Saint-Gobain UK and Ireland Counter Fraud Policy

1. Purpose

This policy sets out the framework for preventing, detecting, and responding to fraud within Saint-Gobain entities in the UK & Ireland. It aligns with the Saint-Gobain Group's "Policy to Prevent Fraud in the Activities of the Saint-Gobain Group" but incorporates UK legal obligations under the Fraud Act 2006 and the Economic Crime and Corporate Transparency Act 2023 as well as the Republic of Ireland, primarily governed by the Criminal Justice (Theft and Fraud Offences) Act 2001.

2. Scope

This policy applies to:

- All UK and Ireland based employees, contractors, agents, subsidiaries, and other associated persons.
- All business units and functions operating in or through the UK and Ireland.
- All types of fraud, including internal, external, and third-party fraud irrespective of Saint-Gobain being a victim or a beneficiary.

3. Definitions

- **Fraud**: Dishonest acts intended to gain advantage or cause loss, including false representation, failure to disclose information, and abuse of position.
- **Associated Person**: Any individual or entity performing services for or on behalf of the organisation (e.g., employees, agents, contractors, subsidiaries).
- **Senior Manager**: Anyone with significant decision-making or operational responsibilities, regardless of board-level status.

4. Policy Statement

Saint-Gobain is committed to:

- Conducting all business in an honest and ethical manner. Ethical business practices are not only necessary for preserving our reputation and improving business overall, but also for adhering to the law. We take a zero-tolerance approach to fraud and are committed to acting professionally, fairly and with integrity in all our business dealings and relationships wherever we work and implementing and enforcing effective systems to counter fraud.
- Upholding all laws relevant to countering fraud in all the jurisdictions in which we operate. Compliance with UK laws including the Bribery Act 2010, The Criminal Finances Act 2017, the Fraud Act 2006 and the Economic Crime and Corporate Transparency Act 2023 as well as for the Republic of Ireland the Criminal Justice (Theft and Fraud Offences) Act 2001, the Criminal Justice Act 1992 and applicable EU Directives and regulations which form part of the laws of the Republic of Ireland.
- Having a fraud prevention framework supported by the following six pillars:
    1. top level commitment
    2. risk assessment
    3. proportionate risk-based prevention procedures
    4. due diligence
    5. communication (including training)
    6. monitoring and review
- A Whistleblowing Policy designed to enable Saint-Gobain's employees, temporary workers, agency workers, officers, consultants, contractors, interns, trainees, apprentices, volunteers, customers, suppliers and other stakeholders (any individual or organisation affected by the decisions made by Saint-Gobain) to raise genuine concerns which relate to suspected wrongdoing or dangers at work.

5. Top-Level Commitment

Regional and Business Management Teams

- Managing Directors through their senior managers actively promote a culture of integrity and respect for the law.
- Managing Directors must ensure the Principles of Conduct and Action are communicated and upheld, and risk management processes prioritise internal control support.
- The organisation must ensure clear responsibilities with proper segregation of duties and controlled delegation of powers.
- Internal control procedures should be defined, understood by relevant employees, with training provided as needed.
- The Internal Control Reference Framework must be integrated and aligned with major risks and control activities.

- Adaptation of controls should be made, if necessary, with compensatory measures in place if controls cannot be applied.
- Managing Directors are responsible for periodic evaluations of the internal control system and its performance, giving clear guidance and accountability for fraud prevention.
- Through the annual Compliance Statement, the Managing Director must provide assurance:
    - They have implemented these controls properly and efficiently,
    - The action plans arising from the self-assessment have been activated and implemented within the given time frame,
    - Major internal control incidents, fraud and violations of the Principles of Conduct and Action have been reported to the Chief Compliance and Business Ethics Officer and General Counsel.

Management:

- Managers at every level of management must make sure they convey to all the employees concerned, on a timely basis, all the relevant information so they can perform their duties effectively.
- The objectives and procedures to counter fraud and risk management system of the business units are clearly communicated to the employees so they understand and adhere to the organisation's policy regarding risks and control.

All Employees and Associated Persons:

- The Principles of Conduct and Action constitute the Code of Ethics and the foundation of all our policies and commitments. They define the values and rules applicable to all entities, business units and employees, regardless of the nature of their employment contract (permanent, fixed term or temporary), as well as to our subcontractors and suppliers
- Report suspected fraud via designated channels.
- Cooperate with investigations.

6. Risk Assessment

Saint-Gobain Group has progressively developed its Risk Universe, published in the annual Internal Control Reference Framework, reinforcing the risk approach within the internal control process.

The Risk Universe has three main objectives:

1. Provide support for risk identification,
2. Assist the entity General Managers with the elaboration of their general risks analysis,
3. Indicate the risk categories corresponding to the controls included within the Internal Control Reference

The Fraud Triangle (Appendix 1) is a powerful conceptual tool to understand and mitigate the risk of fraudulent behaviour. It consists of three elements:

1. **Pressure (or Incentive)** - This refers to the motivation or incentive to commit fraud, which could be financial, professional, or personal. Businesses must:
    a. Identify areas where employees may face financial stress (e.g. bonus structures, personal debt).
    b. Assess performance targets that may be unrealistic or overly aggressive.
    c. Consider external pressures such as economic downturns or industry instability.
2. **Opportunity** - Fraud occurs when individuals perceive they can commit and conceal wrongdoing. Businesses must:
    a. Evaluate internal controls and segregation of duties.
    b. Review access rights to financial systems and sensitive data.
    c. Assess the effectiveness of audit trails and monitoring mechanisms.
    d. Identify weak spots in oversight, especially in remote or decentralised operations outside of the Professional Services and Shared Service Centres.
3. **Rationalisation** - This is the motivation for individuals to commit fraudulent actions and to counter these businesses must:
    a. Gauge ethical culture, questioning if misconduct is tolerated or excused?
    b. Review tone from the top ensuring leadership behaviour sets the standards and the messaging is not blocked as it cascades down through the business structures.
    c. Analyse past incidents to look for patterns of justification or minimisation.

7. Proportionate Risk Based Prevention Procedures

The Internal Control Reference Framework is structured by domain, identifying the main risks associated with the processes within each domain, and determines the essential controls which can eliminate or minimise those risks.

For each process, a control/risk matrix is used to reference the types of risks by control and thus contributes to the understanding of the control system. Controls protecting against fraud risk are shown in Appendix 2)

The reference framework is updated annually by the Audit, Risks and Internal Control Department assisted by the Corporate Functional Departments. The results of audits, compliance statements, incidents and risk maps provide valuable input for the periodic update of the controls included in the ICRF.

Concentrations of duties in main functions are to be avoided with sufficient compensatory controls in place when tasks are concentrated. (Refer to summary table in Appendix 3)

8. Due Diligence:

Businesses must vet associated persons and third parties and conduct ongoing monitoring for high-risk situations.

Acquisition projects are evaluated in line with Group procedures. The Strategic Development Director and General Counsel will analyse the target to detect any questionable practices, or to identify politically exposed people (maintaining close relationship with public authorities) or with a noncompliant profile (fraud, court cases, terrorism, etc.).

9. Communication and Training:

To ensure our employees adhere to our ethical code, the Principles of Conduct and Action, we have an E-Learning training program comprising:

- **ADHERE**: training program dedicated to the Principles of Conduct and Action, the Group's code of ethical conduct
- **COMPLY**: training program dedicated to antitrust law
- **ACT:** training program dedicated to the prevention of corruption- Promote awareness of whistleblowing channels.

10. Monitoring and Review:

Internal audit is a centralised function at the level of Compagnie de Saint-Gobain. The Internal Audit Department of Saint-Gobain Group complies with the international professional standards, as described in the Internal Audit Professional Framework (RPAI) - 2020 version, and with the International Professional Practices Framework (IPPF) of the global “Institute of Internal Auditors” (IIA), published in 2024 and applicable in 2025.

Employees, whatever their level in the management line, are obliged to show due diligence and transparency in the answers they provide in response to the requests of the internal auditors and in making available documents, data and information of whatever kind may be necessary for the accomplishment of their mission. Any hindrance to the accomplishment of an audit mission or dissimulation of information from the internal auditors constitutes a breach of the Principles of Conduct and Action and may result in disciplinary action.

At the end of the audit, the internal auditors, with the assistance of the audited business, draw up priority action plans to strengthen the mitigation of the risks identified, and produce a report presenting their main observations and recommendations.

This report is sent to the audited entity for review: the contradictory process is a key element in the quality of audit reports and the transparency of discussions between auditors and auditees.

The final report is communicated to the Senior management of the Group and to the entity's operational management (Region, Country, Business Unit).

An action plan management and monitoring database is used to centralise the measures implemented to remedy non-conformities identified in the compliance statement, as well as the action plans drawn up following audits conducted by the Group's internal audit department.

11. Reporting and Investigation

- Reports can be made via the whistleblowing channels.
- The Chief Compliance and Business Ethics Officer will lead investigations and is supported by the General Counsel.
- Findings are reported to senior leadership and corrective actions implemented.

12. Sanctions

- Disciplinary action for confirmed fraud.
- Legal proceedings where appropriate.
- Recovery of misappropriated assets.

13. Record Keeping

- Investigation records retained for a minimum of 5 years.
- Annual fraud report submitted to senior management.

14. Policy Review

- This policy will be reviewed annually or upon significant changes in legislation or business operations.

15. Useful Links to Related Documents

Whistleblowing Policy – Speak Up @ Saint-Gobain

Principles of Conduct and Action

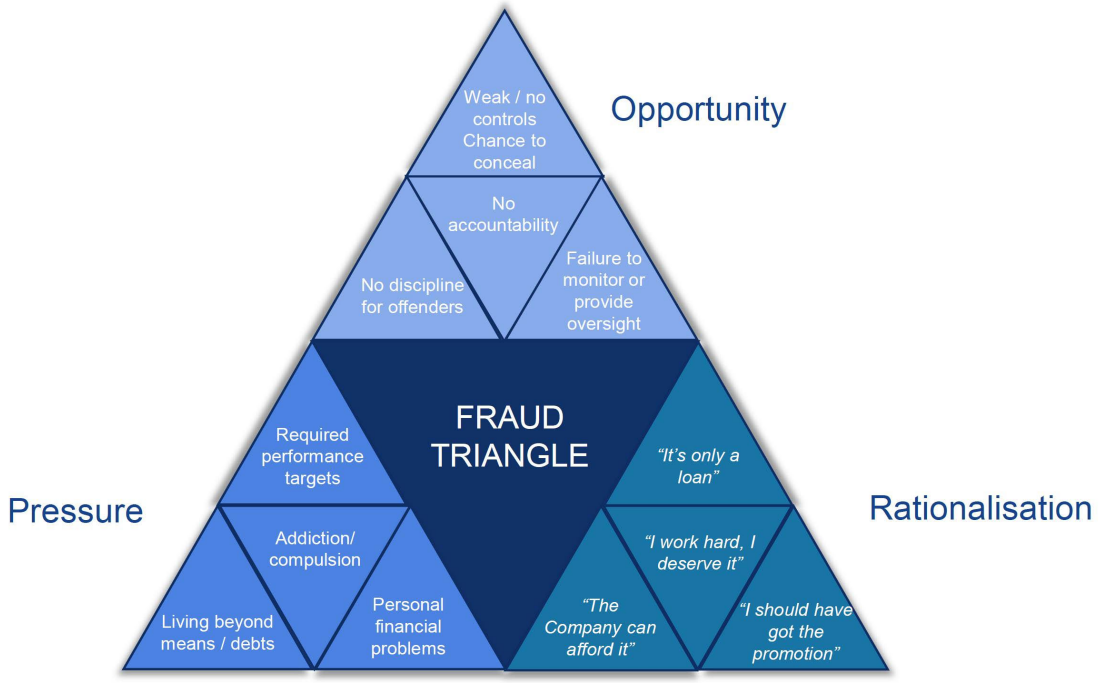
Anti-Corruption Policy

Suppliers Charter

Purchasers Charter

APPENDIX 1: FRAUD TRIANGLE

Dr. Donald Cressey was one of the first individuals to study how white-collar criminals differ from violent offenders. Part of Dr. Cressey's work on occupational fraud included the development of the Fraud Triangle. According to this theory, three elements must be present for occupational fraud to occur:



Cressey's Fraud Triangle asserts there are three interrelated elements enabling someone to commit fraud: the motive or pressure driving a person to want to commit the fraud, the opportunity enabling them to commit the fraud, and the ability to rationalise the fraudulent behaviour.

The vulnerability an organisation encounters from individuals capable of combining all three of these elements is fraud risk. Fraud risk can come from sources which are both internal and external to the organisation, and it is one of the risks managed by an organisation.

APPENDIX 2 – CONTROLS TO MITIGATE FRAUD RISK EITHER BY MISAPPROPRIATION OR MISREPRESENTATION

C1.1.01 - Management of the major risks to which the entity is exposed
C1.2.01 - Organization of internal control
C1.2.02 - Monitoring of the internal control system
C1.2.03 - Delegation of powers and powers of signatures; authorization matrices
C1.2.04 - Segregation of duties and access rights
C1.3.05 - Security and Anti-Fraud Guidelines
C2.4.01 - Security policy of R&D centres
C3.2.01 - Product Management
C3.2.03 - Other operational marketing activities (communication, digital marketing & cost control)
C3.2.04 - Assessing the performance of the marketing activities
C4.1.01 - Segregation of duties and Access Rights
C4.2.01 - Sales policy
C4.2.02 - Prices
C4.2.03 - Discounts, preferential rates and special terms of sale
C4.2.04 - Customer rebates
C4.2.05 - Sales to employees
C4.3.01 - Evaluation and acceptance of the customer
C4.3.02 - Formalization of customer contracts
C4.3.03 - Creation/modification/deletion of customer data
C4.3.04 - Setting the credit limits
C4.4.01 - Management of relations with commercial agents, and other sales-related intermediaries
C4.5.01 - Offers and quotes
C4.5.02 - Customer orders
C4.5.03 - Confirming a client's credit balance upon placing an order
C4.5.04 - Cash sales (over the counter)
C4.6.01 - Billing obligation
C4.6.02 - Billing peculiarities
C5.1.01 - Stock management policy
C5.1.02 - Principles of organization of the inventory (physical and in the ERP)
C5.1.03 - Principles of organization for consignment stocks or stocks held by subcontractors
C5.1.04 - Segregation of duties and access rights
C5.2.01 - Control over stock receipts
C5.2.02 - Control over dispatches / goods pick-up
C5.2.03 - Control over inter-site transfers
C5.2.04 - Recording of goods movements in accounting
C5.2.05 - Review of stock adjustments
C5.3.02 - Review of stock anomalies
C5.3.03 - Assessing the performance in inventory management
C5.4.01 - Principles of organization for the stock count
C5.5.01 - Approving the method for identifying obsolete stock
C5.5.02 - Approving the scraping and destruction of stock
C6.1.01 - Ensuring purchasers' independence (excluding Trade Purchasing)
C6.1.02 - Segregation of duties and access rights

C6.2.01 - Purchasing management policy
C6.2.03 - Assessing the performance of the purchasing activities
C6.3.02 - Competitive offers and calls for tenders
C6.4.01 - Evaluation and acceptance of a supplier
C6.4.02 - Formalization of the supplier contracts
C6.4.03 - Creation/modification/deletion of tariffs and supplier data
C6.5.01 - Formalizing commitments towards suppliers
C6.5.02 - Processing of exceptions on purchase orders
C6.6.01 - Matching the physical goods' receipt, delivery note and purchase order
C6.7.01 - Matching the invoice, the purchase order and the goods receipt note
C6.7.02 - Registration and validation of supplier invoices
C6.8.01 - Supplier rebates
C7.3.02 - Production sequencing
C7.3.03 - Production performance monitoring
C7.4.01 - Quality Management System
C7.6.02 - Purchase of production equipment
C8.1.01 - Appointments of a Risk Prevention Coordinator and Insurance Correspondent
C8.2.01 - Knowledge of the Prevention of Industrial and Distribution Risks Manual
C8.2.02 - Training on the prevention of industrial and distribution risks
C8.2.03 - Self-assessment using the « Risk Grading » tool
C8.3.01 - Legal and regulatory obligations relating to insurance
C8.3.02 - Group insurance obligations
C8.3.03 - Taking out the Group's international insurance policies
C8.3.04 - Review of the insurance policies
C8.3.06 - Notification of damages
C8.4.01 - Property Management
C9.1.02 - Knowledge of EHS requirements
C9.3.02 - Safety at work management
C10.1.01 - Operating rules between the SSC and its client entities
C10.1.03 - Segregation of duties and access Rights
C10.6.01 - Travel and mission Expense Reports’ Management
C10.6.02 - Procedure for using company credit cards and similar
C10.6.03 - Advances and loans granted to employees
C10.7.01 - Creation/modification/deletion of payroll data
C10.7.02 - Validation of the payroll data
C10.7.03 - Validation of the payroll transfer
C10.7.04 - Relations between the payroll SSC and accountants
C11.1.01 - Communication plans and actions
C11.4.02 - Partnerships, sponsoring and corporate patronage
C12.1.01 - IT Strategy and governance
C12.1.02 - Operating Rules between the SSC and its client entities
C12.2.01 - Documentation of the IT/IS environment
C12.3.01 - Infrastructure and security of IT/IS premises
C12.3.02 - Securing Saint-Gobain’s computer network
C12.3.03 - Control of users and administrators’ accounts, robots (RPA) and access rights
C12.4.02 - Management of incidents
C12.5.01 - Change management and production deployment

C12.6.01 - IT and digital Purchases and contracts
C15.2.01 - Local treasury management policy
C15.2.02 - Segregation of duties and access Rights
C15.3.01 - Funding of needs
C15.5.02 - Processing cash receipts / collection
C15.6.01 - Cash management
C16.1.01 - Operating rules between the SSC and its client entities
C16.1.02 - Segregation of duties and access rights in the entities / SSC
C16.2.01 - Application of the accounting standards and Anticorruption Accounting Controls
C16.3.01 - Processing journal entries
C16.4.01 - Accounting closing process
C16.4.02 - Periodic meeting between the SSC and the client entity
C16.4.03 - Review of the balance sheet accounts
C16.4.04 - Justification and review of provisions
C16.4.05 - Other accounting verification operations
C16.4.06 - Review of financial statements and controlling data
C16.4.07 - Review of adjustments in local accounts / IFRS
C16.4.08 - Balance Sheet Review
C16.5.01 - Supplier data management and Accounts Payable
C16.6.01 - Recording of sales & losses on trade receivables
C16.6.02 - Customer data management and Accounts Receivable
C16.7.01 - Bank Reconciliation
C16.8.01 - Specific operations related to tax and duties accounts
C16.9.01 - Validation of the consolidation scope
C16.9.02 - Preparation of the reporting
C16.9.03 - Communication of weaknesses identified by the Statutory Auditors
C16.10.01 - Investment process
C16.10.02 - Monitoring the life of the assets
C16.10.03 - Special Case of impairment losses
C16.10.04 - Special case of lease agreements
C16.11.01 - Group Authorization Requests
C16.11.02 - Completion of the operation in accordance with the authorized “DAC”
C16.12.01 - Update of the pension obligations
C16.13.04 - Validation of inventory valuation and actual production Costs
C16.13.05 - Margin Analysis
C16.13.06 - Monitoring Working Capital Requirement (WCR)
C16.13.07 - Monitoring of cash flow indicators
C17.1.03 - First contacts with the target and launch of the discussions
C17.1.05 - Due diligence
C17.1.06 - Group Authorization Request (« DAC »)
C17.1.07 - Negotiation and drafting of the acquisition contract

Highlighted items are designated as “Essential” controls

APPENDIX 3: CONCENTRATIONS OF DUTIES BY PROCESS TO BE AVOIDED OR MITIGATED BY COMPENSATING CONTROLS

Chapter 4 Sales & Customer Services Process	Sales activities and customer master data management
	Account receivables and customer receipts management
	Invoicing and customer master data management
	Account receivables and credit notes /credit memos management
	Price management and sales orders management
	Handling dispatches shall be segregated from other functions (sales orders, invoicing, customer master data)
Chapter 5 Stocks & Logistics	Stock control vs. Physical handling of stocks vs. booking of stock movements in the system
	Validation of non-standard movements and stock adjustments vs. Physical handling of stocks/booking the transactions in the system on a daily basis
	Approval of stock take results vs. Counting / Stock responsibility
	Inventory management vs. write-access to accounting
Chapter 6 Purchasing	Purchase orders approval and good receipts recording
	Booking of purchase orders and “OK to pay”
	Management of supplier master files and tasks of purchasing, goods receipt and payments. In particular, employees who are in contact with suppliers must not be able to edit supplier details in the purchasing management system
	Account payables and tasks of purchasing, good receipt and payments
Chapter 7 Production	Creation / edition of BOMs and declarations of consumptions / production declarations
	Production and Inventory Management
	Access to the production system and Access to the accounting system
Chapter 10 Human Resources & Payroll	Prior approval of payroll items (fixed and variable) and booking of these payroll items into the system
	Processing and payment of salaries
	Personnel master file management and write-access to the payroll system or to the payment file
Chapter 15 Treasury & Financing	Account receivables and customer receipts management
	Accounts payable and disbursements
	“OK to pay”, issuance and booking of payments, and signing the payment
	Bank reconciliations and the authority as a bank signatory, receipts and general accounting (ability to book entries onto the treasury accounts)
	Persons working in the “cash management” department vs. signature of the payment orders and payments
	Users with write access rights to customer and supplier master files vs. signature of the payment orders and payments
	The people in charge of accounts payable in the SSC, even if they do not have write access rights to the ERP vs. signature of the payment orders and payments
Chapter 16 Accounting - Financial Controlling	Accounts payable and write-access to master files and cash management
	Accounts receivable and write-access to master files, cash management and issuance of credit notes
	General accounting and write-access to the sub-ledger accounting modules and cash management
	Payment management and write-access to accounting
	Supervision of accounting work (SSC Director and process managers* / Accounting Director) and write-access to the accounting and cash management modules (*G/L, A/P, A/R, Cash Management)