences. All suspicious transactions, including attempted transactions, should be reported, regardless of the amount.

Conflicts of interest whether actual, potential or perceived, should be avoided wherever possible and properly disclosed and managed when they arise. This helps ensure that our people always act in the best interests of UniCredit, its customers and its stakeholders. Any situation that could give rise to a conflict of interest **should** be promptly reported. This includes interests held by close/next relatives – as defined by applicable local laws - who may benefit from a business decision or transaction that an employee can influence. Where an Employee knows that a person or entity is a UniCredit customer or supplier, any purchase of goods or services from that person or entity must be made on arm's-length terms and at prevailing market prices, without preferential treatment or undue advantage.

Upon termination of their employment or any other professional relationship with UniCredit, all persons subject to this Code must not retain, transfer, disclose or use any confidential information belonging to the Group. Obligations relating to confidentiality, data protection, intellectual property and the proper handling of information continue even after employment or any other professional relationship with the Group has ended. They remain responsible for safeguarding information obtained during their employment or engagement with the Group and must not use such information for their own benefit or for the benefit of third parties.

Any Employee who breaches this Code or otherwise acts inconsistently with the obligations set out herein, **may be subject to disciplinary action** by the People & Culture function in accordance with UniCredit's procedures. The individuals responsible for such breaches may also be subject to administrative sanctions imposed by the competent local or International regulatory authorities, as well as legal proceedings in accordance with the applicable law.

Serious violations of this Code and the applicable local procedures and regulations may result in termination of employment or other appropriate measures, as applicable.

Social Media and External Communications

The way we communicate, both online and offline, can have a direct impact on UniCredit's reputation, our customers' trust and our business relationships.

Every employee has a responsibility to use social media and communication channels responsibly.



Social media offers valuable opportunities to engage, collaborate and share knowledge. However, improper use may expose the Group to legal, regulatory, cybersecurity and reputational risks.

Employees must ensure that any communication relating to UniCredit complies with applicable laws, regulatory requirements, internal policies and confidentiality obligations.

Unless specifically authorized, employees must not speak on behalf of the Group, disclose confidential information, comment on sensitive business matters or create the impression that personal opinions represent UniCredit's position.

BEHAVIOURS AND TIPS

Use social media responsibly

- Think carefully before posting, commenting or sharing content
- Remember that online information may remain publicly accessible indefinitely
- Act in a manner consistent with UniCredit's Values and reputation

Protect confidential information

- Never disclose confidential, proprietary, customer or inside information
- Do not share internal documents, screenshots, business plans or sensitive data
- Follow all information security and data protection requirements

Be clear about personal opinions

- Do not represent personal views as those of UniCredit

I use social media and external communication channels responsibly, considering the possible impact of my words and actions on UniCredit's reputation, customers' trust and business relationships.

I protect confidential and sensitive information and never present my personal opinions as UniCredit's official position, unless I am specifically authorized to do so.

Employees' voices

Client Interest Protection

At UniCredit, we have regulatory, legal and ethical obligations to safeguard our customers' financial interests.

People trust us with their assets and with decisions that directly affect their livelihoods.

It is our responsibility to ensure that we protect their best interests in our daily professional activities.



First and foremost, people acting on behalf of UniCredit have to show **reasonable care** and **prudent judgment** toward our customers. We need to act in our customers' best interests, while complying with all applicable laws and regulations and our own internal rules. We also need to obtain proper authorisation from the customer and from our supervisors whenever this is required.

One of the ways we protect the interests of our clients is through **fair dealing** and by avoiding **mis-selling**, treating customers fairly and in the same way – without inappropriate preferential treatment. Transparency should be at the core of our interactions with the people we serve every day.

It is also important to handle the **information** we gather on our customers and our relationship with them with respect and confidentiality, and only disclose it to third parties outside UniCredit Group when we are legally allowed to do so or with the customer's explicit written consent.

Everyone at UniCredit is expected to do their best to understand our clients' **needs and expectations** and to address customer complaints in a fair and timely manner.

Lastly, whenever we provide **financial advice** to customers or make investment decisions on their behalf, we must consider the suitability of our choices to the client's specific situation, including risk tolerance and stated preferences.

BEHAVIOURS AND TIPS

Take a holistic view of your customers' needs and work with them to identify the most appropriate customised solutions

- Interact with your customers and listen to their needs to evaluate the available options to meet them
- Involve your customers in decision-making and always keep them informed throughout the process
- Collaborate with other departments to develop a holistic perspective and identify better solutions

Build customers' trust and provide them with complete information and documentation

- Ensure that any information you share is accurate, complete and communicated clearly so that your customers recognise you as a trusted advisor
- Demonstrate your knowledge and expertise by using all available materials in a structured and professional manner
- Reply to requests in a timely manner, taking into account both the Bank's and customers' legitimate interests
- Remember that those acting on behalf of a Client must always have specific authorization. In any case, employees (including, among others, relationship managers and branch staff) must not have direct responsibility for, or exercise any decision-making authority over, customer relationships involving family members or individuals with whom they have an equivalent close personal relationship.

Communicate clearly, using straightforward language that is appropriate to your audience and the communication channel

- Consider who your audience is and adapt your behaviour accordingly
- Use simple language and avoid jargon
- Provide explanatory documentation to help customers understand mandatory clauses
- Communication should be adapted to the channel used: adjust your language and tone accordingly

Employees' voices

"I ask other departments for advice if I think it can help better satisfy my customers' needs."

"I always try to strike a balance between the Bank's interests and customers' requirements."

Antitrust

Effective competition enables businesses to compete on equal terms, while putting them under pressure to strive continuously to offer the best possible products at the best possible prices.

Preventing Antitrust risks means that markets remain competitive, to the benefit of our customers and suppliers. Due to the cross-business and cross-functional nature of Antitrust all employees must fully comply with Antitrust rules.

UniCredit has always been highly committed to compliance with Antitrust rules, with the aim of promoting and safeguarding free and fair competition in the market. UniCredit staff must also comply with relevant Antitrust regulations. Antitrust rules fight illegal practices such as price-fixing, market sharing, bid-rigging conspiracies, cartels, sharing of commercially sensitive information among competitors, and abuse of dominant position on the market.

As per law requirements, no one at UniCredit shall enter into anticompetitive agreements, – i.e., agreements which prevent, restrict, or distort competition. Anticompetitive agreements may occur not only when an oral or written properly so-called agreement is concluded, but also through common understanding or conscious cooperation. Also, passive participation in an infringement, such as the presence in meetings where an anticompetitive agreement is concluded is indicative of collusion capable of making the business liable for the infringement.

In relationships with competitors, employees must refrain from exchanging, disclosing or receiving strategic or commercially sensitive information - e.g., confidential data on future market behaviours or product strategies, such as prices, costs, customer lists, marketing plans, etc., and from passing on such information to third parties, as it may lead to uniform conduct on the market to the detriment of competition.

In case of dominant position, – i.e., market share equal to or higher than 40%, any abuse – e.g., predatory pricing, discriminatory conditions, specific kinds of rebates, as well as imposing exclusivity or tie-in on products or services – shall be avoided.

In case of transactions involving the acquisition of significant governance rights in third party undertakings, the need to proceed with prior notification of concentration before the relevant Antitrust Authority shall be carefully assessed.

If you have any questions, please do not hesitate to reach out to our Compliance department before taking action.

BEHAVIOURS AND TIPS

Prevent anticompetitive cooperation with competitors

- Avoid entering into an anticompetitive agreement of any kind – oral or written – with a competitor
- Always avoid sharing commercially sensitive information with competitors, even if not in a professional context
- Leave any meeting with competitors if someone starts a discussion regarding the allocation of customers or regions, prices or other matters that may violate Antitrust laws

Never abuse a dominant market position

- Never apply discriminatory conditions to different customers unless it is economically justifiable
- Never grant loyalty rebates or discounts which have the effect of tying a customer

Deal with transactions involving the acquisition of significant governance rights in third party undertakings

- Do proper Antitrust due diligence and seek appropriate advice from Compliance before starting any transactions
- Notify the transaction to the competent antitrust authority (where required)

Employees' voices

We have to avoid anticompetitive alignments with competitors.

During a trade association meeting, a competitor started talking about its future prices.
I immediately left the meeting and ensured that my departure was placed on record, as I understood that such discussion was inappropriate according to Antitrust rules.

Market Integrity

Everyone at UniCredit who is engaged either in proprietary trading or in the execution of client orders is expected to follow specific rules aimed at protecting market transparency and integrity.



Employees must not engage in practices that distort prices or artificially inflate trading volume with the intent of misleading market participants. **Market manipulation** is a criminal offence in every relevant jurisdiction.

Taking personal advantage of **inside information** is another serious offence. Employees who possess information of a precise nature, which has not been made public, relating, directly or indirectly, to one or more listed financial instruments (or relevant issuers), and which, if made public, would be likely to have a significant effect on their market prices, must not act (disclose or use them to execute transactions for personal or other interest) or cause others to act on the information.

As a general principle, employees cannot use client or third-party information acquired in the course of their working activity with UniCredit to execute personal dealings or to obtain any personal benefit. They shall avoid personal investment that might result in reputational risk or conflict with an interest of the Group or entailing the use, abuse or unfair diffusion of confidential information concerning both clients and/or their transactions. Even the appearance that you may be using such information for **personal dealings** is best avoided.

Employees are recommended to trade, to the extent permitted by the applicable law and internal regulations, responsibly and reasonably, according to their financial resources, preferring long-term investments and avoiding speculative trading.

Cryptocurrency trading carries significant risk due to volatility and complexity; it should be avoided except for a limited portion of the employee's financial resources and only through regulated intermediaries and exchanges.

BEHAVIOURS AND TIPS

Prevent leaks of inside information, even through your colleagues

- Inside information should not be discussed on trading floors, in lifts, restaurants, cafes, on public transport or in any other public place where others may overhear it
- Always consider if there is a legitimate business need to know before sharing information, and ensure that any recipient is added to the relevant insider list
- Business activities must be conducted over channels authorized and, where required, recorded by the Group

Inside information can never be used to influence the market, neither to buy nor sell financial instruments

- Inside information can never be employed to gain personal advantage nor to favour friends and family
- Never act on someone else's "hot tips"

Never make personal transactions that may constitute market abuse or provide an undue advantage from a situation of conflict of interest

- Never use information on customers' pending orders ("front-running") or engage in market manipulation. Be sure to avoid speculative behaviours, only trading according to your financial resources
- Make yourself familiar with all the restrictions that apply to you because of your role within the Bank

Employees' voices

"I always archive communications in a tidy way instead of deleting them."

"I always pay attention to unusual questions and carefully review email chains and attachments before forwarding them applying the Azure Information Protection classification of emails and documents."

Anti-Money Laundering, Counter-Terrorist Financing and Financial Sanctions

As a financial institution with banking operations around the world, UniCredit is a responsible member of the international community.

We have no tolerance for knowingly allowing our products or services to be used for a financial crime anywhere in the world.



UniCredit Group is firmly committed to the fight against financial crime. It aims to actively manage the Money Laundering and Terrorism Financing (ML/TF) risk by continuing to enhance the AML programme comprised of robust tests and regular reviews, policies and procedures (periodically tested and reviewed), a strong control environment, careful client selection.

The programme is supported by Compliance initiatives on training and culture and shapes the risk management culture. The strategy includes a risk appetite statement and framework, client acceptance criteria, a dedicated control environment, regulatory strategy, and collaboration with the Authorities.

Enhanced controls are deployed on customers presenting a higher risk of money laundering/terrorism financing.
The Group does not enter into relationships if the risk exposure cannot be properly mitigated.

Each employee is personally responsible for adhering to Group rules and to this commitment through conduct aimed at:

Being alert to and contributing to the fight against all forms of economic crime, including money laundering, terrorist financing and sanctions evasion, regardless of the circumstances or stakeholders involved

Making sure that adequate due diligence and controls are performed in order to know the customers and how they use the Group's products and services

Protecting the Group against money laundering and financial sanctions risk by having an understanding of their customers' usual behaviour (in terms of transactions) as well as of any potentially suspicious business activity

Reporting any suspicious transaction/ relationship or when sanctions risk is detected to Senior Management or to the local Compliance team



As UniCredit's employees, we should never conduct any transaction that may support efforts to launder money or provide financing to terrorists.

UniCredit set up UniCredit's **Know Your Customer** guidelines and other anti-money laundering procedures. While trust plays a major role in our business, we should consider all customers and transactions with a critical eye and always be on the lookout for signs that something may be amiss, being properly equipped to spot trouble before it occurs, to raise concerns and to report suspicions in a timely manner. While our main goal is to serve our customers as best as we can, this does not mean turning a blind eye to any potential criminal activity.

Our people must be familiar with UniCredit's **Financial Sanctions Policy** and with all related regulations, as well as with the control procedures applied within their daily activities. And when financial sanctions change – as they do, from time to time – we must take note of how such changes may affect our business activities.

UniCredit significantly invests in automated solutions to prevent financial sanction breaches. In order to keep UniCredit Group and its customers as safe as possible, it is crucial to support our awareness of financial sanctions risks, which may be non-transparent: detecting them requires a thoughtful approach and full cooperation with the subject matter experts.

BEHAVIOURS AND TIPS

Anticipate potential issues by monitoring how your work activities can affect market integrity

- Ensure that your work activities do not violate internal or external regulations

Identify and assess customers, transactions or actions potentially connected to sanctioned countries, persons or forbidden activities

- Do not rely on historical knowledge of sanctions, always check and adhere to all the policies and internal regulations currently in place
- Contact your local Financial Sanctions team for any clarification you may need

Report any suspicion about anti-money laundering, terrorist financing activities or financial sanctions risk

- Always be vigilant
- Rely on procedures and alerts that might lead you to identify money laundering or other financial crimes
- Assess scrupulously all the available information and raise a report if you suspect that the customer is using the bank for money laundering/terrorism financing
- Sanctions are a complex set of rules, therefore escalate financial sanctions and potential sanction evasion risk to financial sanction experts for analysis, don't rely on past knowledge as sanction restrictions may change

Stay up to date on changes in regulations

- Check periodically for changes in regulations
- Complete all mandatory training on policies, internal and external anti-money laundering (AML) regulations and financial sanctions
- Adhere to the regulators' guidelines in all your work activities
- Remind your colleagues of the anti-money laundering (AML) and Financial Sanctions (FS) systems and controls in place
- Never leave potential financial sanctions risk unaddressed in case such risks come to your knowledge

Employees' voices

"I always keep my eyes open for risks because I never underestimate a risk."

"I once reported the case of a customer who deposited cheques that were clearly disproportionate to his employment status."

Anti-bribery and Anti-corruption

Engaging in bribery or corruption is not just against UniCredit's rules. It is illegal in all jurisdictions and will result in criminal prosecution when exposed. UniCredit has a zero-tolerance approach to colleagues and third parties who give, offer, promise, receive, accept, demand or solicit illegal payments to public officials, customers, co-workers, media representatives or anyone else.



Bribery and corruption risks can arise in a number of areas that we deal with every day – e.g., gifts and business hospitality, interactions with public officials, roadshows, use of third parties, provision of goods and services, hiring practices and acquisitions. You are responsible for preventing, detecting, and reporting bribery and other forms of corruption related to our Bank's business.

Gifts of cash are forbidden. Any business transaction should be undertaken only for legitimate business purposes and not influence future business decisions of outside parties. We shall start or renew business relationships with a third party based on good knowledge about the partner and only if the relationship is based on legitimate purposes.

Similarly, charitable contributions or sponsorships must not be undertaken with the purpose of steering specific business deals to our Group. Likewise, offers of employment cannot be made to influence a business outcome. Lastly, UniCredit's colleagues are not allowed to make political contributions on UniCredit's behalf.

We expect suppliers, contractors, consultants, agents and other business partners to act consistently with the principles and standards set out in this Code.
Before entering into or renewing a business relationship, appropriate due diligence should be performed to assess integrity, reputation and compliance risks.
We do not knowingly engage with third parties whose conduct is inconsistent with our Values, applicable laws or ethical standards.

BEHAVIOURS AND TIPS

Do not give, offer, promise, receive, accept, demand or solicit payments or gifts for personal benefit

- Always operate according to the highest standards of integrity, ethics and professionalism
- Should you have doubts about whether to give or accept a gift or not, check the applicable policies or consult your manager
- Avoid personal transactions that could potentially be construed as acts of corruption
- Use extra care when interacting with public officials. This includes employees of state-owned enterprises. Many countries, states and local jurisdictions have limits on what gifts and other things of value can be offered to these parties

Report unacceptable behaviours to your manager without fear of retaliation

- Be confident when reporting unethical or unlawful behaviours: retaliation is never tolerated
- Maintain and encourage confidentiality to foster an environment where reporting is perceived as the right thing to do, at all times
- Highlight personal situations that might generate conflicts of interest
- Each of us is responsible for detecting and reporting potential or actual fraud. Any activity that you believe reasonably constitutes potential or actual fraud should be reported immediately, regardless of where the conduct occurs and whether it involves employees, clients, counterparties or third parties acting on behalf of UniCredit

Respect and promote anti-corruption standards and policies. Be a good example to your colleagues

- Share your knowledge of anti-corruption rules with others to strengthen the Bank's defences
- Keep yourself up to date on evolutions in regulations and in the wider banking environment
- Help your colleagues by providing advice where necessary

Choose business partners carefully

- Perform appropriate due diligence
- Monitor relationships throughout their lifecycle
- Escalate concerns regarding unethical behaviour
- Avoid relationships that may expose the Group to legal, regulatory or reputational risk

Employees' voices

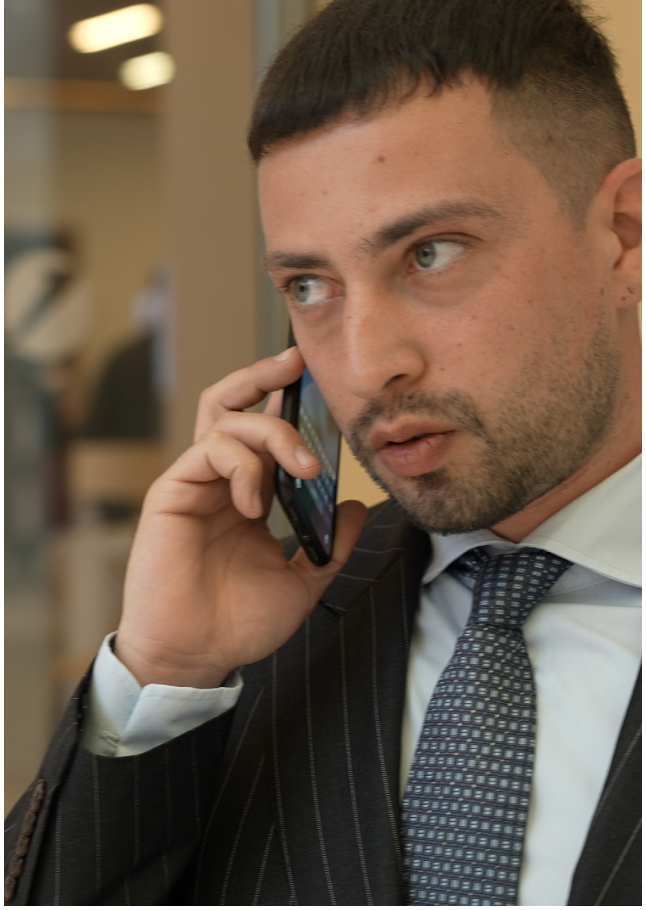
"We often have to avoid becoming too friendly with customers."

"I declined the offer of a concert ticket as I understood it could be interpreted as an act of bribery."

Data Protection

We live in a digital age, and data plays an essential role in the future success of UniCredit. Our Group processes, collects and analyses vast quantities of data and information, transforming them into actionable insights for our business and operational activities.

Our clients and counterparties trust us with their data, and our capacity to protect and use them properly is crucial to work as a credit institution and operate as a financial organisation.



Data confidentiality is very important to UniCredit; everyone in the Group is responsible for protecting our clients' private information as well as our own proprietary data.

Given the tremendous strategic value of these pieces of data, we have developed strict rules governing their use.

BEHAVIOURS AND TIPS

Process customers' personal data in a proper way

- Collect, store and use only the pieces of personal data which are strictly limited to legitimate business purposes (limitation principle)
- Before processing personal data, ask yourself why you need it (need to know principle) and if it is processed in a fair and transparent way for the customer
- Ensure that any information you process is correct, complete and updated (accuracy principle)

Protect customers' data from loss, destruction and unauthorised access or use

- Keep personal and sensitive data confidential; disclose them only to colleagues who have a legitimate business need
- Always adequately protect data before sending emails and documents, especially outside the organisation e.g. by using appropriate encryption when required by internal policies
- Use secured and authorised channels to share customers' information or data

Comply with the Bank's policies on data security

- Use and manage credentials in the required manner
- Use the Bank's email system and devices strictly for purposes permitted by the Bank's policies
- Your corporate email is the only account you are allowed to use to send or receive work materials
- Pay attention to the documents you leave on your desk
- Remember to lock your laptop when leaving your desk, even for short periods
- Pay attention when using corporate tools supporting your daily business activities where recording functionalities are available as no recording of meetings, calls etc. can be activated without explicit prior consent and awareness by the relevant participants

BEHAVIOURS AND TIPS

Promote information security in every situation

- Promote a Culture of cyber security and risk awareness
- Always consider the risk that data can be stolen or manipulated
- Stay alert and immediately involve the Security Functions in case you notice anomalies which might highlight potential hackers' attacks

Protect personal data and report suspected breaches immediately

- Handle personal data carefully, securely and responsibly. Doing so is essential to protecting individuals' privacy and maintaining the trust of our customers, employees and other stakeholders
- Stay alert to personal data breaches, including those resulting from human error, such as information sent to the wrong recipient, incorrect access rights, or lost documents or devices
- Immediately report through the designated internal channel any suspected loss, destruction, alteration, unauthorised disclosure, unauthorised access or unavailability of personal data, even if all facts are not yet known, and follow the applicable Security and Data Protection procedures

Use AI and other digital tools responsibly

- Before using AI, GenAI or other digital tools, ensure that the tool is authorised by the Group for the relevant business purpose and type of information
- Share only the minimum information necessary and use anonymised or pseudonymised data whenever the purpose can be achieved without directly identifiable personal data

Employees' voices

"I always sensitise my customers to the real risks of online scams, and they appreciate my tips."

"I use Bank's tools for business purposes in line with UniCredit Guidelines."

Glossary

AI system: as defined in Article 3(1) of Regulation (EU) 2024/1689 (Artificial Intelligence Act), a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

Antitrust: Legislation which maintains market competition in an open marketplace by regulating anti-competitive behaviour by companies. It prohibits agreements or abusive behaviours of companies which restrict free trade and competition, and ensures that consumers can benefit from low prices, higher-quality products and services, a wide variety of choices, and eventually greater innovation.

Authorities: Local and International Supervisory organizations, Regulators, Public/State authorities like Governments and their representatives, and Judicial Tax authorities.

Anti-Money Laundering: Money laundering is an activity aimed at disguising the illicit origin of criminal proceeds and at creating the appearance that their origin is legitimate.

Bribery and Corruption: Promising, offering, giving, demanding, soliciting, accepting or receiving monetary or other benefits to influence the receivers to secure undue advantage for the giver. UniCredit Group has zero tolerance towards acts of bribery and corruption and prohibits them in any form, not even if these activities should be permitted, tolerated or not prosecuted under the laws in force in the Countries where the Group operates; does not tolerate any conduct involving the offer or acceptance of money or other benefits - directly or indirectly - with the aim of inducing or rewarding the performance of a function/activity or the omission of the same.

Client/Customer: A group or an individual who uses the services of the Group Legal Entities.

Conflicts of Interest: Conflicts of Interest refer to any matter involving the Group, its employees and/or stakeholders, where either the Group or an employee is in a position to exploit a professional or official capacity in some way to obtain an undue advantage, for either Group or personal benefit (also potentially to the detriment of the Group) damaging one or more customers or groups of stakeholders. A conflict of interest may exist even if no unethical or improper act results, but however there is the potential for the appearance of impropriety, which can undermine confidence in the Group.

Data Protection: Refers to the regulatory framework governing the collection, processing, storage and use of data and information in compliance with subject's rights and freedoms and with the appropriate level of confidentiality.

Data Security: Enforcement of technical and organisational security measures to protect the confidentiality, integrity and availability of data.

Employees: All persons linked through an employment contract and all members of the executive, strategic or control bodies of UniCredit/ Group Legal Entity.

Financial Sanctions: Restrictions on dealings with countries, entities and individuals applied, amongst others by the European Union ("EU"), United States ("US") Office of Foreign Assets Control ("OFAC"), United Nations ("UN") and any legislative provision in countries where Group Legal Entities operate or are located.

Group: Or "the Group" refers to UniCredit i.e., UniCredit S.p.A. and the Legal Entities belonging to the Group.

Group Legal Entity: Legal Entity directly or indirectly controlled by UniCredit S.p.A. (hereafter also "Group Company", "Legal Entity", "Company").

High Standards of professional conduct: Principles regarding organisational Values and beliefs, that, when followed, promote conduct such as trust, good behaviour, fairness and integrity

Holding Company: UniCredit S.p.A. (hereafter also UniCredit).

Human Rights: fundamental rights and freedoms inherent to all individuals, including dignity, equality, non-discrimination, privacy, freedom of expression, fair and safe working conditions and protection from harassment, exploitation, forced labour and child labour. Respect for Human Rights requires UniCredit/ Group Legal Entities and Employees to prevent, mitigate and address any actual or potential adverse impact on employees, customers, suppliers, communities and other stakeholders.

Know Your Customer: The due diligence that UniCredit/ Group Legal Entity must perform to identify its customers and ascertain relevant information pertinent to doing financial business with them.

Market Abuse and Market Manipulation: Any behaviour which occurs in relation to investments admitted to trading on a market (or in respect of which a request for listing has been made) and which involves insider trading, improper disclosure of inside information, misuse of information, manipulating transactions, manipulating devices, disseminating information likely to give a false or misleading impression or misleading behaviours or market distortion. Market Abuse can be both a criminal and civil offence.

Mis-selling: Deliberate, reckless, or negligent sale of products or services in circumstances where the potential client is misled about the product characteristics, or the product or service is unsuitable for the client's needs.

Mobbing: Repeated and intentional behaviors that undermine a person's dignity, well-being, or professional reputation in the workplace. Examples include: spreading false information or rumors, violating an individual's privacy, assigning meaningless tasks or unjustifiably removing responsibilities, verbal abuse or humiliation, threats of physical violence, social exclusion, and persistent, unfair criticism of a person's work performance. Mobbing can occur both between individuals at different hierarchical levels and among colleagues at the same organizational level.

Political Donations: Any donation on behalf of /in the name of UniCredit/ Group Legal Entity, made in cash or in kind, to support a political cause. Donations in kind can include gifts of property or services, advertising or promotional activities endorsing a political party, the purchase of tickets to fundraising events, donations to research organizations with close associations with a political party and the release of employees without pay to undertake political campaigning or to stand for office.

Social Media: online platforms, applications and digital communication channels that allow users to create, publish, share or exchange information, opinions, images, videos or other content. The use of Social Media may affect UniCredit's reputation, customers' trust, business relationships, confidentiality, data protection and information security. Unless specifically authorized, Employees must not speak on behalf of UniCredit/ Group Legal Entities or present personal opinions as the Group's official position.

Terrorist Financing: Means the provision or collection of funds, carried out by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out acts of terrorism or to provide support for individuals or groups of individuals looking to carry out these acts.

Unacceptable Behaviours: Action or inaction during work or related to it, and in relation with UniCredit stakeholders, that is or could be harmful to, or jeopardise the Group and/or its employees, including conduct that is:

- Illegal, unfair or unethical (outside of what is considered right for the industry we operate in, a behaviour which can deliberately disadvantage one or many stakeholders)
- A breach of laws and regulations
- A failure to comply with internal rules

UniCredit Stakeholders: Customers, employees, investors, regulators, communities of UniCredit and its belonging companies.