CODE OF ETHICS AND GOOD CONDUCT

DAHER

THE ESSENTIALS OF THE CODE OF ETHICS AND GOOD CONDUCT

1. Do not make sexually inappropriate comments or engage in sexually suggestive behaviour.
2. Do not engage in any discriminatory behaviour.
3. Look after your own health and safety, as well as that of the people around you at work.
4. Do not impede freedom of expression.
5. Pay special attention to any vulnerable individuals.
6. Do not process any personal data without notifying your superiors and/or the Data Protection Officer.
7. Legal and regulatory requirements for the protection of physical environments (water, air), natural spaces (sea, forest) and natural heritage must be strictly observed.
8. Gifts, invitations or benefits of any kind, received, solicited, proposed or given, whether directly or indirectly, must comply with special rules.
9. Benefits cannot be offered to third parties to obtain a decision in favour of the Group.
10. Requests for corporate philanthropy or sponsorship must be directed to your superiors and to the Group Legal Department.
11. Each employee must refrain from making a decision for the direct or indirect benefit of a person with whom they have a familial, financial or friendly relationship.
12. Do not grant any gift or favour to a person, political party or religious cause without first obtaining approval from the Ethics Officer.
13. Check the integrity of the partners with whom you collaborate and remember to check whether they appear on blacklists linked to criminal activity.
14. Never discuss prices, customer breakdowns, products or contracts with a competitor, even within professional associations.
15. Never release strategic information.

16 Classification, value and country of origin must be clearly determined for all imports.

17 Make sure to always avoid any situation that may cause conflict between your personal interests and your obligations towards the Group.

18 Employees who have made or contributed to the making of an invention must declare it according to the applicable procedure.

19 It is strictly forbidden to use Group property or funds for personal benefit.

20 Do not communicate any of the Group's confidential information without first obtaining the signature of a confidentiality agreement.

21 Make sure that all contractual documents are negotiated, approved and signed according to defined internal procedures.

What is the Code of Ethics and Good Conduct?

The Code of Ethics and Good Conduct lays out general principles intended to guide the actions of all Group employees on a day-to-day basis. When necessary, the Code is supplemented with detailed rules that must be consulted, which the Code directly refers to using active links.

Who is the Code for?

The Code is for all senior managers and employees of the Group, in France and around the world. Principles and Rules detailed in the Code must also be extended to and followed by all suppliers, customers and business partners (intermediaries, agents) with whom our Group has an established relationship.

OUR SOCIAL AND ENVIRONMENTAL ETHICS

RESPECT FOR INDIVIDUAL DIGNITY AND PROMOTION OF RECIPROCAL TRUST

- It is strictly forbidden to repeatedly engage in sexually suggestive comments or behaviour that undermine a person's dignity due to their humiliating or degrading nature, or which create an intimidating, hostile or offensive environment.
- Any serious pressure, even if not repeated, that is carried out with the actual or apparent aim of obtaining a sexual act for one's own benefit or for the benefit of a third party is completely prohibited.
- No tolerance will be granted for malicious acts towards a person, whether repeated or not (derogatory remarks, acts of intimidation, insults), if they lead to a significant deterioration in the working conditions of the victim and infringe upon their rights and dignity, alter their physical or mental health, or compromise their professional future.
- Such acts constitute offenses punishable by law.
- In case of a hierarchical relationship, the penalties incurred are more significant.
- No sanction will be imposed on a person reporting and combating harassment except in the event that the report is made in bad faith, with the sole aim of causing harm, based for instance on facts which are perfectly known to be inaccurate.

WHAT TO DO:

- Do not make sexually inappropriate comments or engage in sexually suggestive behaviour.
- Do not make threats or offensive remarks, and do not engage in violence against a fellow employee.
- Report any inappropriate behaviour towards yourself or those around you to your supervisor or Ethics Officer, or via the internal whistle-blower system.

RESPECT FOR DIVERSITY AND PROMOTION OF EQUAL OPPORTUNITIES BASED ON MERIT AND COMPETENCE

- All discriminatory practices are prohibited when they are based on: national or ethnic origin, sex, marital or pregnancy status, physical appearance, a particular vulnerability resulting from an apparent or known economic situation, surname, place of residence, health, loss of autonomy, disability, genetic characteristics, mores, sexual orientation, gender identity, age, political opinions, trade union activities, the ability to express oneself in a language other than French, and membership or non-membership in an actual or supposed ethnic group, nation, race or religion.

- On the basis of these criteria, it is prohibited to refuse to supply goods or services, or to hinder the normal exercise of an economic activity, or to exclude a person from a recruitment procedure or from accessing an internship or a training period in a company.

- No employee may - on the basis of the criteria above – be sanctioned, dismissed or endure discrimination, direct or indirect, in particular in terms of remuneration, profit-sharing, distribution of shares, training, reclassification, assignment, qualification, classification, professional promotion, transfer or renewal of contract.

- It is also forbidden to participate in the recruitment, promotion, retention, training, development or remuneration of any individual from your family or personal environment.

WHAT TO DO:

- Support and encourage the Group's diversity and integration initiatives.
- Avoid any discriminatory behaviour.
- Report any suspected discrimination to your supervisor or Ethics Officer, or via the internal whistle-blower system.

PROTECTION OF HEALTH AND SAFETY AT WORK AND PROMOTION OF WELL-BEING AT WORK

- The Group is required to prevent occupational risks and harsh working conditions, inform and train its employees, and set up an organisation with appropriate resources.
- Each employee, according to their training and means, must take care of their own health and safety, as well as the health and safety of other people affected by their acts or omissions at work.
- Employees with a certain level of responsibility within the Group must follow the training courses on this topic and ensure the health and safety of the teams under their management or lead.

WHAT TO DO:

- Take care of your own health and safety, as well as the health and safety of those working with you.
- Strictly follow safety instructions when using equipment and/or tools and when wearing protective equipment.
- Familiarise yourself with the Group's documentation and follow the training courses provided by the Group.
- Alert your manager in the event of any serious or imminent danger at work, or in the event of any malfunction in a protection system.
- Report to your supervisor any harsh working conditions, any risks related to health or safety at work, or any defect in the evaluation or control of a risk already identified.
- Participate in all efforts to continuously improve health and safety at work.

RESPECT FOR COLLECTIVE FREEDOM OF EXPRESSION AND RESPECT FOR FREEDOM OF ASSOCIATION

- It is prohibited to restrict individual and collective freedom of expression, as long as this restriction is not justified or proportionate to the intended aim.
- Individual freedom of expression must be exercised within the limits of the employee's duty of loyalty (duties of confidentiality, discretion and non-competition).
- The right to direct and collective expression relates to content, conditions of exercise and the organisation of work. It is intended to define the actions needed to improve working conditions, organisation and production quality within the employee's work unit and the company.
- Any discrimination based on the establishment of a trade union organisation, membership in a trade union organisation, or representation by a trade union organisation, is strictly prohibited.

WHAT TO DO:

- Promote quality dialogue within the Group by using, and encouraging everyone else to use, their right of expression in a climate of trust.
- Report any situation in which you, or someone around you, has been disproportionately prevented from speaking out on the work performed, proposing improvements to your working conditions, or expressing your opinion.
- Make sure that your collective freedom of expression is not infringed.
- If you have any questions, contact your supervisor or Ethics Officer.

PROHIBITION OF CHILD LABOUR

- Local laws and regulations must be strictly enforced, in addition to the following principles enacted by Conventions 138 and 182 of the International Labour Organization.
- It is strictly forbidden to employ children under the age of 16.
- It is forbidden to employ children under the age of 18 for particularly difficult or dangerous work.
- Children between the ages of 16 and 18 may be employed as long as it does not prevent access to schooling.

WHAT TO DO:

- Always check the age of anyone placed under your responsibility at work.
- You are responsible for ensuring that the principles given above are duly respected by the Group's subcontractors and suppliers, in particular by including standard contractual clauses, which you can obtain from the Legal Department.

PROHIBITION OF FORCED LABOUR

- It is strictly forbidden to obtain work or services from someone under threat of penalty, and without that person offering their services willingly.
- It is also forbidden to employ someone whose vulnerability or state of dependence is apparent or known, to perform unpaid services or in exchange for compensation clearly unrelated to the importance of the work performed.

WHAT TO DO:

- You are responsible for ensuring that the principles given above are duly respected by the Group's subcontractors and suppliers, in particular by including standard contractual clauses, which you can obtain from the Legal Department.
- Pay special attention to vulnerable people in order to help them with the procedures and decisions regarding their employment.
- Do not threaten or pressure people to work for the Group's benefit.

PROTECTION OF PERSONAL DATA

- Personal data must be collected and processed in accordance with applicable local laws and regulations.
- Access to personal data must be strictly reserved for persons needing to know it who are duly authorized for this purpose, to the extent that the purposes pursued are defined, legitimate and necessary.
- Any consultation or processing of this type of data in any form whatsoever outside this framework is prohibited.
- Some regulations impose restrictions on the international transfer of personal data, even within the same Group.

WHAT TO DO:

- Refuse access to personal data absent any need, authorisation or defined, legitimate and proportionate purposes.
- Do not process any personal data without reporting it to your supervisors and/or Data Protection Officer.
- Check the applicable rules before any transfer of personal data internationally, including within the Group.

RESPECT FOR AND PROTECTION OF THE ENVIRONMENT

- Legal and regulatory requirements for the protection of physical environments (water, air), natural spaces (sea, forest) and natural heritage must be strictly observed.
- Measures to prevent pollution, risks and nuisances (classified facilities, waste, noisy activities, visual disturbances, nuclear safety) must also be strictly observed.

WHAT TO DO:

- Support and encourage the Group's policy by contributing to the development of systems for monitoring environmental certifications, indicators and objectives.
- Attend training and awareness sessions organised by the Group for its employees.

OUR BUSINESS ETHICS

ANTI-CORRUPTION POLICY

What is wrongdoing?

- Acts of corruption and influence peddling are prohibited by international conventions and local laws in most of the countries where our Group operates.

- Since certain national anti-corruption regulations apply extraterritorially, the existence of a bank account, the use of a local intermediary, or even the sending of an e-mail may be sufficient to give jurisdiction for local courts to criminally prosecute a Group company located in another country, regardless of where the offense was committed.

- Accordingly, the Group's companies must not only comply with French and EU anti-corruption regulations, but also those of other countries, including American law (the FCPA) and English law (the UK Bribery Act).

- All forms of corruption are prohibited, including:
  - Active or passive corruption: active corruption is the act of the person offering or granting the undue advantage; passive corruption is the act of the person who solicits, accepts or receives the undue advantage.
  - Public or private corruption: public corruption characterises the abuse of power committed by a public official in return for an undue advantage, while private corruption describes a situation in which a private sector employee abuses their position.
  - Direct or indirect corruption: corruption can be perpetrated directly or indirectly (through a local intermediary, for instance).

- Whatever the benefit granted (donations, loans, fees, gifts, taxes, etc.), the practice is prohibited.

- Acts of corruption include:

  - paying or offering to pay a commission to the purchaser of a public entity in order to distort the tender procedure for industrial equipment;
  - offering to a public official to acquire a stake in a project company through a strawman, one of whose clients is the authority that employs this public official.

- Whatever act (positive act or abstention) is expected in return for the benefit granted, the practice is prohibited.

- Acts of corruption include:

  - asking a public official to bury a document establishing a right of way over land in the public domain in order to allow an administrative, emphyteutic lease to move forward;
  - asking a public official to artificially create conditions that allow you to ignore the rules governing public contracts in order to obtain the contract.

What are the principles and rules to follow?

Our Group enacts and ensures that all employees comply with very strict rules to prevent acts of corruption and influence peddling.

Benefits, gifts and invitations: gifts, invitations or benefits of any kind, solicited, received, offered or given, directly or indirectly, are prohibited for both public officials and private persons.

On an exceptional basis, gifts of small or symbolic value granted in a transparent manner may be tolerated if they are not likely to influence a decision or behaviour. Any gift or invitation, regardless of its value, must be subject to prior written authorisation by a direct supervisor.

Facilitation payments: unofficial payments made to a public official (French or foreign) to speed up an administrative procedure relating to their duties (customs clearance of goods, obtaining a visa or a building permit, etc.) are forbidden.

Influence peddling: it is forbidden to provide – unlawfully, directly or indirectly - offers, promises, gifts or benefits to a third party (private person or public official) to use one's real or supposed influence with a decision-maker, in order to obtain a decision favourable to the Group.

Patronage and sponsorship: replies to patronage and sponsorship requests are closely supervised by the Group. Any employee who receives such a request must refer to their superior or to the Legal Department to find out about the internal procedure applicable to patronage and sponsorships.

Any payment of a donation or contribution to an association or a foundation - in violation of the applicable internal procedure - is likely to be qualified as an act of corruption.

Assessment of intermediaries and compliance with the Code: relationships with third party partners (in particular intermediaries and local agents) are particularly susceptible to corruption risks.

Consequently, each employee in contact with a third party partner must:

- Before starting or renewing a business relationship with a third party partner, carry out a risk analysis according to the Group's specific procedures on corruption, including the third party verification procedure ("Intermediary Compliance Questionnaire - Information Form").

- If there are any doubts about the integrity of the third party, carry out a more in-depth examination; according to the information obtained, it may be decided not to enter into a business relationship or renew the contract with the intermediary.

- Ensure that the contract binding the company to third party partners contains standard clauses, under which the third parties undertake to respect DAHER's Code of Ethics and must expressly avoid acts of corruption and/or influence peddling. If these clauses are not contained in the current contract, an amendment to the contract must be signed with the third party.

Conflicts of interest: each employee must refrain, within the framework of their responsibilities, from making a decision that may appear to be contrary to the interests of the Group, either for the direct or indirect benefit of a person with whom they have familial, financial or friendly ties.

WHAT TO DO:

- Keep yourself informed and trained in accordance with the Group's obligations, and refer to the Group's specific procedures on corruption.
- Incorporate our standard anti-corruption clauses into all commercial, supplier and intermediary contracts. Please refer to the Legal Department for this.
- Send and collect the completed "Intermediary Compliance Questionnaire/Information Form" before entering into business relations with intermediaries. Once done, please contact the Ethics Officer or the Legal Department to have said questionnaire duly analysed.
- If you suspect or are certain that you are being asked to pay or accept a bribe (of any kind whatsoever), please report this to your supervisor or Ethics Officer.
- Use the Internal Whistleblower System if you wish to report an act of corruption confidentially.
- No employee will be sanctioned, dismissed or subject to discriminatory measures for having reported, related or testified to any acts of corruption and/or influence peddling, in good faith and in a disinterested manner, either through their supervisor or the Internal Whistleblower System.
- If you have paid a bribe of any amount or you know that someone else has done so, you should report it to your supervisor, your Ethics Officer or the Legal Department.

RELATIONSHIP WITH POLITICAL PARTIES

- Employees are perfectly free to make personal contributions to a candidate or a political party of their choice.
- Any contribution via any of the Group's resources in favour of a party and/or candidate and/or political campaign and/or religious cause must be done strictly in accordance with local laws and regulations.
- Any representation of interests for and on behalf of the Group, on a regular basis, must be declared to the High Authority for Transparency in Public Life.

WHAT TO DO:

- Do not grant any gift or favour whatsoever to any person, political party or religious cause for and on behalf of the Group without having previously obtained express approval from the Ethics Officer.
- Make sure to inform the Ethics Officer of any attempt to approach political actors for and on behalf of the Group.

FINANCIAL INTEGRITY AND ANTI-LAUNDERING POLICY

- Any money-laundering operation is strictly prohibited.
- Strict compliance with accounting laws and regulations is required, particularly regarding the transparency, regularity and reliability of accounts, which must perfectly and strictly reflect the transactions carried out.
- Any recording of inaccurate, misleading, incomplete or false information is strictly prohibited and will be severely punished.
- Any alteration or deletion of the Group's accounting entries, without prior authorisation, is strictly prohibited.
- Any communication of false financial data to mislead a customer, supplier, regulator or third party is strictly prohibited.
- Accounting documents must be maintained in accordance with the regulations in force and the Group's internal procedures.

WHAT TO DO:

- Make sure you know your customers and suppliers well and be vigilant about any unusual invoices, orders or payments; report any unusual transaction to the Ethics Officer; check the accuracy of the information you send to accounting and financial services.
- Never agree to misrepresent anything and/or participate in fictitious transactions.
- Check the integrity of the partners with whom you are collaborating, and remember to check whether they appear on blacklists linked to criminal activity.
- Be particularly vigilant for all cross-border transactions.
- Report any suspected breaches.

COMPLIANCE WITH COMPETITION RULES

Economic actors operating in the same market, domestic or international, must refrain from distorting competition and acting unfairly towards their competitors and partners.

What are the main anti-competitive practices penalised?

- Agreements between competitors to fix prices and divide customers and/or markets between them.
- Exchanges of confidential or strategic information between competitors.
- Resale prices imposed on distributors.
- Abuse of dominant position (over 30 to 40% of market share).

What are the main inappropriate and unfair practices?

- Exploiting competitors' efforts and investments at a lower cost ("parasitism").
- Discrediting competitors (denigration).
- Poaching a competitor's staff despite a non-competition clause.

WHAT TO DO:

While negotiating commercial or acquisition agreements between competitors and/or partners:

- Never discuss prices, customer breakdowns, products or contracts, (especially in the context of RFQs), even within professional associations or shared organisations (joint ventures, consortia, etc.).
- Never divulge any strategic information (commercial, financial, industrial, etc.).
- Be vigilant about your commercial practices in the event of a dominant position (market share over 30 or 40%).

While poaching a competitor's employees:

- Always check if the employee has a non-competition clause in their employment contract and verify its scope.
- Always check the procedures for obtaining information on the competitor from the poached employee, and be vigilant about using any strategic information thus obtained.

COMPLIANCE WITH INTERNATIONAL TRADE RULES

- Exports and re-exports of goods and technologies (technical data, know-how, software, etc.) are subject to laws and requirements (including simple declaration, prior authorisation, restrictions or prohibitions) when exporting to certain countries, individuals or organisations.

- Some countries, such as the USA, restrict the export or re-export of products originating from their territory but located in another territory and/or incorporated into materials of foreign origins.

- The intervention of a third party to carry out mandatory administrative checks and formalities does not absolve the prime contractor of any liability.

- Imports are also subject to strict administrative formalities and potential customs duties, both of which may vary according to the nature of the imported products, tangible or intangible, as well as their value and country of origin.

WHAT TO DO:

- Learn and familiarise yourself with the export control procedures described in the Internal Compliance Programme (MAN-0013).
- Before entering into a contractual relationship, check that the prospective partner(s) and shareholder(s) are not blacklisted, registered by the USA or Europe as people and countries subject to sanctions, or part of the Daher Country List (duly updated by the Group Risks Department, by Audit and by Internal Control). Make sure that all regulatory formalities have been completed, and take special care to ensure the required documentation is kept up to date.
- Make sure that export control obligations and their breakdowns are included in contractual agreements with our partners (customers, prime contractors, agents, etc.).
- Make sure to clearly determine the classification, value and country of origin of all imports.
- Never sign an agreement relating to compliance with export control regulations, the final use of purchased materials, or the export control classification of manufactured materials.
- Contact the Legal Department for any questions or approvals.

POLICY FOR SELECTION AND USE OF ECONOMIC PARTNERS

- Our Group wishes to establish healthy, fair, equitable and transparent relationships with all its partners, including suppliers and intermediaries. The main aims are to establish, develop and consolidate long-term partnerships based on mutual trust.

- Suppliers are selected based on a responsible purchasing policy which most of the time entails competition. Suppliers are on the same equal footing all throughout the procedure and are selected using objective, fair criteria communicated transparently.

- Intermediaries are also chosen via a rigorous selection process, and must uphold the values of the Code. An evaluation of the intermediary's integrity must be systemically performed during selection or renewal of their contract, and should be implemented in accordance with the procedure "Intermediary Compliance Questionnaire - Information Form".

- It is necessary at all times to ensure that the services rendered by the intermediary are real, and that their remuneration is duly justified and proportionate to the services rendered.

- No act of corruption at the impetus of the employee (active corruption) or supplier or intermediary (passive corruption), with the aim of circumventing the Group's selection rules, should be proposed, accepted or tolerated by the Group.

- All employees must avoid selecting a supplier or intermediary with whom they have ties (financial, familial or friendly), even indirect or distant.

- In any event, and before selecting the supplier or intermediary in question, the employee must make a conflict of interest declaration.

WHAT TO DO:

- Before signing contracts with suppliers and/or intermediaries, check whether they include compliance clauses regarding the Group's Ethics Code and/or anti-corruption policy.
- Refuse any attempt or act of corruption by a supplier or intermediary, and report this incident to your supervisor or through the Internal Whistle-blower System.
- Do not offer or accept a contract with a supplier or intermediary who does not meet the selection criteria adopted by the Group or with whom you have a relationship or ties, even indirect.
- Declare any ties or relationship – direct or indirect - with a supplier or intermediary, according to the "Prevention and Declaration of Conflicts of Interest" procedure.

COMPLIANCE WITH THE RULES OF GOOD CONDUCT TOWARDS THE GROUP

PREVENTION AND DECLARATION OF CONFLICTS OF INTEREST

- It is forbidden to take decisions for and on behalf of the Group in a conflict of interest situation without having been previously authorised to do so.
- It is forbidden to influence a RFQ or the negotiation of contracts by using one's function within the Group.
- For instance, there is a conflict of interest when:
  - an employee, a member of your family or someone you know is likely to realise personal gains because of your position, your influence or your knowledge of confidential information within the Group;
  - an employee holds interests in a company competing or carrying out an activity complementary to that of the Group.

WHAT TO DO:

- Avoid any situation that could create conflicts between your direct or indirect personal interests and your obligations towards the Group and/or affect the impartiality and objectivity of your decision-making.
- Contact the Ethics Officer if there is a conflict of interest, even potential, (e.g. regarding emotional or family ties with a third party with whom a business relationship may be initiated), or if you have any questions.
- Use the Internal Whistle-blower System to report any behaviour that you believe to be in violation of the Anti-Corruption Policy.

PROTECTION OF AND RESPECT FOR INTELLECTUAL AND INDUSTRIAL PROPERTY

- The Group's intangible assets (IP) must be protected just like its tangible assets. Each year, the Group devotes a significant budget to this, particularly in Research & Development (R&D). It is forbidden to put the Group at risk by behaving in a way that undermines its IP and/or third parties' IP.

What are intangible assets or IP?

- Intangible assets include trademarks, inventions (patentable or non-patentable), patents, copyrights, trade or business secrets, and know-how.
- WARNING: any employee of the Group who has invented or contributed to the making of an invention must declare it according to the applicable procedure.

WHAT TO DO:

- Regarding commercial and/or partnership agreements (consortia, subcontracting, co-contracting):
  - Never disclose or use the company's IP without first obtaining the signature of a confidentiality agreement and/or without the express prior authorisation of the company's duly authorized representatives.
  - Never appropriate and/or use documents/information from third parties' IP, without first checking their origin and their free availability.
  - If you have created an invention, patentable or not, you must declare it according to the "Invention Declaration Procedure".

FRAUD PREVENTION

- The Group's funds and tangible assets, owned by its shareholders, are at the disposal of its employees only for business purposes and in the exclusive interest of the Group.
- This includes industrial facilities, equipment and financial resources.
- Employees must do their utmost to protect them, and under no circumstances may they be used for illicit purposes or for reasons unrelated to Daher.
- It is strictly forbidden to appropriate, damage or alter any company property or funds for personal purposes or to make them available to third parties for use outside the Group.
- It is also strictly forbidden to use any Group property or funds for personal benefit, or to allow their use by other people not employed or authorised by the Group.
- It is forbidden to use the Group's means of communication other than for business purposes.
- Employees must play a part in internal control and the dissemination of information, while strictly adhering to internal procedures to avoid any attempt at external fraud, concealment, deception or dishonesty (CEO fraud, fake invoices, etc.).

WHAT TO DO:

- Report any suspicious behaviour or transaction via the Whistle-blower System.
- If you have any questions, contact the Ethics Officer.

PROTECTION OF INTERNAL AND EXTERNAL CONFIDENTIAL INFORMATION

- Any information (in any form whatsoever) relating to Daher's environment and activities is an essential part of the Group's assets and is, by nature, confidential.

What is "confidential information"?

- The concept of "confidential information" should be broadly interpreted. "Confidential information" includes but is not limited to any information relating to people, products, studies, projects, industrial data, IP data, commercial, financial or industrial plans, etc.
- It is every employee's duty to protect and preserve the Group's assets (tangible or intangible) against any degradation, theft, misappropriation or attack against their integrity, and to not use them for personal purposes.
- To this end, it is up to everyone to take care not to divulge confidential information outside the company, or even inside the company to unauthorised persons (service providers, trainees, etc.), without following the appropriate framework and applicable internal procedures.
- Everyone is required to respect this "confidentiality obligation", even outside the workplace and after leaving the Group.

WHAT TO DO:

- Confidential Group data must not be communicated without the prior signing of a confidentiality agreement.
- Contact the Legal Department to confirm whether enhanced protection is required via individual confidentiality agreements.
- Do not communicate confidential information belonging to a third party without its prior written authorisation, and without the prior written authorisation of any authorised person (your direct supervisor or Ethics Officer).
- Never provide access to the Daher network to unauthorised persons, or to Group employees located outside the country without first checking with the Information Systems Department that the required level of protection is in place.
- Use the information system appropriately: secure your computer's access codes (do not lose them), do not lend your computer equipment, and do not install any software that is not approved by the Group's Information System. Refer to and follow the Group's IT Procedure.

MANAGEMENT AND STORAGE OF DOCUMENTS

- Proper management and storage of documents ensures good and stable relationships with the Group's third parties, and secures the Group's rights and interests during a government inspection, litigation or regulatory audit.

WHAT TO DO:

- Make sure that all agreements made with third parties (suppliers, customers, service providers) are based on a legal contract, order or any other supporting document having legal value.
- Insist wherever possible that all commitments be formalised in a contract using the contract templates available with the Legal Department.
- Make sure that all legal documents are negotiated, approved and signed as per the defined internal procedures.
- When drafting a document, keep in mind any implications that its content may have for the Group.
- Refer to any internal procedures for the destruction, storage or archiving of documents.

WHISTLEBLOWER SYSTEM

Who can use this whistleblower system?

- The use of the Internal Whistleblower System is open to all employees (internal, external and occasional employees of the Group), but remains optional and is subject to independent judgement.

- The system does not replace the usual internal reporting channels. As such, employees may alternatively or simultaneously contact their supervisor, their human resources manager, the Ethics Officer and/or staff representatives.

What incidents may be reported?

- Any incident of which the employee has personal knowledge and which may constitute:
  - a crime or an offence,
  - a serious and manifest violation:
    - of an international agreement ratified or approved by France
    - of a unilateral act taken by an international organisation on the basis of such an agreement
    - of the law
    - of a regulation
  - a threat or serious harm to the general interest.
- A behaviour or situation that violates the Code and constitutes an act of corruption or influence peddling.
- A risk to or serious violation of human rights and fundamental freedoms, human health and safety, and the environment, resulting from the Group's activities and/or those of the Group's subcontractors and suppliers, in France and abroad.

How to use this system

STEP 1: use the internal channel

- This report can be made by logging in to a "secure and encrypted" address on the site of an external supplier (for more details, refer to the **My Legal Ethics and Compliance section of the Group's intranet**), which guarantees confidentiality.

- The identity of the whistleblower will be kept anonymous, as the internal whistleblower system does not record IP addresses or other metadata (i.e. data that can identify the whistleblower).

CAUTION: if you do not follow step 1 for any reason, you will lose the legal protections granted to whistleblowers.

STEP 2: contact an administrative / judicial authority or a competent professional association

- Condition: if the report was not processed via step 1 within a reasonable timeframe

- Depending on the subject of the report, you may contact: a judicial (public prosecutor, judge) or administrative authority (prefect, inspection agency, French Anti-corruption Agency (AFA), regional health agency, etc.) or a competent professional association (Order of Lawyers, Doctors, Accountants, Notaries, etc.).

STEP 3: make the report public (media, associations, NGOs, unions)

- You may go directly to step 3 if you can show that:
    - The report was not processed within a 3-month period by the authority contacted in step 2, and/or
    - There is a serious and imminent danger or risk of irreversible damage, which necessitates skipping steps 1 and 2.

The internal whistleblower system cannot be used for emergency situations. In the event of serious and imminent danger or risk of irreversible damage, you must go directly to Steps 2 or 3.

The internal whistleblower system only applies to step 1.

To provide a whistleblower channel in compliance with legal requirements, the Group has set up a whistleblower system, details of which can be found in the My Legal Ethics and Compliance section of the Group's intranet.

How to use the internal whistleblower procedure (STEP 1)

Before submitting a report:

Before reporting any of the above incidents, make sure you can claim whistleblower status.

Log in to the Group's intranet (MyLegal, "Ethics and Compliance" section); once connected, you will be given the login address for the external supplier's site.

Once you have reached the external supplier's site, please indicate the following:

- The category of incidents to be reported (acts of corruption, environment, health and safety, miscellaneous, etc.).
- Your identity, unless you wish to remain anonymous.
- A description of the incidents you wish to report (if possible, attach to your message any useful documents or files to substantiate your report). Please be as precise as you can.

Submission/receipt/admissibility/processing of the report

- Please confirm submission of your report by clicking on the "SEND" button.
- Your report will then be transmitted and processed by the Ethics Officer, securely and confidentially, in accordance with the applicable rules for the protection of personal data.
- Once notification is received, the Ethics Officer will access the report using a personal password and a secondary password.

- Once your report is submitted, you will receive an acknowledgment of receipt directly on your screen with a “username and password” in order to access a secure reserved area. This space may be accessed by clicking on the "FOLLOW-UP" button on the site's home page. This acknowledgment of receipt does not imply that the report is admissible.

- You will be kept informed of the status of your report, as well as its closure.

- Before the report can be reviewed in-depth, it will be checked - within fifteen days – to ensure it is within the scope of the system in question (conditions described above).

- During this examination, if it turns out that the report is not admissible (due to a lack of merit, bad faith on the part of the author, false allegations, unverifiable or insufficiently substantiated facts), the author will be informed, and the report will be filed and archived.
- Any admissible reports may trigger an investigation, to be managed internally by the members of the Risk Committee (who are specially authorised and bound by a stricter confidentiality obligation), or by occasional external agents (also covered by the strictest confidentiality), in order to carry out the investigations deemed necessary.

- The individual(s) covered in the report will be informed (without revealing the identity of the author):

    - Of any personal data recorded, in order to allow them to oppose the processing of such data for any legitimate reasons, in accordance with the Data Protection Act.
    - Of the facts they are accused of, so that they can have the opportunity to respond to them as part of the investigation.

Note: to prevent the destruction or possible alteration of useful evidence, information regarding the individual(s) covered in the report may still be used after taking any precautionary measures deemed necessary to preserve the evidence.

Data retention and destruction:

- Any data arising from an inadmissible report or that does not receive any follow-up (particularly legal and/or disciplinary proceedings) will be kept and archived as "classified without follow-up" once all investigations and admissibility inquiries are completed.

- The author of the report and the individuals covered will be informed once the case is closed.

- Data from admissible reports that lead to legal and/or disciplinary proceedings (against the individual covered in the report or the author of the report, if false) will be kept until the procedure is completed and then archived in compliance with the rules in force.

How is the whistleblower protected?

- **Confidentiality guarantee:** strict confidentiality is guaranteed to the whistleblower. Everything is done to ensure that their identity is never communicated to the person(s) implicated in the report throughout the procedure. The content of the report will not be brought to the attention of any person outside the Risk Committee – *(which is made up of a limited number of people responsible for processing the report)* - except if the involvement of one or more person(s) is necessary to process the report; in this case, this/these person(s) will be subject to a stricter confidentiality obligation. However, this confidentiality commitment cannot be enforced if disclosure is required for a legal or administrative proceeding.

- **Lack of disciplinary or criminal proceedings:** use of the whistleblower system in good faith and in compliance with the reporting rules cannot, under any circumstances, expose the author of the report to any discrimination, retaliation, demotion, disciplinary sanction or criminal prosecution.

- Any direct or indirect retaliation against the whistleblower or persons who provided assistance to the investigation during processing of the report will not be tolerated within the Group and may give rise to disciplinary sanctions, including termination of the employment contract, in accordance with applicable law.

- REMINDER: anyone guilty of obstructing the transmission of a report, disclosing the identity of the whistleblower or filing a false defamation complaint against the whistleblower will incur heavy criminal penalties (up to 2 years in jail and a fine of €30,000).

- **Right to access, rectify and oppose personal data processing:** the whistleblower, as well as the individuals covered in the report, may access their respective data; if this data is inaccurate, incomplete, dubious or out of date, they may request its rectification or deletion. Any request to this effect must be addressed to the Legal Department.

- The individuals covered in the report may not under any circumstances request or obtain information concerning the identity of the author of the report.

What is the responsibility of the whistleblower?

- To avoid losing legal protections and exposing yourself to legal action, including criminal prosecution, it is strongly recommended to:

    - verify that you can claim whistleblower status;
    - follow the procedures step by step (1/2/3) as listed above, except in the identified exceptions;
    - avoid any generalisations, overstatements or accusations not supported by evidence and not materially verifiable: be sure to gather all evidence (letters, reports, testimonies) prior to the report in order to put together a file to substantiate the report you plan to make.