

# School of Coding & AI

## ANTI-BRIBERY AND COUNTER FRAUD POLICY

### 1. Introduction

#### 1.1 Purpose

The School of Coding & AI (“SOC”) is committed to ensuring that all its business is conducted in an honest and ethical manner. SOC takes a zero-tolerance approach to Bribery, Corruption and Fraud and is committed to acting professionally, fairly and with integrity in all its business dealings and relationships wherever it operates and to implementing and enforcing effective systems to counter Bribery and Fraud.

SOC will take appropriate action to prevent Bribery, Corruption and Fraud within SOC. It will uphold all laws relevant to countering Bribery and Fraud in all the jurisdictions in which it operates. However, SOC remains bound by the laws of the UK, including the Bribery Act 2010 (“Bribery Act”), the Fraud Act 2006 (“Fraud Act”) and the Economic Crime and Corporate Transparency Act 2023 (“ECCTA”), in respect of its conduct both at home and abroad.

Bribery and Fraud may be punishable for individuals by up to ten years’ imprisonment, and if SOC is found to have taken part in Corruption it could face an unlimited fine, be excluded from tendering for public contracts or funding and face damage to its reputation. SOC therefore takes its legal responsibilities very seriously.

The purpose of this Anti Bribery and Counter Fraud Policy (“Policy”) is to:

- (a) ensure compliance with applicable laws, including the Bribery Act, Fraud Act, and ECCTA .
- (b) uphold SOC’s zero tolerance approach towards Fraud and Bribery by promoting the detection and prompt investigation of fraud and bribery.
- (c) implement and maintain reasonable procedures to prevent Fraud, Bribery and other Financial Irregularity, proportionate to the size, resources, and complexity of the organisation.
- (d) protect SOC’s finances, assets, and reputation.
- (e) provide information and guidance on how to recognise and report Fraud and Bribery issues.

This Policy is owned and overseen directly by SOC’s Board of Directors and embedded throughout the organisation. All investigations will be conducted in accordance with applicable data protection legislation including the UK GDPR and Data Protection Act 2018.

#### 1.2 Scope

This Policy applies to all individuals working at all levels and grades, including senior managers, officers, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff,

volunteers, interns, agents, sponsors, or any other Associated Person (collectively referred to as “workers” in this Policy). It covers all activities, including those delivered overseas. Fraud or bribery committed by non-UK associated persons may still fall within scope where there is a UK connection. All international partners, agents, and contractors are required to meet equivalent counter fraud and antibribery standards and comply fully with SOC’s requirements.

Enhanced scrutiny is applied to activities assessed as having a higher inherent risk of Bribery or Corruption. These include:

- procurement and tendering processes;
- contract negotiations, consultancy, and commission arrangements;
- joint ventures, subsidiaries, and collaborative partnerships; and
- any engagement with agents, intermediaries, or consultants.

Additional high-risk areas include:

- interactions with public officials, regulators, or accrediting bodies;
- donations, sponsorships, and research funding; recruitment, promotion, admissions, scholarships, bursaries, and assessment decisions;
- overseas travel to higher risk jurisdictions;
- the giving or receiving of gifts and hospitality;
- the provision of references, peer reviews, or endorsements;
- and the handling of confidential or commercially sensitive information.

Any concerns or disclosure relating to personal relationships, are addressed by the Staff and Student Relationships Policy.

It is a condition of employment that employees shall abide by the rules and policies made by SOC from time to time, which includes this Policy. Any alleged failure to follow this Policy will be investigated (and, where appropriate, action taken) in accordance with SOC’s disciplinary procedures. SOC reserves the right to terminate its contractual relationship with other workers and organisations if they breach this Policy.

### 1.3 Definitions

The following definitions shall apply in this Policy:

- **AsSOCiated person** — any individual or organisation acting for on behalf of, or in connection with SOC’s activities, including subsidiaries, contractors, agents, intermediaries, partners, joint ventures, advisors, and any other party performing services or handling public funds in relation to SOC.
- **Bribery** — offering, promising, giving, or accepting any financial or other advantage to induce, reward, or permit the improper performance of a function or activity, including Facilitation Payments.
- **Corruption** — offering, giving, receiving, or soliciting an advantage to secure an illegal, unethical, or untrustworthy outcome; now largely encompassed within bribery offences.
- **Facilitation Payments** - unofficial payments made to secure or expedite a routine or necessary action (for example, by a government official);

**Financial Irregularity** — any breach of rules (including internal rules and policies), standards, or legal requirements governing the use of public funds, whether deliberate (such as Fraud or Bribery) or accidental (such as error or mismanagement).

- **Fraud** — any dishonest act intended to secure unlawful gain or cause loss, including false representation, failure to disclose information, abuse of position, dishonest use of services, false accounting, false statements, conspiracy to defraud, and the falsification, manipulation, concealment, or destruction of records or data to mislead, obtain advantage, or disguise wrongdoing.
- **Third Party:** any individual or organisation with whom a worker comes into contact during their course of work for SOC, and includes actual and potential clients, customers, suppliers, distributors, business contacts, agents, advisors and government and public bodies, including their advisors, representatives and officials, politicians and political parties.

## 2. Anti-Bribery and Counter Fraud Policy Principles

- **No worker shall seek a financial or other advantage** for SOC through Bribery, or shall offer, promise, give, request, agree to receive or accept a bribe for any purpose. SOC prohibits any form of Fraud within its operations, and no worker may engage in any form of Fraud with regard to activity carried out within or on behalf of SOC.
- **Proportionate procedures** — SOC takes appropriate action to prevent all forms of Bribery and Fraud within SOC and maintains risk based and proportionate controls across all relevant activities and procurement processes, ensuring that preventative measures reflect the level of Bribery and Fraud risk.
- **Leadership and organisational commitment** — SOC operates a zero-tolerance approach to Bribery and Fraud, with visible and active leadership from senior executives, including the Principal and the Chief Operating Officer (COO), who are responsible for setting expectations and ensuring an effective organisational response.
- **Risk assessment** — Bribery and Fraud risks are assessed on a regular basis by the senior management team and formally on an annual basis by the Board of Directors, including exposure within procurement, commissions, gifts and hospitality, and other high-risk operational areas, with findings used to strengthen controls. Any worker who suspects that Bribery or Fraud has occurred is required to immediately report such instances in accordance with this Policy.
- **Due diligence** — proportionate due diligence is undertaken on all partners, agents, contractors, and AsSOCiated Persons, including fit and proper persons checks, financial and reputational screening, and sanctions checks where appropriate.
- **Communication and training** — all workers receive mandatory annual training on counter fraud and anti-bribery and counter fraud requirements, with enhanced training provided to those in procurement, contract management, international engagement, or other higher risk roles.
- **Monitoring and assurance** — the Board of Directors, as set out in section 3.

## 3. Responsibilities

Role holder(s)	Responsibility
All SOC workers	<ul style="list-style-type: none"> <li>● <b>Act honestly and with integrity</b>, and declare any conflict of interest (in accordance with the conflict of interest guidance at Annex B),</li> </ul>

	<p>gifts or hospitality that could influence, or appear to influence, operations or decision-making.</p> <ul style="list-style-type: none"> <li>● <b>Read, understand and comply</b> with this policy (including, but not limited to, the conflict-of-interest guidance at Annex B) and any associated procedures and guidance and follow SOC's Financial Regulations and procurement procedures.</li> <li>● Ensure one's <b>personal conduct</b> does not give rise to suspicion of a conflict between their official duties and private interests.</li> <li>● <b>Be vigilant</b> to signs of fraud and bribery and promptly report concerns or gaps in controls, assisting with investigations as required. If in any doubt, a member of staff or associated person should contact the Chief Operating Officer of the Clerk to the Board for professional advice.</li> <li>● Complete relevant mandatory <b>training</b>.</li> <li>● Conduct appropriate <b>due diligence</b> to assess whether there is a risk that Bribery or Fraud might occur in relation to a particular transaction, Third Party or territory;</li> </ul>
<p>Senior Management Team</p>	<ul style="list-style-type: none"> <li>● <b>Report and escalate concerns appropriately</b> by recording relevant details accurately, preserving evidence without interference, and sharing information only through authorised channels. Managers must ensure that concerns are raised responsibly and not pursued through personal investigation, direct confrontation, or informal discussion that could compromise an inquiry.</li> <li>● <b>Exercise heightened vigilance in decision making</b> by declaring any actual or perceived conflicts of interest, conducting proportionate due diligence on suppliers, partners, and contractors, and ensuring that procurement and contracting processes are free from improper influence.</li> <li>● <b>Provide effective oversight and promote awareness</b> by ensuring that staff understand their obligations under this policy, complete mandatory training, and receive appropriate supervision to identify and mitigate risks of fraud, bribery, or irregularity.</li> <li>● <b>Embed preventative controls in operational practice</b> by integrating fraud resistant processes into team activities, maintaining clear audit trails, and ensuring that decisions relating to procurement, contracting, recruitment, or financial commitments are transparent, evidence based, and compliant with institutional requirements.</li> </ul>
<p>Chief Operating Officer</p>	<ul style="list-style-type: none"> <li>● Overseeing the development, implementation and maintenance of robust <b>financial risk management</b>, fair and transparent tender procedures, and internal controls that assist in the prevention and detection of fraud and bribery.</li> <li>● <b>Implementing, maintaining, and reviewing this Policy</b> to secure compliance with the law.</li> </ul>

	<ul style="list-style-type: none"> <li>• Overseeing <b>investigations and maintaining records</b>, making referrals to external bodies unless the case involves staff within the COO's team, then the investigation and maintenance records will be the responsibility of the Clerk to the Board.</li> <li>• Overseeing <b>training</b> for all workers.</li> </ul>
Principal	<ul style="list-style-type: none"> <li>• <b>Report</b> immediately to the Board of Directors</li> <li>• <b>Notify the Office for Students (OfS) of material adverse events</b> (including suspected or actual Fraud or Financial Irregularity).</li> </ul>
Clerk to the Board	<ul style="list-style-type: none"> <li>• Overseeing <b>investigations and maintaining records</b> for cases where the COO has a conflict of interest.</li> <li>• Ensure the <b>Conflict-of-Interest Guidance</b> at Annex B of this policy aligns with section B3 of the Code of Governance.</li> <li>• <b>Secure independent professional advice</b> related to cases covered under this policy for the Board of Directors if required.</li> <li>• Maintain the register of declared conflicts of interest.</li> </ul>
Board of Directors	<ul style="list-style-type: none"> <li>• Ultimate responsibility for ensuring SOC maintains robust Fraud and Bribery prevention policies and oversight mechanisms.</li> <li>• Review investigation report where wrongdoing has been identified as Medium-Risk Case or High-Risk Case.</li> <li>• Review on an annual basis risk associated with anti-bribery and fraud in light of relevant higher education sector cases and OfS regulatory guidance and the changing risk profile of SOC.</li> </ul>

#### 4. What is Bribery?

Examples of Bribery include:

- a) offering a bribe: offering events tickets or gifts to a potential partner conditional on awarding SOC business;
- b) receiving a bribe: a supplier offers an internship for a member of SOC staff's relative in return for favourable treatment by SOC; or
- c) bribing a foreign official: offering an unofficial payment to expedite approvals (Facilitation Payment).

An offence of Bribery is committed as soon as the offer of a bribe is made regardless of whether the bribe is accepted.

SOC will not make, and will not accept, Facilitation Payments of any kind. If a worker is asked to make a payment on SOC's behalf, such worker should always be mindful of what the payment is for and whether the amount requested is proportionate to the goods or services provided. A worker should always ask for a receipt which details the reason for the payment, and in the event of any suspicions, concerns or queries regarding a payment, concerns should be raised in accordance with this Policy. All workers must avoid any activity that might lead to, or suggest, that a Facilitation Payment will be made or accepted by SOC.

#### 5. Gifts and hospitality

This Policy does not prohibit normal and appropriate hospitality (given and/or received) to or from third parties. However, excessive or lavish gifts or hospitality in relation to business transactions or arrangements might constitute Bribery.

The giving of hospitality is not prohibited, if the following requirements are met:

- a) it does not exceed normal business courtesies;
- b) it is not made with the intention of influencing a Third Party to obtain or retain business or a business advantage, or to reward the provision or retention of business or a business advantage, or in explicit or implicit exchange for favours or benefits;
- c) it complies with local laws;
- d) it is given in the name of SOC, not in a specific worker's name;
- e) it does not include cash or a cash equivalent (such as gift certificates or vouchers);
- f) it is appropriate in the circumstances (for example, it is customary for small gifts to be given at Christmas time);
- g) taking into account the reason for the gift, it is of an appropriate type and value and given at an appropriate time; and
- h) it is given openly, not secretly.

However, gifts should not be offered to, or accepted from, government officials or representatives, or politicians or political parties. SOC appreciates that the practice of giving business gifts varies between countries and regions and what may be normal and acceptable in one region may not be acceptable in another. The test to be applied is whether in all the circumstances the gift or hospitality is reasonable and justified. The intention behind the gift should always be considered.

In any event, a gift or gifts with a total value of £100 or above should be declared and recorded as noted in Annex B.

## **6. What is not acceptable**

It is not acceptable for any worker to:

- a) offer (including a promise to offer) or receive gifts or hospitality with the expectation of a business advantage or to reward a business advantage already given;
- b) offer (including a promise to offer) or receive Facilitation Payments;
- c) accept payments, gift, or hospitality from a Third Party in exchange for preferential treatment or business advantage;
- d) retaliate against anyone, including another worker, who has refused to commit a Bribery offence or who has raised concerns under this Policy; or
- e) engage in any activity that risks breaching this Policy.

## **7. Donations**

SOC does not make contributions to political parties. SOC only makes charitable donations that are legal and ethical under local laws and practices. No donation must be offered or made without the prior approval of the Clerk to the Board.

## **8. What is Fraud?**

Fraud is a criminal act involving deception or dishonesty to secure an improper gain for oneself or another or to cause someone else to incur a loss. This can include theft, the misuse of funds or other resources, or more complicated crimes such as false accounting and the supply of false information. It is also an offence to fail to prevent Fraud by an AsSOCIated Person, which means SOC will be liable if an AsSOCIated Person commits a

Fraud and such Fraud is intended to benefit SOC (directly or indirectly) or a person to whom services are provided on behalf of SOC.

Examples of Fraud include admissions or recruitment Fraud, misappropriation of property, unauthorised use of funds or other resources, manipulation of financial or academic records, payroll Fraud, procurement or payment Fraud, or cyber-enabled schemes such as payment diversion Fraud.

## **9. Raising a concern**

All workers are encouraged to raise concerns about any issue or suspicion of malpractice at the earliest possible stage. If any worker is unsure whether a particular act constitutes Bribery, Fraud, Corruption or other Financial Irregularity, these should be raised by following the procedure for handling and investigating suspected Fraud, Bribery, Corruption or Financial Irregularity set out under Annex A of this Policy.

All concerns must be reported promptly to the Clerk to the Board in accordance with the procedure set out under Annex A.

However, if the individual believes the matter cannot be reported through normal management channels or fears detriment as a result of raising it, the concern must be raised as set out in SOC's Whistleblowing Policy, which provides a protected disclosure route and additional safeguards for those reporting in the public interest.

## **10. Record-keeping**

SOC must keep financial records and have appropriate internal controls in place which will evidence the business reason for making payments to Third Parties.

All workers must declare and keep a written record of all hospitality or gifts accepted or offered with a cumulative value of £100. Such a declaration must be in writing to the [COO], who will maintain a log. These logs will be available for inspection by the Clerk to the Board and the Board of Directors.

All accounts, invoices, and other records relating to dealings with Third Parties including suppliers and customers should be prepared with strict accuracy and completeness. No accounts must be kept "off book" to facilitate or conceal improper payments.

## **11. Monitoring and Review**

This Policy is reviewed annually by the Board of Directors.

## **12. Related Policies**

This Policy should be read in conjunction with other relevant SOC policies and procedures including:

- a) Whistleblowing Policy
- b) Staff Disciplinary Procedure
- c) Staff and Student Relationship Policy
- d) Risk Management Policy

## Annex A

### Procedure for Handling and Investigating Suspected Fraud, Bribery, Corruption or Financial Irregularity

#### 4.1 Raising a Concern

Concerns about suspected Fraud, Bribery, Corruption or other Financial Irregularity must be reported promptly to the Clerk to the Board. Reports should include factual observations, dates, times, individuals involved, and any supporting information. Evidence must not be altered or examined by the reporter and should be secured until collected by the Investigating Officer.

#### 4.2 Initial Triage and Risk Assessment

The Clerk will conduct an initial assessment of the seriousness, potential impact, and urgency of the allegation. This includes assessing risks to individuals, SOC operations, public funds, and regulatory compliance, and determining whether the matter may constitute an adverse material event requiring external reporting.

#### 4.3 Appointment of the Investigating Officer

The COO will act as the Investigating Officer for all cases. Where the COO has a conflict of interest, is implicated, or is otherwise unable to act, the Clerk to the Board will assume the role. The Investigating Officer must be independent of the matter under review and have the authority to access relevant records, systems, and personnel.

#### 4.4 Preservation and Collection of Evidence

The Investigating Officer will secure all relevant evidence, including documents, digital records, financial data, communications, and physical materials. Evidence must be logged,

stored securely, and handled in accordance with legal and regulatory requirements. Staff must cooperate fully and must not attempt to investigate independently.

#### **4.5 Conducting the Investigation**

The Investigating Officer will undertake a structured fact-finding process, reviewing records, interviewing relevant individuals, and analysing financial or operational data. Interviews must be documented, and individuals must be informed of their rights and responsibilities. The investigation must remain impartial, confidential, and proportionate to the allegation. External professional advice and expertise may be procured to support the investigation e.g. legal and digital forensics.

#### **4.6 Interim Measures and Escalation**

If emerging evidence indicates significant risk—such as financial loss, safeguarding concerns, criminal conduct, or potential regulatory breach—the Investigating Officer may implement interim controls or escalate the matter to external bodies, including law enforcement, funding bodies, auditors, or the OfS where required.

#### **4.7 Investigation Report**

At the conclusion of the inquiry, the Investigating Officer will prepare a written report setting out the concern, the evidence reviewed, the findings reached, and any recommended actions. This report will be submitted to the Clerk to the Board for consideration. The Board of Directors will receive either the full report or an appropriate summary, including in cases where no wrongdoing is established, to provide assurance that the procedure has been followed correctly and that this Policy is being applied consistently.

#### **4.8 Decision Making- and Outcomes**

The Board of Directors will review the investigation report and determines the appropriate outcome. Decisions must be evidence based, consistent with SOC policies, and proportionate to the findings. Where misconduct is substantiated, disciplinary or contractual processes will be initiated-. Where concerns are unfounded, steps are taken to restore trust and ensure no detriment to individuals who acted in good faith.

#### **4.9 Regulatory and External Reporting**

Where required, SOC will report adverse material events, Fraud, or misuse of public funds to the OfS, funding bodies, or other regulators. Criminal matters may be referred to law enforcement.

#### **4.10 Learning, Remediation, and Control Improvements**

Following each investigation, SOC will review the underlying causes and implement any necessary improvements to systems, processes, training, or oversight. Lessons learned will be shared with relevant teams, and the Board of Directors may commission internal or external reviews of the effectiveness of new controls.

## Annex B

### Guidance on the management of conflicts of interest

#### 1. Purpose of this guidance

Conflicts of interest can create real or perceived risks to the integrity of SOC's decision-making, particularly in areas vulnerable to Fraud, Bribery, or improper influence. This guidance sets out how workers must identify-, declare, and manage conflicts to ensure transparency, accountability, and compliance with regulatory requirements.

#### 2. What constitutes a conflict of interest

A conflict of interest arises when an individual's personal, financial, or professional interests could improperly influence—or be perceived to influence—their judgement, decisions, or actions on behalf of SOC. Conflicts may be:

- **actual** — a direct conflict exists now.
- **potential** — a conflict may arise in the future.
- **perceived** — a reasonable person might believe a conflict exists, even if the individual does not.

Examples include personal relationships with suppliers or applicants, financial interests in partner organisations, external roles that overlap with SOC duties, or situations where impartiality could reasonably be questioned.

### 3. Responsibilities of workers

All workers must:

- **identify and declare conflicts promptly**, including perceived or potential conflicts, using the process set out in the Conflicts of Interest guidance.
- **refrain from participating in decisions** where a conflict exists until the conflict has been formally reviewed and managed.
- **cooperate fully** with any review, mitigation, or oversight measures put in place.
- **maintain transparency** in procurement, contracting, recruitment, assessment, and other high-risk- activities.

Senior Management team have additional responsibilities to:

- **review and assess declared conflicts**, determining whether they can be managed or whether recusal is required.
- **ensure appropriate controls** are in place, such as alternative decision -makers, enhanced oversight, or segregation of duties.
- **promote awareness** of conflict-of-interest- obligations within their teams and ensure staff complete required training.
- **document decisions and mitigation measures** to provide a clear audit trail.

### 4. Declaring and recording conflicts

Conflicts must be declared:

- **as soon as they are identified**, including during procurement, contract award, recruitment, assessment, or partnership discussions.
- **through the formal declaration process**, ensuring full and accurate disclosure.
- **whenever circumstances change**, requiring an updated declaration.

Declarations are recorded in the central register (managed by the Clerk to the Board) and reviewed periodically to ensure they remain accurate and appropriately managed.

### 5. Managing conflicts of interest

Once declared, conflicts must be managed in a way that protects the integrity of SOC's processes. Mitigation may include:

- **recusal** from decision making- or access to sensitive information.
- **independent oversight** or review by an uninvolved manager.
- **reallocation of responsibilities** to remove the conflict.
- **enhanced scrutiny** of procurement, contracting, or financial decisions.
- **external validation or audit** where risks are significant.

Where a conflict cannot be adequately managed, the individual must not participate in the relevant activity.

## 6. Conflicts and high-risk- areas

Conflicts of interest require heightened vigilance in areas with elevated Bribery or Fraud risk, including:

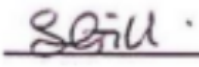
- procurement and tendering.
- contract negotiation and consultancy arrangements.
- partnerships, agents, and intermediaries.
- recruitment, promotion, and assessment.
- gifts, hospitality, sponsorship, and donations (over £100).
- handling of confidential or commercially sensitive information.

In these areas, even perceived conflicts can undermine trust and must be managed proactively.

## 7. Non-compliance

Failure to declare or appropriately manage a conflict of interest may constitute misconduct and could lead to disciplinary action. Serious breaches may also trigger external reporting obligations, including to the OfS, funding bodies, or law enforcement where relevant.

Name of provider: School of Coding & AI Ltd  
Name of nominated accountable officer: Suki Gill  
Designation: Principal

Signature:   
Date: 18th June 2026