

COMPLIANCE HOUSE

Our Code of Conduct



Integrity. Independence. Responsibility.

ISO
37301
CERTIFIED

ISO
37001
CERTIFIED



Our standards begin with us.

We established Compliance House to help organisations make integrity and compliance part of everyday decisions. That responsibility begins with our own conduct.

Our advice must be honest, independent and grounded in evidence. Commercial pressure never justifies changing findings, concealing risks or overstating our capabilities. Sometimes the right decision is to decline an engagement or pause work already underway.

I ask every colleague to seek guidance when uncertain and speak up when something seems wrong. Leaders must listen and protect people who raise concerns from retaliation. This Code is our commitment to practise the standards we recommend to others.

Tayfun Zaman
Founder · Compliance House





We examine the path together.

In the Sherpa Program, guidance does not mean deciding for the client. It means understanding the conditions, making risks visible and supporting informed choices. We carry that same responsibility in our own work.

Understand the conditions.

Compare claims with evidence and make gaps in our knowledge explicit.

Choose a responsible path.

Select safeguards that protect our independence, people and information.

Take responsibility together.

Raise concerns early, learn from outcomes and improve how we work.

Your guide to conduct

19 risk areas. A policy and ten practical actions for each.

01 Anti-bribery and corruption	5
02 Gifts, hospitality and expenses	6
03 Conflicts of interest and independence	7
04 Professional quality and truthful claims	8
05 Fraud, financial integrity and tax	9
06 Money laundering and illicit finance	10
07 Sanctions and cross-border trade	11
08 Fair competition and market conduct	12
09 Third parties and responsible procurement	13
10 Confidentiality and personal data	14
11 Cybersecurity and software integrity	15
12 Responsible artificial intelligence	16
13 Human rights and labour standards	17
14 Respect, inclusion and fair employment	18
15 Health, safety and wellbeing	19
16 Environment and responsible resource use	20
17 Intellectual property and public communications	21
18 Political activity, donations and public affairs	22
19 Speaking up, investigations and records	23

24 Decision guide · 25 Speaking up · 26 Accountability · 27 Commitment



01 / Anti-bribery and corruption

We prohibit bribery, kickbacks and facilitation payments, directly or through others, in public and private business.

Our work can involve procurement teams, public officials, referral partners and decision-makers whose choices affect our business. No commercial opportunity justifies offering, requesting or accepting an improper advantage, whether money, employment, a personal favour or another benefit. This applies equally to payments made by someone acting for us. Fees must reflect legitimate services and be supported by clear records. Where a demand or arrangement raises concern, we pause the transaction, seek guidance and document the response. A threat to personal safety requires a safety-first response followed by reporting as soon as it is safe.

DO

- 01 Check the purpose of every payment.
- 02 Verify recipients and supporting records.
- 03 Escalate demands for unofficial payments.
- 04 Record interactions with public officials accurately.
- 05 Prioritise safety under threats and report when safe.

DON'T

- 01 Offer anything to influence a decision improperly.
- 02 Accept a kickback for a referral or purchase.
- 03 Use an intermediary to make a prohibited payment.
- 04 Disguise bribes as consulting fees or donations.
- 05 Treat customary practice as permission to pay.



02 / Gifts, hospitality and expenses

Business courtesies must be modest, transparent, lawful and free from any expectation of preferential treatment.

Hospitality can support a professional relationship, but it can also create an obligation or the appearance of influence. We assess the purpose, value, frequency, timing and participants together, including whether a tender, selection or assessment is underway. An offer that seems modest in isolation may be inappropriate when repeated or extended to relatives. We follow the recipient's restrictions as well as our own approval requirements. Expenses must have a genuine business purpose, and declining an inappropriate offer must never disadvantage the person who raises the concern.

DO

- 01 Check both our rules and the recipient's rules.
- 02 Seek approval before sensitive or unusual hospitality.
- 03 Record the value, recipient and business purpose.
- 04 Decline offers that could compromise your judgment.
- 05 Submit accurate receipts for legitimate expenses.

DON'T

- 01 Give or accept cash or cash equivalents as gifts.
- 02 Offer hospitality to influence a tender or review.
- 03 Split expenses to bypass approval.
- 04 Charge personal entertainment to a client.
- 05 Assume an invitation is acceptable because it is reciprocal.



03 / Conflicts of interest and independence

We disclose and manage actual, potential and perceived conflicts before they affect advice, procurement or client acceptance.

Clients rely on us to exercise judgment without hidden loyalties. Personal relationships, investments, outside work, referral arrangements and software sales incentives can all affect that judgment or how it is perceived. Disclosure is therefore required before participation in a relevant decision, not only after a conflict causes harm. We assess whether the conflict can be managed through separation of responsibilities, independent review or appropriate disclosure and consent. Consent alone does not make every conflict acceptable. If credible safeguards cannot protect independent judgment and confidentiality, we decline or end the affected work.

DO

- 01 Disclose relevant financial and personal interests.
- 02 Check conflicts before accepting an engagement.
- 03 Step back from decisions involving connected parties.
- 04 Document safeguards and necessary client disclosures.
- 05 Update disclosures when circumstances change.

DON'T

- 01 Hide an outside role or competing interest.
- 02 Recommend software because of an undisclosed incentive.
- 03 Review your own work as if independently assured.
- 04 Favour relatives or friends in commercial decisions.
- 05 Use client relationships for undisclosed personal gain.



04 / Professional quality and truthful claims

Our advice, training and software claims must be evidence-based, within our competence and clear about their limitations.

Our reputation depends on whether clients can use our work to make sound decisions. We define the question being addressed, the evidence available and the boundaries of each engagement. Advice must reflect the client's circumstances rather than simply repeat a template. Training must have relevant learning objectives, and software must be described according to its tested capabilities. We distinguish legal requirements, professional judgment and illustrative guidance. Significant limitations and contrary evidence belong in our conclusions. Where specialist competence is needed, we obtain it rather than imply expertise we do not possess.

DO

- 01 Agree scope, deliverables and responsibilities in writing.
- 02 Verify sources and distinguish facts from assumptions.
- 03 Use qualified reviewers for material deliverables.
- 04 Explain tool scores, uncertainty and limitations.
- 05 Correct material errors and inform affected clients.

DON'T

- 01 Guarantee certification or regulatory approval.
- 02 Present self-assessment as independent certification.
- 03 Invent credentials, findings or client endorsements.
- 04 Omit adverse findings to preserve a sale.
- 05 Accept work beyond competence without suitable support.



05 / Fraud, financial integrity and tax

We maintain complete, accurate records and prohibit fraud, false billing, asset misuse and assistance with tax evasion.

Financial integrity includes how we propose, deliver, record and charge for our services. Clients and colleagues must be able to trace charges to agreed work and understand who approved a commitment. We separate preparation and approval where practicable, review exceptions and retain evidence sufficient to explain transactions. Performance targets must not encourage inflated hours, misleading revenue recognition or concealed liabilities. Company resources are entrusted to us for authorised purposes. Suspected fraud requires careful preservation of records and appropriate review, not informal adjustments that hide the underlying issue.

DO

- 01 Record time, expenses and revenue accurately.
- 02 Follow delegated approval limits.
- 03 Reconcile invoices with agreed services.
- 04 Preserve reliable accounting and tax records.
- 05 Report unexplained transactions or discrepancies.

DON'T

- 01 Bill for work not performed.
- 02 Alter receipts, dates or performance records.
- 03 Create undisclosed accounts or off-book funds.
- 04 Use company or client assets for unauthorised purposes.
- 05 Help conceal income or falsify tax information.



06 / Money laundering and illicit finance

We seek to understand who we work with and reject arrangements that disguise criminal proceeds or illicit funding.

Professional services can be misused to lend credibility to questionable entities or to explain movements of funds that lack a genuine commercial basis. Our checks therefore consider ownership, the nature of the requested work, payment arrangements and inconsistencies in the information supplied. The depth of review should reflect the risk and applicable obligations; it is not a claim that every engagement is subject to identical regulated-sector duties. We do not proceed merely because payment is available or a client is well known. Unresolved concerns require escalation and, where necessary, refusal or lawful reporting.

DO	DON'T
01 Verify client identity and relevant ownership information.	01 Accept unexplained third-party payments.
02 Understand the commercial purpose of engagements.	02 Return funds to unrelated accounts without verification.
03 Check unusual payment sources and refund requests.	03 Structure transactions to evade checks.
04 Escalate concerns before proceeding.	04 Provide services to conceal illicit ownership or funds.
05 Follow applicable reporting requirements with specialist advice.	05 Warn subjects of a confidential inquiry where disclosure is prohibited.



07 / Sanctions and cross-border trade

We assess applicable sanctions, export controls and cross-border restrictions before providing services, software or technical assistance.

Cross-border exposure may arise through client ownership, connected banks, technology access, subcontractors or the eventual use of our advice. We examine the restrictions relevant to the jurisdictions and activities involved rather than assume one screening list provides a complete answer. Controls must consider indirect ownership, service restrictions and changes during the engagement. A request to remove a country reference or introduce an unexplained intermediary is a reason for further review. We do not design structures to evade restrictions or give assurance beyond the facts and specialist analysis available.

DO

- 01 Check parties, ownership, destinations and end use.
- 02 Reassess exposure when facts or restrictions change.
- 03 Seek specialist advice on uncertain restrictions.
- 04 Document checks and required authorisations.
- 05 Pause potentially restricted work pending review.

DON'T

- 01 Rely only on a name-screening result.
- 02 Use intermediaries to evade restrictions.
- 03 Conceal destinations, owners or end users.
- 04 Assume advisory services are always exempt.
- 05 Promise a transaction is lawful without adequate review.



o8 / Fair competition and market conduct

We compete on quality and value, safeguard competitively sensitive information and prohibit collusion and misuse of inside information.

We may meet competitors through conferences, professional networks, partnerships and joint proposals. These settings do not justify sharing information that reduces independent competition. We distinguish legitimate collaboration from arrangements that coordinate prices, customers or bidding behaviour, and seek review where the boundary is unclear. Information obtained through client work must not become an advantage in personal trading or another engagement. Confidentiality continues after the project ends. When a discussion becomes improper, silence is not sufficient: we make our objection clear, leave where appropriate and report the incident.

DO

- 01 Set prices and commercial terms independently.
- 02 Use legitimate sources for market research.
- 03 Leave and report improper competitor discussions.
- 04 Protect non-public information about client transactions.
- 05 Review joint bids and collaborations for competition risk.

DON'T

- 01 Agree prices, bid outcomes or customer allocation with competitors.
- 02 Exchange future pricing or confidential strategies.
- 03 Obtain competitor secrets through deception.
- 04 Trade securities using inside information.
- 05 Tip others about confidential market-sensitive developments.



09 / Third parties and responsible procurement

We select and monitor partners, instructors, suppliers and subcontractors using proportionate integrity and capability checks.

Others who represent us can affect our clients and reputation as directly as our own employees. Selection must therefore consider integrity, competence, security and the ability to meet agreed standards, not price alone. We apply checks proportionate to the service and exposure, set clear contractual expectations and review material changes over time. Outsourcing does not transfer away our responsibility to exercise oversight. Where concerns arise, we evaluate the severity, available remedies and consequences of continuing the relationship, documenting why corrective action, suspension or termination is appropriate.

DO	DON'T
01 Assess risk before onboarding a provider.	01 Outsource prohibited conduct.
02 Verify qualifications, ownership and references where relevant.	02 Skip checks because a supplier is recommended by a client.
03 Include confidentiality and conduct requirements in contracts.	03 Accept unexplained fees or vague deliverables.
04 Monitor performance and significant changes.	04 Allow unauthorised subcontracting or data access.
05 Address concerns through corrective action or disengagement.	05 Ignore credible misconduct because replacement is inconvenient.



10 / Confidentiality and personal data

We protect client and personal information throughout its lifecycle and use it only for authorised, lawful purposes.

Compliance work can reveal allegations, employee details, commercial strategies and sensitive evidence. Access to that information is a responsibility, not permission to use it freely. We define the purpose of collection, limit what we request and establish appropriate access, retention and disposal arrangements. Client material must remain separated where necessary, including in demonstrations and training. Personal data rights and contractual confidentiality both require attention. Before sharing information with a platform, supplier or another country, we check the relevant safeguards and authorisations. Suspected exposure is escalated promptly so that containment and any required notifications can be assessed.

DO

- 01 Collect only information necessary for the task.
- 02 Confirm the lawful basis and required notices.
- 03 Restrict access to people with a business need.
- 04 Use approved storage, transfer and deletion methods.
- 05 Report suspected data exposure promptly.

DON'T

- 01 Reuse client data for another engagement without authorisation.
- 02 Publish client names, logos or cases without permission.
- 03 Discuss confidential matters in public places.
- 04 Keep personal data indefinitely for convenience.
- 05 Transfer data across borders without checking requirements.



11 / Cybersecurity and software integrity

We protect systems and client evidence through secure access, careful development and prompt incident response.

Our websites, tools and document-sharing arrangements must be designed around the information they handle and the harm that unauthorised access could cause. Security involves clear permissions, secure configuration, tested recovery arrangements and careful management of changes. A feature is not ready simply because it functions in a demonstration. We consider how it behaves with real client information, errors and misuse. Suppliers and integrations require similar scrutiny. When an incident occurs, the priority is containment, preservation of relevant evidence and coordinated communication, rather than hiding the issue or making unverified assurances.

DO	DON'T
01 Use strong unique credentials and multifactor authentication.	01 Share passwords or access tokens.
02 Keep approved devices and software updated.	02 Store confidential evidence in publicly accessible folders.
03 Test access controls, backups and relevant security measures.	03 Disable security controls for convenience.
04 Review software changes before release.	04 Install unapproved software or use untrusted devices for client work.
05 Report phishing, lost devices and vulnerabilities promptly.	05 Hide a breach or promise absolute security.



12 / Responsible artificial intelligence

We use AI with human accountability, appropriate data safeguards and verification proportionate to the consequences of its use.

AI can assist research, drafting, analysis and software development, but it does not carry our professional responsibility. We assess each use by its impact on people, confidentiality and the reliability of the resulting advice. Review must be substantive: a person approving an output must be able to challenge its sources, logic and conclusions. We consider provider data practices, intellectual property, bias and the need to explain AI-supported work to clients. Where adequate verification or safeguards are unavailable, we limit or avoid the use. Efficiency never justifies presenting uncertain machine-generated content as established fact.

DO

- 01 Use approved AI tools for defined purposes.
- 02 Verify generated facts, citations and recommendations.
- 03 Check outputs for bias and unfair effects.
- 04 Keep a qualified person responsible for material decisions.
- 05 Explain material AI use and limitations when relevant.

DON'T

- 01 Upload confidential data to an unapproved model.
- 02 Present fabricated sources as verified research.
- 03 Delegate consequential judgments entirely to AI.
- 04 Generate deceptive impersonations or endorsements.
- 05 Assume AI output is lawful, accurate or owned by us.



13 / Human rights and labour standards

We respect human rights and seek to prevent, address and avoid contributing to abuses in our operations and business relationships.

Human rights considerations extend beyond our own workplace to the clients, suppliers and activities with which our services are connected. We pay attention to vulnerable people and to circumstances in which our work could enable, legitimise or conceal harm. Reviews should consider the severity of potential impacts, not only the commercial risk to Compliance House. Where we identify concerns, we use the influence available to prevent or reduce harm and assess appropriate remedy. Disengagement decisions must also consider their effects on people. We do not treat contractual assurances as a substitute for examining credible evidence of abuse.

DO

- 01 Consider human rights impacts in client and supplier reviews.
- 02 Check for forced labour, child labour and exploitation risks.
- 03 Respect lawful worker representation and association.
- 04 Listen to affected people and escalate credible concerns.
- 05 Support appropriate remedy where we cause or contribute to harm.

DON'T

- 01 Retain identity documents to restrict a worker's freedom.
- 02 Tolerate coercion, trafficking or exploitative recruitment fees.
- 03 Ignore abuse because it occurs at a subcontractor.
- 04 Obstruct legitimate worker concerns or representation.
- 05 Provide advice intended to conceal human rights abuses.



14 / Respect, inclusion and fair employment

We maintain a respectful workplace and learning environment, free from discrimination, harassment, bullying and retaliation.

Respectful conduct is required in offices, client premises, training sessions, travel and digital communications. Seniority, commercial importance or a successful track record does not excuse intimidation or exclusion. We aim to make opportunities and participation accessible through fair criteria and reasonable adjustments. Managers must respond to concerns without blaming the person affected or assuming that informal behaviour is harmless. Complaints require attention to dignity, fairness and the rights of everyone involved. A person should be able to disagree professionally, ask for help or report inappropriate conduct without fear of losing opportunities.

DO	DON'T
01 Base recruitment and advancement on relevant merit.	01 Discriminate on personal characteristics unrelated to the role.
02 Use respectful language in person and online.	02 Make unwanted sexual comments, advances or contact.
03 Consider reasonable accessibility and accommodation needs.	03 Humiliate colleagues, clients or training participants.
04 Intervene safely or seek support when misconduct occurs.	04 Exclude people as punishment for raising concerns.
05 Handle complaints fairly and sensitively.	05 Dismiss abusive behaviour as humour or commercial pressure.



15 / Health, safety and wellbeing

We plan work, travel and events to protect physical and psychological wellbeing and prevent avoidable harm.

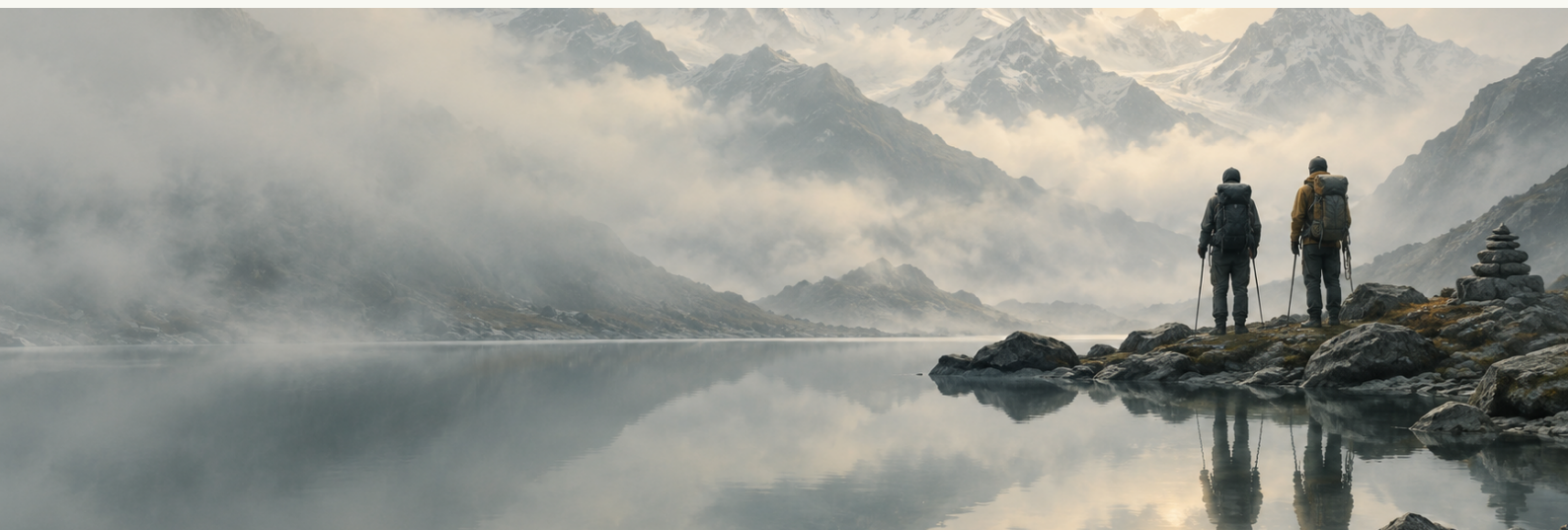
Our work may involve intensive deadlines, remote working, travel and unfamiliar client locations. We assess these conditions before they create avoidable harm, including fatigue, isolation and psychological pressure. Everyone has a responsibility to follow relevant precautions and raise concerns, while leaders must provide realistic workloads and respond to unsafe conditions. Client deadlines do not override safety. Incident and near-miss reporting is used to learn and improve, not to discourage disclosure. Where specialist or emergency support is needed, obtaining that support takes priority over maintaining the appearance of uninterrupted service.

DO

- 01 Assess risks before travel and on-site activities.
- 02 Follow venue safety and emergency procedures.
- 03 Report hazards, incidents and near misses.
- 04 Manage workload and fatigue responsibly.
- 05 Stop unsafe work and seek assistance.

DON'T

- 01 Pressure anyone to continue in unsafe conditions.
- 02 Work or drive while impaired.
- 03 Ignore signs of severe stress or exhaustion.
- 04 Block exits or bypass safety instructions.
- 05 Conceal injuries or discourage incident reporting.



16 / Environment and responsible resource use

We seek to reduce the environmental impact of our operations and make environmental claims only when supported by evidence.

Although our services are primarily knowledge-based, travel, digital infrastructure, equipment and purchasing have environmental consequences. We consider practical ways to reduce avoidable consumption without shifting impacts out of sight. Decisions should take account of the useful life and responsible disposal of equipment as well as immediate cost. Environmental reporting must distinguish measured results, estimates and aspirations. We avoid overstating the effect of individual actions or suppliers' claims. Where we advise clients on environmental matters, we stay within our competence and communicate the evidence and limitations behind our conclusions.

DO	DON'T
01 Consider lower-impact travel and meeting options.	01 Make unsupported carbon-neutral or sustainability claims.
02 Reduce avoidable energy, paper and material use.	02 Dispose of batteries or devices with confidential data carelessly.
03 Dispose of electronic equipment through suitable channels.	03 Hide adverse environmental impacts in reports.
04 Consider environmental practices when choosing suppliers.	04 Treat offsets as a substitute for examining actual impacts.
05 Keep evidence for environmental performance statements.	05 Misrepresent estimates as measured results.

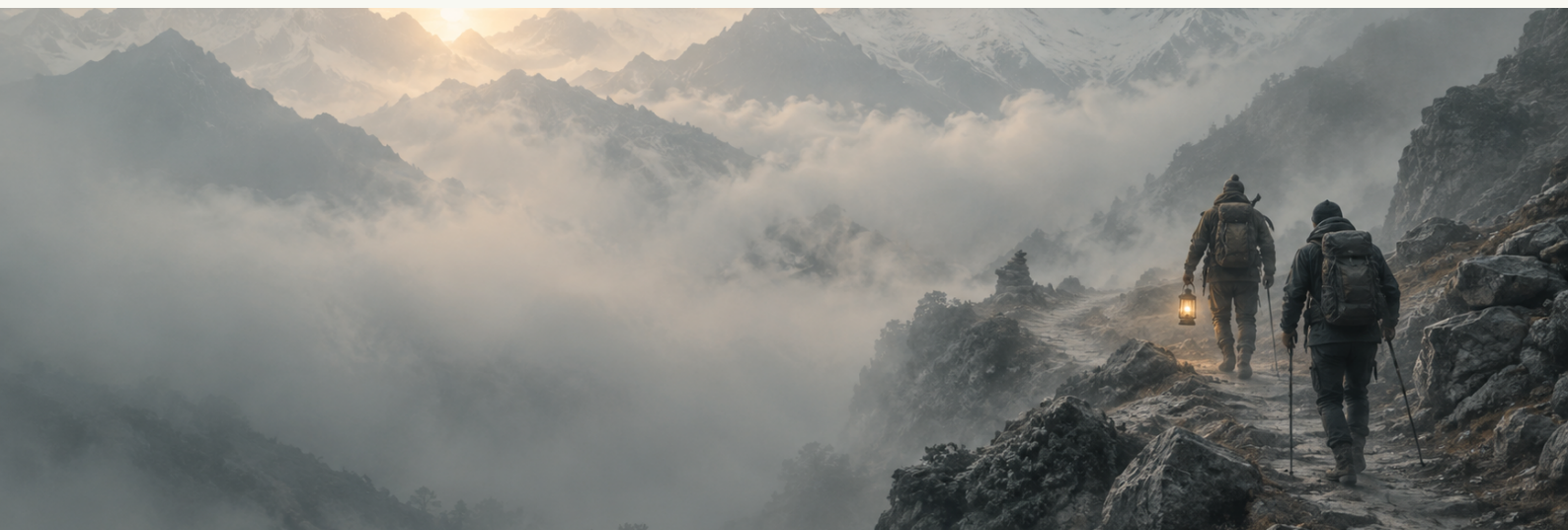


17 / Intellectual property and public communications

We respect ownership and licensing rights and communicate accurately about our work, clients and capabilities.

Our materials combine original work with sources, standards, software and images that may carry separate rights. We establish what may be used, adapted, shared or sold before incorporating it into a deliverable. Attribution does not replace a required licence or permission. Public communication must accurately describe our experience, certifications and relationships, including on social media and in demonstrations. Approval to work for a client is not automatically approval to publicise that relationship. When an error or rights issue is identified, we correct the material and address affected distributions rather than simply remove the local copy.

DO	DON'T
01 Check rights before using standards, images or course materials.	01 Copy proprietary materials without permission.
02 Attribute sources and respect licence conditions.	02 Publish confidential deliverables as marketing examples.
03 Agree ownership and permitted reuse in client contracts.	03 Imply that management system certification endorses every service.
04 Obtain approval for statements on behalf of the company.	04 Claim a client endorsement beyond the permission given.
05 Correct misleading public statements promptly.	05 Present personal opinions as official company positions.



18 / Political activity, donations and public affairs

Political engagement and charitable support must be transparent, properly authorised and never used to secure improper business advantage.

Community support and participation in public debate must remain separate from improper influence. A contribution can create risk even when the recipient is a legitimate organisation, particularly if a client or official requests it during a business decision. We examine the actual beneficiary, purpose and connection to pending matters before approval. Personal political choices remain personal and must not become a condition of employment or business access. Company representation in public affairs requires a clear mandate, accurate statements and records sufficient to explain what was supported and why.

DO	DON'T
01 Keep personal political activity separate from work.	01 Donate to influence a procurement or regulatory decision.
02 Check donation recipients and intended use.	02 Use company resources for personal campaigning without authority.
03 Seek approval for company-funded contributions or sponsorships.	03 Pressure colleagues to support a political cause.
04 Record relevant contacts and expenditure accurately.	04 Hide the beneficiary of a sponsorship.
05 Check applicable restrictions on lobbying and contributions.	05 Claim that personal political views represent Compliance House.



19 / Speaking up, investigations and records

We encourage good-faith concerns, prohibit retaliation and protect fair, impartial fact-finding and relevant records.

Early reporting allows concerns to be assessed before harm grows. A reporter is not expected to prove a breach or conduct an investigation before seeking help. We distinguish an honest concern that cannot be substantiated from a deliberately false allegation. Reviews must be proportionate, impartial and respectful of privacy and procedural fairness. Relevant evidence must remain intact, including when normal deletion schedules would otherwise apply. Information is shared only as needed for legitimate handling and legal duties. Decisions and corrective actions should be documented, and lessons used to improve controls rather than focus solely on individual blame.

DO	DON'T
01 Raise concerns promptly with available facts.	01 Retaliate against a reporter, witness or person seeking advice.
02 Preserve relevant records and follow retention instructions.	02 Knowingly make false allegations.
03 Share case information only with authorised people.	03 Delete, alter or conceal evidence.
04 Cooperate honestly with authorised reviews.	04 Conduct unauthorised surveillance or access private accounts.
05 Disclose investigator conflicts and seek impartial handling.	05 Promise absolute secrecy or prejudge an allegation.



When in doubt, pause.

1 / Understand the situation

What facts do you know? Who could be affected? What information is missing?

2 / Test the decision

Is it lawful? Does it protect independence? Is it supported by evidence? Does it protect people and information?

3 / Seek guidance and document

Pause where uncertainty remains. Seek appropriate guidance and record the rationale and safeguards. Internal approval cannot authorise unlawful conduct.



Advice and speaking up

Ethics Hotline

ethics@compliancehouse.net

Use this address to seek ethics guidance or report suspected misconduct. Describe the facts you know and any relevant dates. Before sharing sensitive documents, request a secure transfer method. If the concern involves those managing this mailbox, seek a conflict-free recipient or independent advice.

Information should be shared only on a need-to-know basis, subject to investigation needs and legal obligations. Good-faith reporting should be protected even if a concern is not substantiated. This Code does not restrict lawful external reporting rights. Contact local emergency services where there is immediate danger.



Implementation and accountability

Management should assign responsibility for implementation, training, controls and handling concerns. Breaches should be reviewed impartially, with corrective action and, where appropriate, proportionate disciplinary or contractual measures consistent with applicable law. The Code should be reviewed at least annually and after significant changes.



In every decision.

Scope

This Code applies to the founder, leaders and employees. Others acting for us are expected to follow the requirements relevant to their work.

My responsibility

I am responsible for understanding the Code, applying it in my work, asking for guidance and raising concerns in good faith.

Document status

Approved by the Board - October 2026



COMPLIANCE HOUSE

Integrity.
Independence.
Responsibility.

compliancehouse.net | info@compliancehouse.net

Ethics Hotline: ethics@compliancehouse.net