



GROUP WHISTLEBLOWING POLICY

Policy name	Group Whistleblowing Policy
Purpose	Explain how concerns may be reported and how the Group receives, assesses, investigates and closes reports.
Scope	Pasqal Holding SA and its subsidiaries worldwide
Audience	All persons entitled to report under applicable French, US and local laws
Drafted by	Compliance Officer
Adopted by	Board of Directors
Document control	Public Version 1.0 Effective date
Related documents	Code of Business Conduct & Ethics/Audit Committee Charter/Data Privacy Notice for Whistleblowing reports

1. Purpose and guiding principles

Pasqal Holding SA (the “Company”) and its subsidiaries (the “Group”) are committed to conducting business with integrity and in compliance with applicable laws. This Policy provides a simple and secure way to raise concerns and explains what reporters and other persons involved can expect. The guiding principles of this Policy are:

- Reports are assessed objectively, promptly and on a need-to-know basis.
- Confidentiality is protected to the fullest extent permitted by law.
- Anonymous reporting is available unless prohibited by applicable local law.
- Retaliation against a person who reports in good faith or assists with a report is prohibited.
- The Audit Committee independently oversees Financial Reporting Concerns and cases presenting specified conflicts of interest.

2. Legal framework and local application

This Policy is designed to support compliance with the French whistleblower framework, including Law No. 2016-1691 of 9 December 2016, as amended by Law No. 2022-401 of 21 March 2022, and Decree No. 2022-1284 of 3 October 2022, as well as applicable U.S. securities law and the rules of the exchange upon which the Company’s securities are listed for trading.

Local mandatory rules prevail where they provide additional requirements or greater protection. Necessary local adaptations, including restrictions on anonymous reporting, must be validated by the Compliance Officer.

3. Definitions

Term	Meaning
Compliance Officer	The Company’s general counsel; provided that in the event there is no general counsel or the general counsel is unavailable, the Company’s Chief Financial Officer shall be authorized to serve as the Compliance Officer in the interim or to designate another person as the Compliance Officer.
Concern	Information about actual or likely misconduct connected with the Group or its activities.
Report	A Concern submitted through the channels described in this Policy.
Reporter	A person who submits a Report.
Group Ethics Committee	The Chief Financial Officer, the Human Resources Director and the Compliance Officer.

Term	Meaning
Audit Committee Matter	A Financial Reporting Concern.
Financial Reporting Concern	A Concern relating to accounting, internal accounting controls, financial reporting, internal control over financial reporting, auditing, financial fraud, market disclosures or related records.
Retaliation	Any direct or indirect adverse action caused by a protected Report or participation in its handling.
Good faith	A Report is considered made in good faith when the Reporter has reasonable grounds to believe that the information reported is true at the time of reporting and does not act maliciously, knowingly provide false information, or seek to cause harm.
Person assisting the Reporter	A person or non-profit organisation who helps a Reporter make a Report or disclose information, in a work-related context, including by providing advice, support or assistance. This includes persons equivalent to “facilitators” under French law and may cover, where applicable, colleagues, trade union representatives, employee representatives, relatives or other persons connected to the Reporter who may face retaliation because of the Report.
Integrity Line Platform	The secure external reporting platform used by the Group to receive Reports, allow secure exchanges with Reporters, keep case information confidential and restrict access to authorised persons only.

4. Who may report?

The reporting system is open to all persons entitled to report under applicable French, US and local laws, including:

- employees, former employees and job applicants, where the information was obtained in the relevant work or recruitment context;
- directors, officers, shareholders and holders of voting rights;
- temporary workers, interns, apprentices, consultants and other external or occasional workers;
- contractors, suppliers and subcontractors, and members of their administrative, management or supervisory bodies and their personnel; and
- any other person entitled to use the system under applicable law.

5. What may be reported?

A Report may concern conduct that has occurred or is very likely to occur, including:

- a crime, offence, breach of law or regulation, or an attempt to conceal such a breach;
- corruption, influence peddling, fraud, theft or misuse of assets;
- competition law, sanctions or export-control breaches;
- an undisclosed conflict of interest;
- serious human rights, health, safety or environmental concerns;
- discrimination, harassment, retaliation or other serious workplace misconduct;
- a breach of the Code of Conduct or another Group policy; or
- a Financial Reporting Concern;
- any other conduct covered under applicable whistleblowing law.

Appendix 1 provides examples of concerns that may be reported under this Policy.

5.1 When is a Report admissible?

A Report may be considered admissible when it meets the following conditions:

- the Report concerns a matter covered by this Policy;
- the Reporter is entitled to use the reporting system under section 4;
- the facts relate to the Group, one of its subsidiaries or its activities;
- the information is provided in good faith and based on reasonable grounds; and
- the Report contains enough factual, serious, precise and relevant information to allow an initial assessment.

A Report may be inadmissible if it is clearly outside the scope of this Policy, is made in bad faith or for malicious purposes, or contains only vague or unsupported allegations that cannot be assessed.

5.2 Financial Reporting Concerns

Financial Reporting Concerns include, for example, improper accounting entries, falsified books or records, misleading financial statements or market disclosures, circumvention or failure of financial controls, auditor independence concerns, or suspected financial fraud. These Reports are routed directly to the Audit Committee.

5.3 Information excluded from the whistleblower regime

A Report must not disclose information protected from disclosure by applicable law. In France, this includes national defence secrecy, medical secrecy, secrecy of judicial deliberations, secrecy of judicial investigations or inquiries, and legal professional privilege. A Reporter may state that protected material exists without uploading or reproducing it.

6. How to report

Reports must be submitted through the Group's external secure reporting platform:

REPORT VIA

Pasqal Integrity Line: <https://pasqal.integrityline.fr/>

- › Available 24 hours a day, 7 days a week
- › Available in English and French Languages

The platform allows the Reporter to submit information and documents, communicate securely with the case handler and follow the status of the Report.

Other internal reporting channels are described in section 7.3.

6.1 Anonymous reporting

Reports may be made anonymously unless anonymity is prohibited by the law of the relevant country. The Group will not seek to identify an anonymous Reporter. An anonymous Reporter should keep the platform access credentials and check the secure mailbox regularly. The ability to investigate may be limited if the information is insufficient or the Reporter cannot be contacted.

6.2 Information to provide

A Reporter should provide facts as clearly and accurately as possible, including relevant dates, locations, persons, supporting documents and potential witnesses. Reporters are not expected to investigate and must not obtain information unlawfully or access records they are not authorised to view.

7. Who handles Reports?

7.1 Group Ethics Committee: general rule

Except for Audit Committee Matters, all Reports are handled by the Group Ethics Committee. It receives and assesses Reports, determines urgency and scope, appoints an appropriate investigator, reviews findings, recommends or decides appropriate action within its authority, and closes the case.

The Group Ethics Committee may delegate specific tasks to a suitably qualified and independent employee or external adviser. Access is limited to persons who need the information to perform an authorised role. Any delegate must sign an enhanced confidentiality undertaking before receiving access to case information.

7.2 Audit Committee: reserved matters

- Financial Reporting Concerns received through the Integrity Line Platform are handled exclusively by the Audit Committee, consistent with the procedures required under the Securities Exchange Act of 1934, as amended, and the Charter of the Audit Committee.

The Integrity Line Platform must be configured so that Financial Reporting Concerns are accessible only to the Chair of the Audit Committee and any other person expressly designated by the Audit Committee. The Ethics Committee has no access to a Financial Reporting Concern unless the Audit Committee expressly authorises it.

The Audit Committee oversees receipt, retention and treatment of Financial Reporting Concerns; determines the investigation approach; may engage independent counsel or experts; reviews material findings and actions; and decides closure. It may delegate investigative work but retains oversight.

Reports presenting a conflict affecting a member of the Ethics Committee are addressed under the conflicts of interest procedure in section 8.

7.3 Other internal reporting channels

As provided in the Code of Business Ethics & Conduct, a person may also raise a Concern with the person they consider most appropriate, such as their manager, Human Resources, a local Compliance Officer or the Compliance Officer. Reports may also be sent in writing to the Ethics Committee.

Managers, Human Resources and local Compliance Officers who receive a Concern that may fall within this Policy must promptly escalate it in writing to the Ethics Committee, or to the Audit Committee where the Concern is an Audit Committee Matter or involves a conflict of interest affecting the person who received it. They must inform the Reporter that the Concern has been escalated, unless doing so would create a risk for the Reporter, another person or the integrity of the review.

A manager or other internal contact who receives a Concern must not investigate the matter alone, promise a specific outcome, alert the person named in the Concern, or share the information beyond those who need to know. If there is any doubt about the correct escalation route, the recipient must contact the Compliance Officer or, for Audit Committee Matters or conflict cases, the Chair of the Audit Committee.

These alternative channels must be used and handled consistently with this Policy, including the rules on confidentiality, data protection, protection against retaliation and conflicts of interest.

8. Conflicts of interest and independence

Any person involved in handling a Report must promptly disclose an actual, potential or apparent conflict of interest and must not access or participate in the matter. Access rights must be removed and the case reassigned. If the conflict concerns a member of the Ethics Committee or that member's direct manager, the Report is transferred to the Audit Committee.

Routing safeguard When there is doubt about the correct route, access must remain restricted and the Chair of the Audit Committee must be consulted before the Report is assigned.

9. How Reports are handled

9.1 Acknowledgement and initial review

The Reporter receives written acknowledgement within seven (7) working days. Each Report then goes through an admissibility review by the competent Committee. This review checks whether the Report falls within the scope of this Policy, whether it concerns a matter that may be reported under section 5, whether the Reporter is entitled to use the reporting system, whether enough information has been provided to conduct an assessment, and whether any conflict of interest or urgent risk requires special handling.

During this first review, the competent Committee may ask the Reporter for additional information through the Integrity Line Platform or any other appropriate secure channel. If the Committee considers, even before the investigation is completed, that the Reporter or another protected person may face a risk to their safety, health, employment or rights because of the Report, appropriate protective measures will be considered and implemented as soon as reasonably possible.

Anonymous Reports are admissible if they concern a matter covered by section 5 and contain facts that are sufficiently serious, precise and detailed to allow an assessment or investigation. Where possible, the anonymous Reporter may be contacted through the secure mailbox to obtain missing information. If the information remains insufficient and the Reporter cannot be contacted, the Report may be closed as inadmissible.

If a Report is considered inadmissible, it is closed and the Reporter is informed in writing of the main reasons, where reasonably possible, within 20 working days. This period may be extended where translation, legal analysis, conflict checks or a more detailed preliminary review are needed.

Reports considered admissible are then investigated or otherwise handled by the competent Committee, or by persons specifically appointed by that Committee, in accordance with the confidentiality, independence and access rules set out in this Policy.

9.2 Emergency situations and evidence preservation

If a Report suggests an immediate risk to health or safety, a risk of retaliation, a risk that evidence may be destroyed, altered or concealed, or a serious legal, financial, regulatory or reputational risk, the competent Committee must consider urgent protective or preservation measures. These measures may include restricting access to information, preserving relevant records, securing electronic data, temporarily adjusting reporting lines or work arrangements, or seeking urgent advice from Legal, Human Resources, Compliance, Data Protection, external counsel or the Audit Committee, as appropriate.

No person may destroy, modify, hide or delete documents, messages, files, accounting records, system logs or any other information that may be relevant to a Report. Where appropriate, the competent Committee may issue a preservation instruction to the relevant persons or functions.

9.3 Investigation

An investigation is conducted when appropriate. It must be impartial, confidential, proportionate, documented and respectful of all persons involved. It may include document and data review, interviews, financial analysis and support from internal or external specialists. The scope may change as facts develop.

9.4 Feedback

Within a reasonable period not exceeding three months from acknowledgement of a Report (or if no notice has been sent, within three months from the expiry of a period of seven working days from the submission of the Report), the Reporter will receive information on action taken or planned to assess the accuracy of the Concern and, where applicable, to address the Concern, as well as the reasons for such action, subject to confidentiality, privacy, legal privilege, business secrecy and the rights of others. The Reporter is not entitled to receive the investigation report or details of individual disciplinary action.

9.5 Outcome, remediation and closure

Actions may include protective measures, control or process improvements, training, disciplinary or contractual measures, recovery of assets, referral to authorities or other proportionate remedial action. Where corrective actions are required, the competent Committee must identify an action owner, expected timing and follow-up method.

A Report is closed when the allegations are inaccurate or unfounded, or when the Report is no longer relevant. Closure and the principal reasons are documented by the competent Committee, and material remediation actions are monitored until completed. The Reporter is notified in writing of the closure of the Report.

10. Protection from retaliation

The Group prohibits Retaliation against a person who reports in good faith, assists a Reporter, provides information, participates in an investigation or refuses to participate in misconduct. Protection applies even if the Concern is not substantiated, provided the Reporter had reasonable grounds to believe the information was true when reported.

Retaliation may include dismissal, discipline, demotion, denial of promotion, unjustified negative evaluation, threats, harassment, discrimination, exclusion, reputational harm or unjustified termination or non-renewal of a contract. Suspected Retaliation must be reported promptly through the Integrity Line Platform and may result in disciplinary action.

Knowingly false, misleading or malicious Reports may lead to action under applicable law. An honest mistake or an unsubstantiated Report made in good faith will not.

11. Rights of persons named in a Report

A person named in a Report is presumed not to have committed misconduct unless and until the facts are established. The person must be treated fairly and may respond to the allegations at an appropriate stage. Notice may be delayed where necessary to protect evidence, witnesses, the Reporter or the integrity of the investigation.

The Reporter's identity will not be disclosed without consent, except where disclosure is required by law. No person has a right to obtain information that would reveal another person's identity or prejudice the investigation.

12. Confidentiality, privacy and records

12.1 Confidentiality

The identities of the Reporter, persons named, witnesses and other participants, together with case information, are shared only on a strict need-to-know basis. Everyone involved must preserve confidentiality. Disclosure may occur where required to investigate, take remedial action, protect rights or comply with law or an authority request.

12.2 Personal data

Personal data is processed in accordance with applicable data protection laws and the Privacy Notice available on the Integrity Line Platform. Only adequate, relevant and necessary data is collected. Access rights are role-based. International transfers are subject to legally required safeguards.

12.3 Retention

Case records are retained only for as long as necessary to handle the Report, implement and monitor action, comply with legal obligations, respond to authorities, or establish, exercise or defend legal rights. Records are then securely deleted, anonymised or archived. The Audit Committee supervises retention arrangements for Financial Reporting Concerns.

13. External reporting

The Group encourages internal reporting so that concerns can be addressed promptly. However, this Policy does not restrict any right to report directly to a competent judicial, administrative, regulatory or other authority, including the French Defender of Rights, competent French or local authorities and European Union bodies, or competent US authorities, where permitted by law. No prior internal Report is required where applicable law permits direct external reporting.

Public disclosure is subject to specific legal conditions. A person considering public disclosure should obtain information on the applicable protection requirements.

14. Misuse of the reporting system and sanctions

The reporting system must be used responsibly. A person who uses it abusively, acts in bad faith, knowingly provides false information or seeks to harm another person may be subject to appropriate action under applicable law and Group rules.

Depending on the seriousness of the facts and the person involved, such action may include disciplinary measures up to termination of employment, claims for damages, or referral to competent authorities.

Examples of conduct that may lead to sanctions include:

- making a Report that is knowingly false, malicious, defamatory or made with the intention to harm;
- disclosing information protected by law, such as national defence secrecy, medical secrecy, legal professional privilege, secrecy of judicial investigations or inquiries, or secrecy of judicial deliberations;
- preventing, obstructing or attempting to obstruct a Report or its handling, by action or inaction;
- breaching the strict confidentiality obligations that apply to the receipt, assessment, investigation or handling of a Report;
- retaliating, threatening to retaliate, or encouraging retaliation against a Reporter, a person assisting the Reporter or a person participating in the handling of a Report.

15. Governance, reporting and review

The Audit Committee is responsible for periodically reviewing this Policy and approving modifications thereto when it deems appropriate.

The Compliance Officer administers this Policy, coordinates communication and training, prepares internal investigation guidelines, prepares practical guidance for managers who receive concerns directly, and monitors the effectiveness of the system. Manager guidance must explain how to listen, preserve confidentiality, avoid retaliation and escalate the concern promptly through the appropriate process. The Group Ethics Committee prepares periodic aggregated reporting on matters within its remit. The Audit Committee receives periodic reporting on Financial Reporting Concerns, conflict cases, timeliness, outcomes and remediation, while preserving confidentiality.

This Policy will be reviewed at least annually during the first two years after implementation, and thereafter periodically or when legal, regulatory or organisational developments require a review.

16. Key performance indicators and continuous improvement

The Group shall monitor the effectiveness of the reporting system through aggregated and anonymised indicators. These indicators are used to identify trends, improve the reporting process, strengthen training, monitor remediation and support periodic reporting to the Group Ethics Committee, the Audit Committee and, where appropriate, the Board of Directors.

Indicators may include, without limitation: the number of Reports received; Reports by category, channel and location where legally permitted; acknowledgement and closure timelines; admissibility and substantiation rates; number of anonymous Reports; retaliation allegations and protective measures; remediation actions and completion status; manager escalation cases; training completion rates; and Financial Reporting Concerns or conflict cases escalated to the Audit Committee.

KPIs must be reviewed carefully and in context. A low number of Reports is not, by itself, evidence that the system is effective. The Group uses KPIs to support continuous improvement while preserving confidentiality, personal data protection and the rights of all persons involved.

17. Questions and effective date

Questions about this Policy may be addressed to the Compliance Officer at ethics@pasqal.com. This Policy takes effect on the date of its adoption by the Board of Directors.

Appendix 1. Examples of reportable concerns

This Appendix gives examples of Concerns that may be reported under this Policy. It is intended to help Reporters understand the types of situations that may fall within the whistleblowing system. The list is not exhaustive. A Concern may still be reported if the Reporter has reasonable grounds to believe that it involves actual or likely misconduct connected with the Group, one of its subsidiaries or its activities.

1. Bribery, corruption and influence peddling

- offering, promising, giving, requesting or receiving an undue advantage;
- payments, gifts, hospitality, donations or sponsorships intended to obtain an improper benefit;
- use of intermediaries, consultants, distributors or agents to make improper payments;
- facilitation payments, unless strictly required to protect immediate safety;
- attempts to influence a public official, customer, supplier or business partner improperly.

2. Fraud, theft and misuse of assets

- falsification of documents, invoices, expense claims, purchase orders or contracts;
- theft, embezzlement or misuse of Group assets;
- improper use of company funds, equipment, data, confidential information or intellectual property;
- deliberate circumvention of approval rules or delegations of authority;
- misappropriation of inventory, equipment, software, research assets or technology.

3. Accounting, internal controls, audit and financial reporting

- inaccurate, false or misleading accounting entries;
- manipulation of financial results, revenue recognition, costs, provisions or cash position;
- concealment of liabilities, losses or off-book arrangements;
- failure or circumvention of internal accounting controls;
- interference with internal or external auditors;
- misleading financial reporting, market disclosures or information provided to investors;
- concerns relating to auditor independence.

These matters are routed to the Audit Committee in accordance with this Policy.

4. Conflicts of interest

- undisclosed personal, family or financial interests in a supplier, customer, partner or competitor;
- participation in a decision where the person has a personal interest;
- preferential treatment of a relative, friend or connected person;
- use of a Group position to obtain a personal benefit;

- external business activities that conflict with the interests of the Group.

5. Competition law and fair dealing

- agreements or discussions with competitors on prices, margins, customers, territories, tenders or market allocation;
- exchange of sensitive commercial information with competitors;
- bid-rigging or coordination in tenders;
- abuse of a dominant position or unfair exclusion of competitors;
- pressure on distributors, suppliers or customers that may breach competition rules.

6. International sanctions, export controls and trade restrictions

- transactions involving sanctioned persons, entities, countries or restricted sectors;
- attempts to bypass sanctions or export-control requirements;
- inaccurate end-user, end-use or destination information;
- shipment, transfer or access to controlled technology without required review or authorisation;
- use of intermediaries, resellers or third parties to conceal a restricted transaction.

7. Human rights, health, safety and environment

- serious health or safety risks;
- failure to follow safety procedures or to report serious incidents;
- forced labour, child labour or serious labour rights concerns in the supply chain;
- serious environmental damage or concealment of environmental incidents;
- unsafe working conditions affecting employees, contractors or third parties;
- serious breach of human rights commitments or responsible business conduct standards.

8. Harassment, discrimination and retaliation

- harassment, bullying, intimidation or humiliating conduct;
- discrimination based on legally protected characteristics;
- retaliation against a person who raised a Concern, assisted a Reporter or participated in an investigation;
- threats, demotion, exclusion, negative treatment or pressure linked to a Report;
- obstruction of a person's ability to report a Concern.

9. Data protection, cybersecurity and confidential information

- unauthorised access, use, disclosure or transfer of personal data;
- failure to report a suspected data breach;
- misuse or disclosure of confidential business information;
- unauthorised access to systems, files, accounts or restricted information;
- intentional weakening or bypassing of cybersecurity controls;

- improper use of confidential information for personal or third-party benefit.

10. Scientific integrity, research, technology and product integrity

- falsification, manipulation or concealment of research, testing or technical results;
- misrepresentation of product performance, quality, reliability or security;
- failure to report a serious technical, safety or quality issue;
- misuse of research funds, grants or public funding;
- improper access to or disclosure of sensitive technology, know-how or research data;
- deliberate non-compliance with applicable technical, security or quality requirements.

11. Serious breach of Group policies or Code of Conduct

- serious or repeated breach of the Code of Business Conduct & Ethics;
- violation of the anti-corruption, data protection, information security or other internal policies;
- instructions to ignore or bypass Group policies;
- concealment of a policy breach;
- failure by a manager to escalate a serious Concern received directly.

12. Attempts to conceal misconduct or obstruct a Report

- destroying, modifying, hiding or deleting relevant documents, emails, messages, records or system logs;
- pressuring a person not to report or to withdraw a Report;
- intimidating witnesses or persons involved in a review;
- disclosing the identity of a Reporter without authorisation;
- interfering with an investigation or providing knowingly false information.

If a person is unsure whether a situation should be reported under this Policy, they may seek advice from the Compliance Officer or use the Integrity Line Platform. Reporters are not expected to prove the facts before reporting. They should provide information that is as factual, precise and complete as possible, based on reasonable grounds and in good faith.

Appendix 2. Routing guide

This guide helps determine which body should receive and handle a Report. When there is any doubt about the correct route, access must remain restricted and the Chair of the Audit Committee must be consulted before assignment.

Route	Typical matters	Access and decision
Ethics Committee	Ethics and compliance; corruption; non-financial fraud; workplace conduct; human rights; health, safety and environment; policy breaches.	Handled by the Ethics Committee. It may appoint an independent internal or external investigator where appropriate.
Audit Committee	Financial Reporting Concerns; Reports or other matters that present a conflict affecting a member of the Ethics Committee.	Access limited to the Chair of the Audit Committee and authorised Audit Committee recipients. The Audit Committee retains oversight and closure authority.
Manager or other internal contact	Concerns raised directly with a manager, Human Resources, a local Compliance Officer or the Compliance Officer, as provided in the Code of Business Ethics & Conduct.	The recipient must preserve confidentiality, avoid retaliation and promptly escalate the Concern in writing to the Ethics Committee, or to the Audit Committee for Audit Committee Matters or conflict cases.
Uncertain route	Any case where classification, seriousness, access rights or independence is unclear.	Keep access restricted. Consult the Chair of the Audit Committee before assigning the Report.

Appendix 3. Whistleblowing FAQ

This FAQ is a practical guide for Reporters, managers and persons involved in handling a Report. It summarises the main steps of the Policy and does not replace the Policy itself.

Integrity Line Platform	Reports may be submitted through the secure platform at: https://pasqal.integrityline.fr/
Questions	Questions about this Policy or the reporting process may be addressed to the Compliance Officer at: ethics@pasqal.com

Question	Operational answer
Who can use the Integrity Line?	Any person entitled to report under applicable French, US or local law, including employees, former employees, applicants, directors, officers, shareholders, interns, temporary workers, consultants, suppliers and contractors.
What should be reported?	Actual or likely misconduct connected with the Group, including corruption, fraud, conflicts of interest, sanctions or export-control breaches, serious workplace misconduct, retaliation, data protection concerns, serious health, safety or environmental risks and Financial Reporting Concerns.
Can I report anonymously?	Yes, unless prohibited by applicable local law. If you report anonymously, keep your platform credentials and check the secure mailbox regularly, because the case handler may need additional information.
What information should I provide?	Provide clear facts: what happened, when, where, who was involved, who may have witnessed it, what documents exist and why you believe the concern is serious. Do not investigate yourself or access information unlawfully.
What happens after I submit a Report?	You receive written acknowledgement within seven working days. The competent Committee then checks admissibility, urgency, conflicts of interest and routing. If the Report is admissible, it is assessed or investigated according to the Policy.
Will I receive feedback?	Yes. Within a reasonable period not exceeding three months from acknowledgement, you receive information on action taken or planned, subject to confidentiality, privacy, privilege, business secrecy and the rights of others.
Who handles my Report?	Most Reports are handled by the Group Ethics Committee. Financial Reporting Concerns and certain conflict cases are handled by the Audit Committee. Access is limited to authorised persons on a strict need-to-know basis.
What if I report to my manager instead?	The manager must listen, preserve confidentiality, avoid any retaliation, avoid investigating alone and promptly escalate the

Question	Operational answer
	Concern in writing to the Ethics Committee or, where relevant, to the Audit Committee.
Am I protected from retaliation?	Yes, if you report in good faith and have reasonable grounds to believe the information is true at the time of reporting. Protection also covers persons assisting the Reporter and persons participating in the handling of a Report.
Can I report externally?	Yes, where permitted by law. The Policy does not restrict the right to report to competent judicial, administrative, regulatory, European Union or US authorities. Public disclosure is subject to specific legal conditions.