THE MAGNUM® ICE CREAM COMPANY

Our Code of Business Integrity

Life tastes better with ice cream.
And integrity is always in our recipe.
Without it, our business melts!

Welcome **to Our Code of Business Integrity (Our Code)**

CEO Statement

"We create and spread joy by living Our Business Integrity Principles – being honest, respectful, fair, caring, innovative, and collaborative. Only with integrity can we succeed."

Living Our Business Integrity Principles

As we embark on our exciting journey as a stand-alone company, we affirm our commitment to always do business with Integrity. We share a responsibility to foster a culture of trust – both within The Magnum Ice Cream Company (TMICC) and in all of the external communities we engage.

This Code sets out the principles that govern our conduct – individually and collectively. Following these principles ensures that the people who work with us feel confident to engage in courageous conversations, to make the right decisions even when difficult, and to Speak Up when something is not right. Please be sure to read the complete Code, including our Code Policies.

These principles protect our people, our property, our reputation, the communities in which we operate, our customers, and our partners. They keep us honest and enable us to deliver results of which we can be proud. **Our Code** cannot cover every single situation you may encounter, but when you are guided by **Our Business Integrity Principles** – you will know what to do. And if you do not, just ask. You are not alone.

Peter

Our **Business Integrity Principles**

Each of us makes life taste better with ice cream. **Respect, Fairness, Honesty, Care, Innovation** and **Collaboration** are essential to our recipe – without them, our success melts.

Our Business Integrity Principles:

Respect

We treat each other, our consumers, our customers, our business partners, and our communities with respect and dignity;

Fairness

We follow the law and act fairly;

Honesty

We are ethical and honest, approaching each situation with integrity and not taking TMICC's opportunities for our personal benefit;

Care

We care for and protect our people, our assets, our confidential information, and our planet;

Innovation

We develop new products and use new technologies that give our consumers more to love, without compromising our high standards for quality and safety;

Collaboration

We rely on the many resources across TMICC to drive the business, answer questions, or raise concerns. We are all partners.

We win **when we live Our Business Integrity Principles and do business the right way**.

Our Code and the related Code Policies explain each of Our Business Integrity Principles. Following them makes TMICC a welcoming workplace, helps prevent injuries, ensures legal compliance, safeguards our reputation, and secures the trust of our people and customers.

We take **Our Code** seriously, and breaching it can lead to consequences, including disciplinary action and termination.

What must **I do?**

- **Understand and comply** with Our Code and Code Policies. The Board and Executive Committee will not criticise me for loss of business caused by complying with Our Code.
- **Complete** mandatory training.
- **Seek** guidance from my Line Manager or Business Integrity Officer if unsure about how to interpret Our Code, Code Policies or behaviours.
- **Follow** the laws of the countries where we do business. Ignorance is not an excuse.
- **Report** breaches (actual or potential) of Our Code or Code Policies honestly and in good faith. Failing to Speak Up is a violation of Our Code.
- **Support** those who report concerns or breaches, taking them seriously, keeping them confidential, and making sure no one is punished for speaking up.
- **Ask** questions and make the disclosures required by Our Code and Code Policies.
- **Cooperate** fully, truthfully and promptly with any investigations or audits by TMICC. Answer questions, share documents and information, and make devices and data available. Do not change or discard any relevant information, especially when subject to a legal hold or other request from Legal.
- **Consult** with Legal when negotiating a contract, working with government agencies, onboarding a third party, evaluating obligations under applicable laws, and purchasing products that may be subject to trade controls or sanctions.

As a Manager or Team Leader, I must**:**

- **Lead** by example, demonstrating integrity in everything I do.
- **Ensure** all team members have read and completed training on Our Code and Code Policies.
- **Collaborate** with my Business Integrity Officer to address concerns, ensuring timely and appropriate action is taken.

Respect

Life tastes better with Respect.

Respect means treating each other, our consumers, customers, business partners and competitors as we want to be treated – like creating an environment where everyone feels comfortable to share ideas, even if different from yours. Every voice and perspective matters, and everyone has the right to respect, dignity and fair treatment. We respect employees' rights to form or join legally recognised unions or other representative bodies and engage in constructive dialogue.

Human Rights

- We respect Human Rights. We aim to provide a living wage and have zero tolerance for forced labour in any form – including compulsory, trafficked or child labour.

Health, Safety and Security

- We are committed to creating a safe, supportive and respectful workplace that protects the occupational health, safety, security and dignity of our employees. We foster a workplace atmosphere that prioritises psychological safety and promotes a learner mindset. We strive towards achieving zero harm to people, showing respect to our neighbours and actively contributing to communities we serve.

Diversity, Equity and Inclusion

- We strive to create an environment of collective belonging, where everyone feels valued for their unique characteristics. We believe our employees must represent a full range of ideas, experiences and backgrounds. We engage and reward every employee equitably, based on their unique contributions.

Discrimination and Harassment

- We are committed to creating an environment where all voices can be heard, free from discrimination of any kind. This includes discrimination based on race, age, role, gender, gender identity, colour, religion, country of origin, sexual orientation, marital status, dependants, disability, social class, political views or any other class protected by law.
- We have zero tolerance for sexual harassment, discrimination based on protected characteristics, harassment, bullying or any offensive behaviour whether direct or indirect. This includes inappropriate jokes, lewd comments, sexual images, community exclusion, intimidation, bullying, malicious acts, violence or insulting behaviour of any kind.
- We provide a transparent, confidential and fair process for raising concerns or reporting unfair or discriminatory treatment, and we do not tolerate any form of retaliation against those who Speak Up.

What does Respect look like?

Discrimination and Harassment

- An employee repeatedly interrupts and demeans a colleague in a meeting, dismissing her as being uninformed based on her race and gender. This unprofessional, offensive, and intimidating conduct is **not tolerated.** It undermines human dignity and violates our commitment to an environment free from bullying and discrimination. You **report** via a Speak Up channel.
- A colleague makes a sexual joke about another employee's appearance. You **report** this conduct via the Speak Up channels immediately, ensuring the workplace remains safe and inclusive.

Health, Safety and Security

- You find exposed wiring on a factory floor. You **report** it and have it fixed immediately to prevent an accident or injury.

Diversity, Equity and Inclusion

- While interviewing candidates for a vacant role, you ensure a **fair** and **equitable** process by asking all candidates similar core questions and valuing diverse backgrounds that strengthen collaboration and innovation.

Fairness

Life tastes better with Fairness**.**

Fairness **means playing by the rules and acting with integrity.** We act strategically and competitively, but always within the bounds of the law.

Anti-Bribery and Anti-Corruption

- We do not offer, give, accept or request benefits of any type, including gifts, hospitality, donations or sponsorships, that are intended to inappropriately influence decisions or that are outside policy limits.

Anti-Money Laundering, Economic Sanctions, and Trade Controls

- We do not facilitate the laundering of money and do not do business with any person or company subject to economic sanctions. We conduct business in compliance with all relevant trade controls and do not engage in unlawful boycotts.
  - **To ensure** TMICC is not working with any criminal entities who are trying to use legitimate business with us to clean their money from criminal activities, we must conduct due diligence on the third parties with whom we work to learn about their reputations, business experience, and beneficial owners and directors.
  - **Trade** restrictions apply to the shipment or transmission of goods (including raw materials and packing, finished products, equipment, promotional and marketing items), services, technology and money across international borders.
  - **Anti-boycott** laws prohibit companies from participating in, or cooperating with, an international boycott that is not approved or sanctioned by the U.S. or E.U.
  - **Economic** sanctions restrict the countries and people with whom we do business. Violating sanctions laws may result in significant fines and reputational harm.

Fair Competition

- We compete fairly and comply with all competition laws, refusing to engage in any kind of anti competitive practice. We never collude with competitors or other third parties to limit competition.

Political Activities and Donations

- We do not support political parties or make political donations, except in our personal capacity. Any personal support of political groups must not affect our work and must not refer to TMICC in any way. TMICC resources – including our time during work hours and our TMICC email – should not be used to support or advance political parties or activities. Any political association could create a perception of a conflict of interest or damage our business because TMICC interacts with different governments as part of our business operations.

Preventing Insider Trading

- We do not trade or encourage others to trade securities when in possession of Inside Information. Using Inside Information to trade or sharing it with others who are not authorised to know the information, is a crime in many countries. Inside Information is information not known to the public that could affect investor choices.

What does Fairness look like?

Anti-Money Laundering, Economic Sanctions and Trade Controls

- Even though qualified and reasonably priced, you **do not** onboard a supplier who is listed on a sanctions database. You **report** the finding to your Line Manager and Legal to evaluate next steps, even if it delays a project.

Fair Competition

- During a bidding process, you **do not** seek non public, confidential information about competitors' bids, keeping the competition fair and lawful.

Anti-Bribery and Anti-Corruption

- You **do not** offer to make a significant donation to a charitable organisation, run by a tax official's husband, in exchange for the tax official reducing the company's tax exposure.

Honesty

Life tastes better with Honesty.

Being honest**, doing the right thing, and following the law are non-negotiable**. We may face challenges or difficult choices, but when we approach each situation honestly, the solutions are obvious.

Avoiding Conflicts of Interest

- We avoid even the appearance of a conflict of interest by immediately disclosing when our personal interests or external commitments – whether personal, professional, commercial, social or political- could be perceived as conflicting with TMICC's and might require company preapproval. Disclosures should be made promptly upon becoming aware of the potential conflict of interest and should be submitted through the Speak Up channel.

Accurate Records, Reporting, and Accounting

- We ensure all our records, accounts and reporting are accurate and transparent, and all transactions are based on valid documents – from our travel expenses, to our emails with our colleagues, to contracts with third parties. We do not tolerate deception or fraud. Accurate financial records and business information are essential for good decision-making, meeting legal and regulatory obligations and maintaining trust.

Company Purchasing

- We spend responsibly and wisely when purchasing services and materials, ensuring every decision reflects our business priorities and supports quality, safety, innovation, sustainability and the long-term interests of TMICC. We conduct diligence on third-party partners and enter into written contracts to protect TMICC's assets.

Gifts, Hospitality & Sponsorship Guidelines

- TMICC may provide (and TMICC employees may accept) reasonably priced gifts, valued at 30 euros and under, on limited occasions.
- TMICC may sponsor charitable events or otherwise support charitable causes, provided the charities meet TMICC's standards and no improper benefit will be provided to TMICC in exchange for the charitable donation. Disclose the gifts, hospitality, and sponsorships through the Speak Up channels.

What does Honesty look like?

Accurate Records, Reporting, and Accounting

- You lost a receipt for a reimbursable expense. **Do not** submit a receipt for a non-reimbursable expense in its place. Be **honest** and provide the details for the appropriate expense.

Company Purchasing

- You are negotiating a purchase for TMICC. You **do not** reveal the maximum price TMICC is willing to pay, but you **do not** misrepresent facts to gain an improper advantage. You can be strategic in negotiating and advocating for TMICC, while still being honest.

Avoiding Conflicts of Interest

- You notice scrap metal set aside for recycling. Your brother's company could put the scrap to good use. You **do not** take the scrap until you ask your manager for approval and evaluate whether a Conflicts of Interest disclosure is necessary.

Gifts, Hospitality & Sponsorship Guidelines

- While evaluating proposals from prospective suppliers, you receive a luxury gift basket from one of the suppliers. You contact BI to **disclose** the gift and to determine next steps.

Care

Life tastes better with Care**.**

We embody Care **every day and in many ways**, including by protecting individual privacy, our reputation, our assets, and our planet.

Protecting Technology, Personal Data and Privacy

- We are committed to respecting the privacy and protecting the personal data of all individuals with whom we work. We care about people's rights and are accountable for protecting their data in compliance with applicable privacy and data protection laws. We ensure all TMICC's digital assets are secure, properly maintained and used only for appropriate work purposes. We protect all forms of TMICC information by classifying, storing, securing, sharing, updating and deleting it in line with our standards and relevant laws, including privacy, security, employment and data retention.

Protecting Physical, Financial and IP Assets

- We protect TMICC's assets, guarding them from fraud and theft and approving only activities within our personal limits. We safeguard TMICC's intellectual property by ensuring our brands and innovations are protected. We respect valid third-party intellectual property rights by obtaining the relevant licences and approvals.

Protecting the Environment

- We work to reduce our environmental impact and to move towards net zero emissions across our own value chain and operations. We source key commodities responsibly and reduce plastic pollution. Through our commitment to environmental compliance, we prevent and reduce pollutants from entering air, land and water. We report our sustainability goals accurately and work diligently to achieve them, consistently with our **Environmental Standard**.

External Engagements and Communications

- We protect TMICC's reputation by ensuring we are trained and approved before speaking to brokers, analysts, shareholders, media, government, NGOs, regulators and trade associations. We post about TMICC on social media truthfully, responsibly and consistently with TMICC's policies.

What does Care **look like?**

Protecting Technology, Personal Data and Privacy

- As an HR professional, you have access to payroll records and bank details. You use this information **strictly** for intended purposes, store it **securely**, and **only** share it with authorised colleagues.

External Engagement and Communications

- An industry journalist contacts you on LinkedIn, asking for your views on TMICC's latest financial results. Instead of replying to the question, you direct them to the **Media Communications Team** because you are not cleared to speak externally.

Protecting Physical, Financial and IP Assets

- You are negotiating a major supplier contract. Before signing anything, you bring **Legal** in to review terms and ensure compliance with our policies.

Innovation

Life tastes better with Innovation**.**

Innovation **is how we grow and create real magic** – developing new products and using new technologies that give our consumers more to love, while collaborating with external partners, bringing fun and disruptive solutions to market and building sustainable ecosystems. We never lose sight of our obligation to ensure product safety and quality and to act responsibly while innovating.

Product Safety and Quality

- Food **safety and quality are non-negotiable**. We design, make and sell products based on sound science, technology and responsible innovation, applying rigorous safety and quality standards, aligned with aligned with GFSI standards, HACCP and science-led systems. We run robust Food Fraud and Food Defence programs, aim to continuously improve, and deliver superior quality to benefit consumers and customers. We invest in training and communication, partner with suppliers, regulators and customers to uphold food integrity.

Responsible Sourcing and Partnering

- We select and work only with partners who can uphold standards consistent with our own commitment. Working with the best partners supports our future growth.

Responsible Risk Management

- We identify, assess, and manage the risks relevant to our roles, recognising that we are a part of something bigger than ourselves. Risk management is essential to our ability to deliver on our strategy and long-term goals. Understanding and addressing risks – from global to local, strategic to operational – helps us make better decisions, comply with regulations, protect our business, and create value. For more guidance, contact the Global Risk and Controls Director or the Risk Management Hub for the **Risk Standard**.

Responsible Marketing

- We sell products that are accurately and transparently labelled, advertised and communicated. We conduct marketing activities and research in line with societal expectations. Our marketing has the power to influence society, so it must be conducted thoughtfully, respectfully, and consistently with applicable marketing laws. For more guidance, refer to TMICC's **Internal Marketing and Brand Guidelines** or speak to your Line Manager.

What does Innovation **look like?**

Product Safety and Quality

- When developing eco-friendly packaging, you partner with materials experts to ensure durability and food safety aren't compromised. The innovation reduces environmental impact, while protecting consumers, demonstrating that **safety** and **sustainability** can go hand in hand with innovation.

Responsible Marketing

- Our marketing avoids exaggerated health claims. We are **upfront** about sugar content to ensure consumers can make **informed** choices and our brands maintain credibility.

Life tastes better with Innovation.

Collaboration

Life tastes better with Collaboration**.**

You must work with TMICC's experts **to reduce risk, ensure compliance with applicable laws, and drive the business in strategic and innovative ways.** Rely on the many resources available to answer your questions and to support your work. Raise your concerns about a potential or actual breach of Our Code through any of the various available channels.

Legal Consultation

It's important that you seek advice to resolve questions, abide by laws and regulations, and protect TMICC from potential claims, financial losses and reputational damage. You must follow Legal's advice.

I must seek guidance from a Legal Business Partner for:

- Commercial contracts, leases, licenses and transactions.
- Onboarding key third parties where red flags exist.
- Legal or regulatory action, such as employment disputes, contractual disagreements and regulatory inquiries.
- Communication with government or regulatory bodies.
- Competition law matters.
- Press communications that impact TMICC's reputation, create legal liability or contain "inside" or "price sensitive" information.
- Claims, brands, trademarks and marketing materials.
- Employment-related issues, including non-compete obligations, non-routine contract terms, disputes and terminations.
- Product safety, tampering or counterfeiting.
- Legal or governance structures.
- Bribery, corruption, sanctions, money laundering or trade control concerns, including questions about the origin of raw materials, limitations on purchasing or selling products in certain countries, and indirect sales.

If you receive a request from law enforcement or a regulator to participate in a government investigation (i.e. a subpoena for documents or information), promptly notify Legal, unless the request specifically prohibits sharing any information even with Legal. Legal will ensure the request is addressed. You must cooperate fully and respond honestly.

Ask for support.

At TMICC, we will handle issues and concerns with care and attention. **Caring** for each other, which includes **challenging** behaviours or actions that go against our values, is a fundamental part of our Ice Cream Way cultural identity.

Many resources are available:

- **Your Line Manager and / or Team:** For questions related to your job responsibilities, or interactions within your team, handling these directly with your manager or team is often the best place to start.
- **Human Resources:** Your HR team can provide support for issues that are not appropriate for, or you are uncomfortable raising with, your manager. Questions related to your place of work, treatment at work (for yourself or others) can be directed to your local HR team.
- **Business Integrity Officers:** If your question relates to Our Code or your understanding of Our Code, contact a Business Integrity Officer or use the **Speak Up** hotline or website.
- For questions relating to a **specific subject area**, contact the team mentioned in the relevant Code Policy.

Report

- **To report** a potential or actual breach of Our Code, use the **Speak Up** hotline or website.

Living Our Code with Integrity

Acting with Integrity **in everything we do is how we bring Our Code to life.** It's how we demonstrate Respect, Fairness, Honesty, Care, Innovation and Collaboration in our roles at TMICC.

This is what our actions look like when we live Our Code with Integrity:

- Treating people with respect, dignity, and fairness.
- Using TMICC assets only for TMICC business and in line with TMICC's policies.
- Keeping business records in line with legal and policy requirements or as instructed, including for audits, litigation or regulatory investigations.
- Recording all transactions accurately, completely, and on time. This includes:
  - **Waiting** until there is an approved purchase order (PO) before making financial commitments or starting any work on the related project or order. Any exceptions must be approved by Supplier Operations first.
  - **Not** splitting purchase orders, unless there is a valid business reason that has been approved by Supplier Operations.
  - **Never** receipting purchase orders, unless the goods or services have been delivered.
  - **Always** reviewing the details of a purchase order, as well as expense reports, before submitting or approving. I can contact our Local PO Helpdesk for more guidance.
- Ensuring financial budgets, where relevant to my role, including trade discounts and rebates, are monitored and reviewed.
- Conducting only business activities I am approved to carry out and ensuring such activities are legitimate and supported by proper documentation.
- Ensuring transactions I approve are within the limits set out in the **Global Schedule of Authorities**, are legitimate and based on valid documentation.
- Consulting with Legal as a strategic partner.
- Disclosing potential and actual conflicts of interest, as well as gifts and hospitality received from a third party.
- Obtaining approvals before offering or accepting gifts or hospitality.
- Informing my Business Integrity Officer and Head of Finance of any suspected fraud, tax evasion or accounting issues; any red flags raised by the behaviour of a business partner or other third party; and any requests for **Facilitation Payments**.
- Understanding that devices used for TMICC business are subject to review and collection in internal and government reviews, subject to applicable laws.
- Cooperating with requests for information and data from TMICC.
- Never artificially inflating or shifting sales or profits between accounting periods.
- Ensure the environmental and social impacts of a decision and associated risks are transparent, understood, and in line with our commitments.

As a Finance professional, I will also:

- Proactively comply with accounting, auditing, tax and environmental procedures, processes, standards and laws on a daily basis.
- Follow all applicable external reporting standards and regulations and the **internal accounting policy manual**, carefully documenting the assumptions that underpin accounting records.
- Demonstrate understanding of TMICC's **Financial Rules and Standards**.
- Ensure there are no hidden or unrecorded accounts, funds or assets.

Facilitation Payments

- Unofficial payments made to government officers to secure or speed up the performance of a routine action they are required to provide anyway. Facilitation payments are illegal in most countries, although a small number provide exceptions under specific circumstances.

Our Business Integrity Principles **and** Code Policies

Business Integrity Principles

- **Respect**
- **Fairness**
- **Honesty**
- **Care**
- **Innovation**
- **Collaboration**
  - **Legal Consultation**
  - **Asking For Help**
  - **Speak Up Channels**

Application

- **Living Our Code with Integrity**

Code Policies

- **Avoiding Conflicts of Interest**
- **Anti-Bribery and Anti-Corruption**
- **Anti-Money Laundering, Trade Controls and Economic Sanctions**
- **Fair Competition**
- **Share Dealing and Preventing Insider Trading**
- **Protecting Physical, Financial, IT and IP Assets**
- **Privacy and Data Protection**
- **Responsible Sourcing and Business Partnering**
- **External Engagements and Communication**
- **Health, Safety and Security**
- **Product Safety and Quality**

Avoiding Conflicts of Interest

Part 1/2

We avoid even the appearance of a conflict of interest by immediately disclosing when our personal interests or external commitments could be perceived as conflicting with TMICC's. Disclosures should be made promptly upon becoming aware of the potential conflict of interest and should be submitted through the Speak Up channel. This includes gifts, hospitality, charitable donations, and sponsorships where you have a relationship with the other party.

Why is it important?

Conflicts of interest arise when we allow our actual, perceived, or potential personal, familial, financial, or non-financial interests to affect our objectivity when performing our job. Conflicts of interest can impact our reputation, our business and our people negatively. A perceived conflict of interest can be just as damaging to our reputation, to trust amongst colleagues, and to morale as an actual conflict of interest.

What must I do?

- Evaluate whether my situation may create a potential or actual conflict of interest by viewing it from TMICC's perspective.
- Report any actual, perceived, or potential conflicts of interest to Business Integrity, including when I:
  - **Receive** or direct money, gifts or other benefits from TMICC through a third party, including a for-profit or non-profit entity, with which I am affiliated.
  - **Hire**, manage, direct business to, or influence the workload, assessment, approvals or rewards of a **Close Personal Contact***.
  - **Have** a **Close Personal Contact*** who is **a Public Official**** with decision-making authority that could impact TMICC's business.
  - **Have** a personal interest – or have a **Close Personal Contact*** with an interest – in the business of TMICC competitors or third parties who work with TMICC, such as an investment in or financial arrangement with a TMICC competitor or with a third-party bidding on or performing work for TMICC, working on products that compete with TMICC or working for a company that takes positions adverse to TMICC.
    - **Investments** through publicly traded pension, index, or tracker funds, where I do not own 5% or more of a TMICC competitor or a company doing business with TMICC does not need to be reported.
  - **Am presented** with an opportunity to potentially profit from TMICC resources or information outside of my normal role, such as from the sale of expired products or by bidding on an opportunity where TMICC is also bidding, or by becoming a franchisee.
  - **Am engaged** in political activity in a personal capacity that may reflect on TMICC or potentially impact TMICC.
  - **Am engaged** in retaining, monitoring, or investigating a third-party in which I, or a Close Personal Contact, have a financial interest.
    - **Financial interest** includes receiving anything of value from that third-party.

*Close Personal Contact includes a parent, grandparent, step-parent, child, step-child, grandchild, sibling, step-sibling, aunt, uncle, first cousin, the spouse or significant other of any such family member, a romantic partner, a close friend, or someone with whom I share a residence or a financial interest.
**A Public Official is an employee of local, national or international government agencies, or government-owned or controlled entities. This term also includes a member of a political party or royal family, a candidate for political office, and an employee of a public international organisation, such as the UN, WTO or UNICEF.

Avoiding Conflicts of Interest

Part 2/2

What must I do?

- Ensure Business Integrity has cleared my conflict of interest before starting or continuing with the potentially conflicting activity.
- Be mindful that external commitments, like second jobs or serving on a board, do not impact my work or performance for TMICC.
    - **Seek** approval before accepting external commitments, including second jobs or a financial interest in a franchise or a supplier.
- Protect confidential and commercially sensitive information about TMICC and our current or potential competitors, including when my TMICC employment ends.
- Ensure that my non-financial interests, including personal beliefs and political views, do not take precedence over TMICC's lawful and ethical expectations.
- Seek approval before representing TMICC in any economic, industry or social advisory groups that are set up by governments.
- Position TMICC for success by performing my job with integrity and with loyalty to TMICC.
- Do not take or divert TMICC business opportunities to others.
- Request approval from Business Integrity before hiring former Public Officials or taking personal directorships in other organisations.

What do I need to know about directorships?

Disclosure is needed if I am:

- Interested in taking up a directorship, whether commercial or not-for-profit, including roles in trade associations or roles for public bodies.
- A new employee who holds directorships that were not disclosed during my recruitment process.

This disclosure requirement excludes roles on school boards, governing positions in amateur sporting or recreational groups, and directors of property / housing blocks in which an employee lives.

I need approval from the Chief Business Integrity Officer before becoming a director of any publicly listed company.

Where do I go for more information?

Business Integrity Officer and Conflicts of Interest Disclosure tool.

Make disclosures, or seek approval or guidance at:
http://uk.core.resolver.com

Anti-Bribery and Anti-Corruption

Part 1/2

We do not offer, give, accept or request benefits of any type, including gifts, hospitality, donations or sponsorships, that are intended to inappropriately influence decisions or that are outside policy limits.

Why is it important?

Bribery and corruption harm communities, damage our reputation, undermine trust, are illegal, and may result in severe consequences, including fines, imprisonment and loss of business. Excessive, unreasonable or frequent gifts and hospitality expenses give the appearance that our success is being bought, rather than built. Acting with integrity in all interactions helps protect both me and TMICC.

What must I do?

- Do not offer or give anything of value or any advantages, including **Facilitation Payments**, to anyone, which are, or give the impression that they are, intended to improperly influence decisions about TMICC or to give TMICC an improper advantage.
  - **An exception** applies if my freedom or physical safety is in danger. I must disclose those circumstances to Business Integrity as soon as practical after the threat ends.
  - **A bribe** is not allowed even if I pay for it with my own money.
  - **Facilitation Payments** are small amounts made to a low-level government employee to secure or expedite the performance of a routine or necessary action to which TMICC is entitled. They are not allowed, except in rare circumstances pre-approved by the Chief Business Integrity Officer.
- Maintain integrity by refusing bribes, anything of value, or any advantages from any **third party*** that could influence improperly the way TMICC makes decisions or my own objectivity and impartiality.
- Follow all TMICC **third party*** and finance processes, such as those for onboarding third parties, conducting diligence on third parties, raising purchase orders, and offering / receiving discounts.
- Include in **third party*** contracts clauses that advise third parties of their obligations to comply with applicable anti-corruption and anti-bribery laws, give TMICC rights to audit the third parties' books and records related to their TMICC business, require the third parties to cooperate fully and truthfully in any audit or investigation by TMICC, and allow TMICC the right to terminate the contract if we have a reasonable belief that the **third party*** is engaged in corruption, bribery, conflicts of interest or other fraud.

*A third party is any entity with whom we have a financial relationship. Certain third parties create greater risk than others, and our processes are risk-based.

Anti-Bribery and Anti-Corruption

Part 2/2

Our Gifts and Hospitality Standard

- **Report** any suspected or actual breaches as set out in Our Code, including any requests for a bribe or other benefit by any Public Official* or other third party with whom TMICC does business.
- Ensure all gifts and hospitality are for legitimate business purposes, proportionate, occasional, and within limits, whilst avoiding cash or equivalents, like gift cards, loans, shares, hotels or other travel benefits.
  - **Use** reasonably priced TMICC-branded gifts or ice-cream coupons (within Gift limits) in lieu of other gifts.
- Report any gifts and hospitality that are above these limits to the Business Integrity Team.
- Decline any gift or hospitality that is outside of the limits set in this Gifts and Hospitality Standard, unless an exception has been approved through the **Disclosure Tool**.

Gifts	Hospitality		
ALL WL	WL 1 & 2	WL 3 & 4	WL 5+
€30	€60	€120	€300

Where do I go for more information**?**

Business Integrity Officer, Global Policy Portal, or Gifts or Hospitality Disclosure Tool.

*A Public Official is an employee of local, national or international government agencies, or government-owned or controlled entities. This term also includes a member of a political party or royal family, a candidate for political office, and an employee of a public international organisation, such as the UN, WTO or UNICEF.

Anti-Money Laundering, Trade Controls and Economic Sanctions

Part 1/2

We do not do business with criminal organisations or with any person or company subject to economic sanctions. We conduct business in compliance with all relevant trade controls, including rules related to boycotts. **Trade restrictions or export controls** apply to the shipment or transmission of goods (including raw materials and packing, finished products, equipment, promotional and marketing items), services, technology and money across international borders. **Anti-boycott** laws prohibit companies from participating in, or cooperating with, an international boycott that is not approved or sanctioned. **Sanctions** come in many forms including: **Financial Sanctions** which prohibit contracting with or paying or receiving money from a person or company listed on a country's sanctions list, and **Trade Sanctions** which restrict the movement of goods to or from sanctioned countries.

Why is it important?

Violating money laundering, trade controls or sanctions laws can result in serious legal consequences, including imprisonment, fines and bans on the sales of our products. As a global company, shipping and sourcing products around the world, we must be aware of the limitations imposed by these laws.

What must I do?

- Conduct due diligence on third parties before onboarding to (1) learn about their reputations, business experience, origin of goods, and beneficial owners and directors and (2) ensure TMICC is not working with any criminal entities who are trying to use legitimate business with us to clean their money from criminal activities.
  - **Ensure** third-party screening is conducted and any issues are remediated in full before contracts are signed and transactions occur; do not assume this has been done – always confirm with Procurement, Supply Chain, Customer Development, and / or Legal.
- Do not transact with any party who is subject to economic sanctions. Follow TMICC processes for onboarding, including verifying third parties are not on sanctions lists before awarding any business, keeping accurate and complete records of transactions, and knowing the background of the third parties with which we are working.
- Notify my Business Unit and Country General Counsel immediately if I suspect a business partner is engaged in any illegal activity, products may be sourced from sanctioned countries or sanctioned third parties or prohibited boycott requests. Typical red flags include unusual or overly complex payment structures, sudden changes in ownership of the third party, inconsistent or incomplete documentation of expenses and experience, resistance to providing required information, or incomplete information about the origin of goods.

Anti-Money Laundering, Trade Controls and Economic Sanctions

Part 2/2

What must I do?

- Obtain prior clearance from my Business Unit and Country General Counsel, plus a senior Finance Manager, before proceeding with any transaction outside normal business terms, such as payments to accounts that do not match the name, country, or currency of the country of the business partner; those made in cash or overpaid; and those split across several bank accounts or purchase orders.
- Do not inform any third party suspected of money laundering that they are under investigation.
- Seek guidance from my Business Integrity Officer when screening outcomes are unclear or where extra scrutiny is needed.
- Disclose to Business Integrity if I need to recuse myself from an Economic Sanctions perspective, for example, if I am a US citizen and prohibited from engaging in a certain transaction.

Where do I go for more information?

Business Integrity Officer, Global Policy Portal or Disclosure Tool.

Fair Competition

Part 1/2

We do not engage in any form of collusion, we compete fairly, and we comply with all competition laws, refusing to engage in any anti-competitive practice.

Why is it important?

We are fully committed to competing vigorously, fairly and in compliance with the law, for the benefit of our consumers and a healthy competitive environment.

Violating competition laws can lead to serious consequences, including large fines, civil damages, criminal sanctions for individuals and damage to TMICC's reputation and relationships.

What must I do?

- Follow and cascade competition law guidance and training to ensure I and my colleagues thoroughly understand, recognise and stay alert to competition law sensitivities.
- Never participate in cartels, even in countries without competition laws.
- Refrain from agreeing, discussing or exchanging information on any of the following, directly or indirectly (i.e., via a customer or a supplier), with competitors unless approved by Legal:
  - **Commercially** sensitive information – including prices or terms of sale; costs or other conditions with third parties; purchasing or other strategies, production, marketing, advertising, sales, recruitment, employment terms, wages or rewards.
  - **Division** or allocation of markets, channels, customers or product lines.
  - **Boycotts** or refusals to deal with certain market players (unless approved by Legal).
  - **Coordination** or allocation of bids or tender quotes.
- Only collect and / or use competitor information from the public domain, and:
  - **Clearly** record the source of competitor information in any internal or external communication and document.
  - **If I acquire** competitor commercially sensitive information unintentionally, notify Legal immediately.
  - **If I want** to collect competitor information beyond the public domain (i.e., for benchmarking), I consult Legal.
- Act with caution when TMICC's market positions are strong, seeking advice from my Legal Business Partner if TMICC's commercial practices could be perceived as abusively excluding competitors or as unfair to customers or suppliers.
- Do not seek to obtain or use information in a way that might violate legal or contractual non-disclosure obligations of third parties or new employees.

Fair Competition

Part 2/2

What must I do?

- Before taking part in a **trade association meeting, industry events, or meetings with competitors**, ensure that:
  - **My Line Manager** approves the activity.
  - **I complete** the required training.
  - **A clear** agenda is shared (by email, in the invite, etc.), including a competition caution (see sample below) that will be read at the start of the meeting and included in the minutes.
  - **Minutes**, which refer to the attendees, purpose, and discussions are circulated after the meeting.
    - **If inappropriate** discussions continue, noticeably leave at once (requesting this be noted in the minutes); report the incident to my Line Manager and Legal immediately.

Sample of Competition Caution:

> All participants at today's meeting must adhere to competition law and shall not enter any discussion, activity or conduct that may breach any applicable competition law. For example, participants shall not discuss or exchange any commercially sensitive information, including non-public information on selling prices and trade terms, revenues, costs, conditions with third parties, or purchasing / production / marketing / advertising / distribution / selling strategies. This applies not only to discussions in formal meetings but also to informal discussions before, during, and after the meeting. Should discussions cover matters that may be problematic under competition laws, the moderator will close the meeting.

What must I do?

In cross-border sales:

- Refrain from taking any action if any of the motivations are to limit cross-border sales within Europe and never complain or comment in a negative way on cross-border sales within Europe, in external or internal communications.

Consult Legal if:

- I want to restrict imports in, or exports to, certain countries in regions other than Europe, to comply with international trade rules.
- I am in doubt on how to apply competition law to a specific situation.
- I want to exchange information or discuss collaboration opportunities with competitors (for example, on joint purchasing, production, R&D, standardisation agreements).
- My discussion or decision may restrict how or where a customer (retailer, distributor, concessionaire, wholesaler, etc.) markets, sells or distributes TMICC products:
- I plan to apply certain commercial practices in markets where TMICC is strong, which may result in an unfair disadvantage of customers or unfairly prevent competitors from entering, remaining or expanding (for example, selling below cost, exclusivity, certain rebates or bonuses).
- I am contacted by, or plan to contact, competition authorities or courts: all such contacts must be coordinated by Legal.

Share Dealing and Preventing Insider Trading

Part 1/3

We do not trade or encourage others to trade securities when in possession of any inside information.

Inside Information is non-public information which would be likely to impact share price if it were to be made public. If I have access to TMICC Inside Information, I will be added to an Insider List and notified. If I am not sure whether information I have is Inside Information, I must behave like it is and / or check with the person who gave me the information.

Why is it important?

Using Inside Information to trade, or sharing it improperly, is a serious disciplinary matter and a criminal offense in many countries, leading to fines, imprisonment and reputational harm. These restrictions apply to Inside Information I learn about TMICC or another publicly traded company with whom TMICC is doing business.

Offenses can occur in many ways, including:

- **Unlawful** disclosure of Inside Information: disclosing Inside Information to any other person, except in the normal exercise of employment.
- **Insider dealing**: using Inside Information to acquire or dispose of (whether for my account or someone else's), directly or indirectly, financial instruments to which the information relates.
- **Market manipulation**: doing anything that gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of, a financial instrument, including entering into a transaction or trade, giving information to the media, or sharing false or misleading information.

As a Director or Senior Manager, I must:

- Take reasonable steps to prevent any dealings in TMICC securities by or on behalf of Close Personal Contact (CPC) with me;
- Advise my CPC that this Policy applies to them;
- Advise my CPCs of the Closed Periods during which they should not deal in TMICC securities; and
- Advise my CPCs that I must get clearance before dealing in TMICC securities.

Share Dealing and Preventing Insider Trading

Part 2/3

Inside Information **Examples:**

- Business results or forecasts.
- Reserves for company debt.
- Major launches and new inventions.
- Significant threatened or potential litigation or claims.
- Cybersecurity incidents.
- M&A, tender offers, JVs, restructuring or divestments.
- Revisions in dividend policy.
- Expansion or reduction of operations.
- Gain or loss of significant customers or suppliers.
- Changes in auditors, Executive Directors or company control.
- Product or Brand defect claims.

What must **I do?**

- **Understand** what is considered Inside Information. It may include information that relates to future, speculative or contingent events not publicly available. Information is not necessarily public merely because it has been discussed in the press or on social media. I should presume that information is non-public, unless I can point to its official release by TMICC, such as by a public filing or press release.
- **Do not** buy or sell TMICC securities (including shares, ADRs and related derivatives and spread bets) for my own account or on anyone else's behalf, or recommend third parties to do so, while I am in possession of Inside Information.
- **Refrain** from sharing Inside Information with anyone not authorised to have it, including other TMICC employees.
- Disclose immediately if I suspect or know Inside Information (1) has been shared with anyone not authorised to have it or (2) is being misused.
- Disclose transactions that may trigger this Policy using these forms

I do not need to disclose transactions when Investing in:

- **A unit** or share in a collective investment undertaking (CIU) in which the exposure to TMICC securities does not exceed 20% of the assets held by the CIU;
- **A financial** instrument which provides exposure to a portfolio of assets in which the exposure to TMICC securities does not exceed 20%;
- If I do not know, and could not know, the investment composition or exposure of such CIU or portfolio of assets in relation to TMICC securities and there is no reason to believe that such exposure is greater than 20%;
- Transactions in TMICC securities executed by managers of a CIU who operate with full discretion and do not need to notify me when executing a transaction.

Share Dealing and Preventing Insider Trading

Part 3/3

What must I do?

- If I am in any doubt about whether I need to seek clearance to deal, I must notify and ask the Company Corporate Secretary for guidance.
- **Contact** the Corporate Secretary for more information, including obligations for persons included in TMICC's Insider List.
- The Insider Lists name all employees and external advisors who have authorised access to TMICC's Inside Information. People on these lists must also comply with the requirements in TMICC's Share Dealing and Disclosure Manuals, available at the Corporate Secretaries' Department.
- **Refrain** from engaging in activities that involve manipulation of publicly listed companies' price or spread of false information.
- **Use** TMICC's information only for legitimate business purposes or as required by law.
- **Report** any concerns about the use of TMICC restricted or Inside Information by any person, including business partners, to my Line Manager or Business Integrity Officer.

What is permitted?

Number of shares which may be sold:

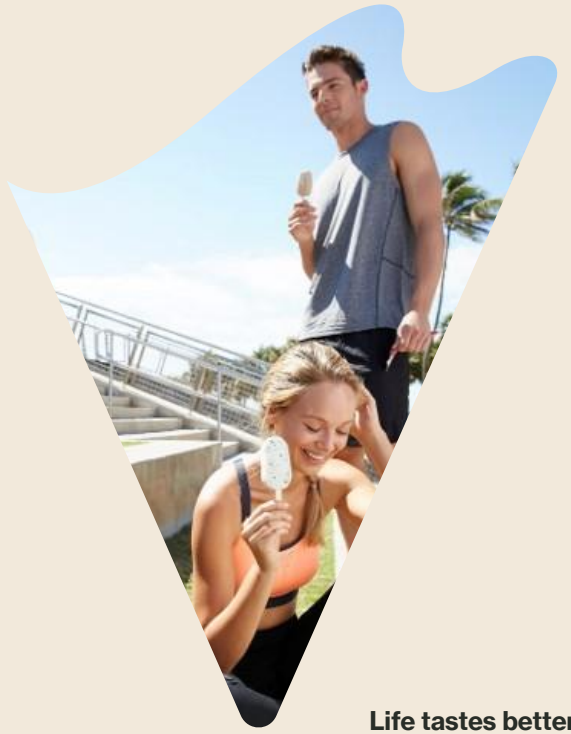
Equity Securities: a WL4 or higher may sell in a three-month period the greater of:

- 1% of the outstanding TMICC securities; or
- The average weekly reported trading volume in the four calendar weeks preceding the transactions.

Debt Securities: a WL4 or higher may sell in a three-month period the greater of:

- The average weekly reported trading volume in the four calendar weeks preceding the sale; or
- 10% of the principal amount of the tranche of debt securities (or 10% of the class of non participatory preferred stock).

Any restricted securities must be held for six months prior to reselling such securities.



Protecting Physical, Financial, IT and IP Assets

Part 1/3

We protect TMICC's assets, guarding them from misuse, fraud and theft and approving only activities within our role and responsibilities. We safeguard TMICC's intellectual property by ensuring our brands and innovations are protected. We respect valid third-party intellectual property rights by obtaining the relevant licences and approvals.

Why is it important?

TMICC's technology and information are vital tools that allow employees and trusted partners to perform their roles effectively. When these assets are misused, stolen, damaged or handled carelessly, the impact can be serious – disrupting operations, breaching legal and privacy obligations, and harming our reputation. By protecting our assets and handling our information with the right level of care and classification, we keep our operations running smoothly, safeguard financial stability, preserve innovation and competitive advantage, protect individual's rights and meet our legal and regulatory obligations.

What must I do?

All assets:

- Handle TMICC's physical assets – for example factory equipment, products, buildings, computers and vehicles – with care, to avoid damage, misuse, or loss.
- Report theft or loss to site SHE Managers promptly.
- Do not remove TMICC assets, except TMICC issued laptops and phones, from any site unless authorised, and do not use TMICC assets inappropriately or for unauthorised personal benefit.
- Identify and manage potential hazards to assets on site, reducing risks to an acceptable level.
- Guard TMICC's financial assets – such as cash, bank accounts and credit cards – against misuse, loss, fraud or theft, and immediately escalate any red flags to my Line Manager.
- Approve financial transactions only within my limits, as defined by my role, and in compliance with the **Global Schedule of Authorities.**
- Address cyber security risks by embedding cyber security standards and controls. This particularly applies if implementing or purchasing technology solutions.
- Beware of cyber security risks on any devices used for TMICC business:
  - **Avoid** opening attachments, unless I know the sender and have verified the accuracy of the email address.
  - **Avoid** visiting websites that may not have adequate security certificates.
  - **Use** multi-factor authentication and strong passwords on devices.

Protecting Physical, Financial, IT and IP Assets

Part 2/3

What must I do?

Intellectual Property (IP):

- Do not use TMICC's IP, except for TMICC's benefit.
- Report suspected counterfeit products or potential IP infringements – such as those related to trademarks, patents, designs, copyrights and domain names – to the Business Group or IP General Counsel.
- Ensure checks and filings are completed for patents, trademarks and other IP rights when launching new brands, sub-brands, products, services or other materials.
- Use contracts with appropriate clauses to protect TMICC's IP when working with third parties.
- Refrain from using valid third-party IP without the appropriate licenses, for example Music, Video, Technology etc. If unsure what is valid, speak with my Legal Business Partner.
- Do not train third party GenAI or any other third party LLM with TMICC IP or confidential information, including trade secrets, designs, patents and trademarks.

Information:

- Classify information, documents, and emails in line with the Information Classification Standard: Public, Internal, Confidential, Restricted.
- Follow the requirements outlined in the Information Handling Standard, which sets out what types of information can be shared with whom. Take personal responsibility for how information is used, shared, stored, protected, and disposed of.
- Share TMICC information only on a need-to-know basis with individuals and authorised third parties for legitimate business purposes, or as required by law.
- Do not forward TMICC information to personal email or storage accounts, sync TMICC data on devices not managed by TMICC or use removable media (i.e. USBs).
- Do not engage in contract negotiations, discuss substantive issues with regulators, address due diligence red flags, or share any non-public TMICC information on unapproved technology or on collaboration and messaging tools (WhatsApp, Signal, etc.).
- Understand that, in accordance with our Business Integrity Principles and applicable laws, all information processed by, or stored on, TMICC-issued or owned systems and equipment (and TMICC information on personal devices) may be monitored, inspected or removed by TMICC without prior notification.

TMICC may monitor, log, diagnose, investigate and assess activity and data including messages and other communications sent, received, and stored on TMICC's network, systems and equipment to the extent permitted by applicable laws, to ensure this policy is being followed and TMICC's technical environment is optimised and risk managed.

Protecting Physical, Financial, IT and IP Assets

Part 3/3

What must I do?

Equipment & technology:

- Use only TMICC-approved technology to share and manage information and take additional care when working in public places.
- Install only approved applications and use only approved services, including Software as a Service and AI.
- Ensure work equipment is used appropriately and kept protected from damage, theft or loss.
- Secure equipment and documents when not in use. Lock any device with a password or PIN when unattended, irrespective of location.
- Do not share TMICC access credentials with anyone, use TMICC passwords anywhere else or use TMICC identities for non-business-related activity.
- Ensure personal use of TMICC technology does not materially impact performance, such as excessive storage or data usage.
- Report any suspected cyber issues or suspicious activity by raising a security incident, such as unauthorised information sharing or unexpected authentication notifications.
- Report lost or stolen devices (TMICC or personal) used to access TMICC information immediately as a security incident.

Malicious activity:

- Do not intentionally access TMICC technology or TMICC information that is not intended for my role, or after leaving TMICC employment.
- Do not disable, bypass or interfere with security controls, for example, browser configuration, anti-virus, privileged access, firewalls or system logs.
- Do not use systems for any illegal activities, or that could cause serious or widespread offence or are associated with violence, terrorism, pornography or insulting content.

If I own, procure or run technology, or manage a third party, what do I need to do?

- Address cyber security risks through the correct application of the Cyber Security Standards and follow the cyber processes detailed on the Cyber Security Zone.

What is the Information Classification Standard?

- Public: Information already available to the general public may be freely distributed.
- Internal: Only shared within TMICC and authorised third parties with a genuine business need.
- Confidential: Only shared on a need-to-know basis with a genuine business need.
- Restricted: Only shared with named individuals who are on the relevant Restricted Information List.

Where do I go for more information?

Chief Information Security Officer, Local SHE Manager or Legal Business Partner, Intellectual Property Standard, Cyber Security Standards, Cyber Security Zone (including to report a Cyber Incident).

Privacy and Data Protection

Part 1/2

We are committed to respecting the privacy of all individuals with whom we work and protecting their personal data in compliance with applicable privacy and data protection laws. **Personal data** is any information that can be used to identify a person either directly or indirectly. We handle personal data responsibly by collecting only what's needed, using it fairly and transparently, keeping it accurate and secure, and only storing it for as long as necessary.

We ensure all TMICC's digital assets are safe, properly maintained and used only for appropriate work purposes. We protect all forms of TMICC information by classifying, storing, securing, sharing, updating and deleting it in line with our standards and relevant laws, including privacy, security, employment and data retention.

Why is it important?

Protecting personal data is fundamental to respecting people and the human right to privacy. It builds trust with our employees, consumers, customers and business partners. It ensures compliance with legal obligations, helping us avoid fines and reputational harm. It safeguards sensitive information from misuse, loss or unauthorised access, and enables individuals to exercise their rights over their own personal data.

What must I do?

- Only collect or access personal data when necessary for my role or business purpose.
- Limit the amount of data I collect to the minimum I need for the specific purpose.
- Use personal data fairly.
- Consider potential harm to individuals when using their data and take steps to mitigate these risks.
- Be transparent with individuals about how their data is used.
- Store personal data securely using approved systems and tools in accordance with our information security policies.
- Keep personal data accurate and up to date.
- Respect individuals' rights (e.g. for access, correction, or deletion) and get consent to use it where necessary (e.g. for e-marketing).
- Complete a **Privacy Risk Assessment** before any new project, campaign, or activity that involves personal data.
- Do not keep personal data longer than needed – delete or anonymise it in accordance with our retention policies.
- Do not put confidential information, including personal data, into publicly available AI tools or on social media, and do not share it with third parties without authorisation and appropriate contract terms, including after my TMICC employment ends.

Privacy and Data Protection

Part 2/2

TMICC has an **obligation to cooperate** with requests from government agencies for information stored on TMICC devices or used for TMICC business. That means that if I receive a request to keep certain information, I must ensure that the requested information is secure, will not be deleted or altered, and is available for review or production by TMICC or relevant third parties, even if the data retention period has expired. If I fail to follow this request, I and TMICC could face fines, liability and reputational harm.

Always speak to Data Privacy Team before:

- Collecting or using any sensitive or special category personal data or data relating to vulnerable people (including children);
- Using innovative technology, AI, or automated decision making to process personal data;
- Monitoring people or their behaviour; or
- Using large volumes of personal data (>100,000 for marketing and >10,000 for HR / R&D).

What are Examples of Personal Data?

Names, email addresses, home addresses, phone numbers, medical information, online cookies, IP addresses, location data, employee ID number, photographs or videos where individuals are identifiable.

Certain categories of personal data, such as race, ethnicity, religion, health, sexuality or biometric data are classified as “sensitive” or “special category” data and require additional protection.

All data on company-issued devices is subject to collection, transfer and inspection, as is company-related data on personal devices used for business purposes.

What is a Personal Data Incident?

A Personal Data Incident is any incident that has the potential for personal data to be lost, damaged or misused. This could be the result of a security failing, and it could be accidental or malicious in nature. A Personal Data Breach is when there is a confirmed loss, alteration, destruction, unauthorised disclosure of, or access to, personal data.

Examples of Personal Data Incidents:

- Accidental Disclosure: HR data (names, salaries) sent to the wrong recipients.
- Malware Attack: Consumer accounts database compromised by malicious software.
- Accidental Destruction: Payroll records deleted, causing payment delays.
- Loss of Paper Records: Health declaration forms mislaid at reception.

Report any Personal Data Incidents immediately to the Privacy Team.

Where do I go for more information?

Chief Privacy Officer, Global Privacy Team, Legal and Business Integrity Teams, Privacy & Data Governance Hub.

Responsible Sourcing and Business Partnering

Part 1/2

We select and work only with partners who can uphold standards consistent with our own commitment.

Why is it important?

TMICC expects the third parties with whom we do business to have their own compliance codes and policies in place that are appropriate to their business and of a comparable standard to ours, and to pass down similar requirements to their supply chain, customers, and / or entities with whom they do business. **Our Responsible Partner Policy** (RPP) sets out the mandatory requirements that all third parties must meet. Our **Purchasing Policy** provides the additional guidelines on purchasing materials and services from third parties. Failing to meet these standards may result in legal and reputational risks for TMICC and the abuse of Human Rights of workers in our supply chain. All employees engaging with third parties play a vital role in ensuring compliance.

What must I do?

- Read and understand the RPP, which contains clear standards for suppliers, customers and other third parties. The RPP is supported by tools, guidance and processes for onboarding, monitoring and addressing non-compliance, and mechanisms for employees to raise and seek resolution of concerns related to third-party conduct.
- Ensure that all third parties are subject to the provided RPP controls for onboarding, contracting and ongoing monitoring, including risk-based auditing and remediation of issues.
- Ensure that third-party selection, shortlisting and tendering processes consider their ability to meet the RPP requirements and legitimate business needs.
- Include contract clauses in agreements with suppliers, distributors and other parties (such as MSAs, MPAs, MRO, CM, among others) to confirm that business partners acknowledge and agree they can meet the RPP requirements as a condition of engagement, including clauses requiring:
  - **Compliance** with applicable laws.
  - **Cooperation** in investigations or audits conducted by TMICC.
  - **TMICC's** right to audit when we suspect non-compliance and to impose the costs of the audit on the third party in the event of non-compliance.
  - **TMICC's** right to terminate for non-compliance.
  - **TMICC's** right to be indemnified for supplier's non-compliant practices.
- Do not agree to contractual changes related to the RPP without first consulting my Legal Business Partner and obtaining written authorisation from the Responsible Business team.
- Supplier must agree with RPP terms before engaging in the RPP process.
- Report to my Line Manager, the Responsible Business team or Business Integrity Officer if I am aware of, or suspect, non-compliance with the RPP or any legal requirement by a third party.

Responsible Sourcing and Business Partnering

Part 2/2

What must I do?

- Engage with the Responsible Business team (i.e. Procurement, Business Integrity, Sustainability) on how to support the remediation of issues before terminating a partner due to non-compliance.
- Discontinue transacting with third parties who have been identified as non-compliant with the RPP, unless a formal exemption has been granted by the Responsible Business team or Legal team.
- Respect the rights of all individuals and communities who are defenders of Human Rights and civic freedoms.
- Seek guidance on both the legal requirements and Human Rights impacts of the transaction, when procuring, disposing of, or changing use of land. TMICC respects customary and legitimate land tenure rights and does not tolerate land grabbing.

Where do I go for more information?

Responsible Business or Human Rights teams, Procurement Team, Sustainability Team, Legal and Business Integrity teams, Responsible Partner Portal (RPP) and Human Rights Portal.

External Engagements and Communication

Part 1/2

We are trained and approved before speaking to brokers, analysts, shareholders, media, government, NGOs, regulators, or trade associations.

Why is it important?

Communicating on social media or with external parties, including brokers, analysts, shareholders, media, governments, NGOs, regulators or trade associations carries risks. Mishandled communication can result in misinformation, legal risk, reputational damage and regulatory consequences. Responsible and transparent engagement builds trust and protects TMICC's ability to operate and grow.

What must I do?

External communication:

- Ensure the accuracy and truthfulness of all information shared.
- Avoid saying or doing anything that may, or may be perceived as seeking to, improperly influence decisions about TMICC by any government, legislators, regulators or NGOs (see the Code Policy on Anti-Bribery and Anti-Corruption).
- Consider TMICC's reputation when communicating externally, applying the rules set out in the Social Media Guidelines for Leaders and Employees.
    - **Do not** post on social media on behalf of TMICC without prior authorisation.
- Seek approval from the relevant teams before making contact on specific topics e.g. contact local **Finance** or **Legal teams** before discussing financial, legal, tax or pensions matters; **Regulatory Affairs** before contacting regulators about products, ingredients or regulatory compliance; local **Communications, Corporate Affairs and Sustainability Team** before contacting NGOs or for any media engagement; local or global **Corporate Affairs teams** before engaging with public policy makers (e.g., governments, politicians, officials).

External engagement:

- Engage only with external parties if I am appropriately trained and specifically authorised and briefed by the appropriate team.
    - **For Engagements** with Trade Associations, refer to the Fair Competition Policy.
- Comply with any authorisation conditions and keep a record of my contact and interactions with external parties. Wherever feasible, meet with authorities with another colleague present.
- Seek prior approval before making contact to represent TMICC's interests, and obtain ongoing clearance if contact is a regular part of my role.
- Follow site procedures for unannounced inspections and know who the designated responsible person is at my site.

External Engagements and Communication

Part 2/2

What I need to remember when using personal social media as TMICC employee?

- Make it personal.
- Be honest and humble.
- Keep confidential information confidential.
- Link to official sources only.
- Keep market talk off the table.

Where do I go for more information?

Communications, Corporate Affairs and Sustainability Team or Product Safety & Regulatory Affairs teams, Business Integrity Officer or Legal, Global Policy Portal.

TMICC Standard on Trade Association Memberships including the governance on trade associations.

Health, Safety and Security

Part 1/2

We are committed to creating a safe, supportive and respectful workplace that protects the occupational health, safety, security and dignity of our employees. We foster a workplace atmosphere that prioritises psychological safety and promotes a learner mindset. We strive towards achieving zero harm to people, showing respect to our neighbours and actively contributing to communities we serve. We identify and mitigate hazards; continuously improving health, safety, and security performance through employee engagements. We play a leading role in promoting best practices in our industry.

Why is it important?

Unsafe practices can lead to serious physical or emotional injuries, environmental harm, or even loss of life. Managers play a key role in implementations, but each employee contributes to a safe workplace. Through individual action and shared responsibility, we protect people, property and the environment, act as a responsible and respectful neighbour, and earn the trust and confidence of our customers and consumers.

What must I do?

- Avoid and report any behaviour that could be offensive, intimidating, malicious, violent, insulting or bullying of any kind. We have a zero-tolerance policy on sexual harassment and discrimination.
- Promote a culture where employees are treated with dignity, and concerns can be raised and addressed promptly and fairly and without retaliation.
- Behave in a safe and health-conscious manner, following all laws, regulations, policies, standards, procedures, instructions and training relevant to my role.
- Never carry weapons on site.
- Perform work only when trained, competent, medically fit, sufficiently rested, functionally capable and alert enough to do so.
- Know emergency procedures in my location, during visits to other sites or when travelling.
- Report all incidents, near-misses, unsafe conditions, injuries, illness or unhealthy conditions to local TMICC management, without delay. Never assume someone else will.
- Support team leaders to ensure all employees, contractors and visitors understand and follow health and safety procedures and instructions.
- Understand the **Life Critical Standards** and follow them.
- Avoid working under the influence of any substance that may negatively impact the health and safety of myself or others.
- Do not carry on with any work that becomes unsafe or unhealthy.
- Speak Up if I have concerns about my ability to meet these minimum requirements or if the environment is unsafe or unhealthy.

Health, Safety and Security

Part 2/2

What must I do as a Manager or Team Leader?

- Establish and maintain a suitable health and safety management system for my site and team, including the appointment of committees, managers, competent experts, and a system for gathering concerns and input from employees, contractors and visitors.
- Set Occupational Health Safety-Security (OHS-S) objectives, review performance achievements and share evaluation outcomes.
- Foster a proactive OHS-S culture by promoting ownership at all levels and encouraging active participation through engagement, consultation, and training.
- Follow a structured methodology to ensure legal compliance and drive ongoing performance enhancement.
- Ensure contractors are responsible for implementing OHS-S measures consistent with this policy.
- Integrate OHS-S performance into employee evaluations, ensuring that safety responsibilities are recognised and rewarded accordingly.
- Maintain constructive, transparent communication with neighbouring stakeholders and affected communities.
- Guarantee that all managers and employees are fully aware of and accountable for fulfilling their roles in accordance with the company's policy.
- Implement strong process safety systems, conduct regular risk assessments and maintain safety-critical equipment to prevent major accidents.
- Drive a comprehensive Health and Wellbeing programme to support the health and wellness of employees.
- Implement measures to ensure the safety and wellbeing of all employees during work-related travel by providing clear travel guidelines.
- Implement targeted programs to enhance road safety performance, supported by effective measures to ensure sustained improvement.
- Ensure all work is based on freely agreed and documented terms that employees understand, and which are available throughout their employment.
- ***Provide*** a pay slip for each pay period, clearly indicating the components of compensation.
- Verify that no one has paid recruitment fees or related costs to gain employment, either directly or indirectly, and arrange repayment of any fees that are found to be paid.

What do I need to know?

Domestic violence and abuse can take many forms. It may appear as a single act or as a repeated pattern of behaviours, including physical harm, verbal abuse, sexual violence, emotional manipulation, psychological control and financial exploitation.

TMICC offers a range of support, such as special paid leave, access to counselling / support services, temporary or permanent change of working times, location, and pattern, etc.

For more information, please contact your HRBP.

Where do I go for more information?

Health, Safety and Security Manager, Site's Health, Safety and Security management system, Global Health, Safety and Security Standards (for Life Critical Standards).

Product Safety and Quality

Food safety and quality are non-negotiable. We design, make and sell products based on sound science, technology and responsible innovation, applying rigorous safety and quality standards, aligned with GFSI standards, HACCP and science-led systems. We run robust Food Fraud and Food Defence programs, aim to continuously improve, and deliver superior quality to benefit consumers and customers. We invest in training and communication, partner with suppliers, regulators and customers to uphold food integrity.

Why is it important?

TMICC prioritises the safety and quality of our products, adhering to all standards and regulations. This commitment builds consumer trust and strengthens our brands.

What must I do?

- Conduct all research and innovation in compliance with our global standards for safety, sustainability and ethical responsibility.
- Ensure risks related to consumer safety, occupational safety and environmental safety are assessed by experts and managed.
- Ensure specifications for raw materials, products and packaging comply with relevant regulatory requirements and standards.
- Ensure research involving human subjects is conducted to the highest ethical standards.
- Support TMICC's commitment to eliminating animal testing, ensuring that any mandatory regulatory testing is approved in advance.
- Maintain complete and accessible records of all research, including data, study protocols and related decisions.
- Apply and uphold Quality Management Standards (QMS) and systems to design, deliver, monitor, measure and continually improve product and process performance to ensure compliance with internal and external requirements.
- Act on risks, issues and feedback from consumers, customers and partners, including taking proactive steps to prevent quality or safety issues and escalating or recalling products that do not meet standards or regulations.
- Foster a quality-first culture by promoting transparency, accountability and timely reporting of concerns to my Line Manager or Quality lead.
- Communicate responsibly and share accurate information about product safety.
- Seek authorisation and follow the escalation procedure before responding to external queries, whether from consumers, business partners, or the media about any product safety or quality concerns.

Where do I go for more information?

Local or Global Quality Team, Quality and Safety Policy, QMS portal and chatbot, R&D Standards Hub.