BYTES TECHNOLOGY GROUP PLC

(Incorporated in England and Wales)
Registered number: 12935776

ANTI BRIBERY, FRAUD AND MONEY LAUNDERING POLICY

---

1. Introduction – Scope and Purpose

The Bytes Technology Group plc and its subsidiaries (the "**Group**") is committed to the highest ethical standards and has a zero-tolerance approach in respect of fraud, bribery and money laundering. All instances of fraud, bribery and money laundering will be investigated rigorously and promptly and appropriate action will be taken.

It is important that the Group uses its income and resources in the most effective way to deliver high quality services. We require all staff and persons employed in a similar capacity at all times to act honestly and with integrity and to safeguard the resources for which they are responsible.

The purpose of the Bytes Technology Group Anti Bribery, Fraud and Money Laundering Policy (the "**Policy**") is to set out individual responsibilities with regard to the prevention of, detection of and response to fraud, bribery and money laundering, including what to do in the event of a suspected fraud or instance of bribery and what action will be taken by us in the event that an offence has been committed.

The Group expects our employees, board/committee members, agency staff, consultants and contractors to conduct themselves in accordance with this Policy. The Group will investigate all breaches or suspected breaches of this Policy and, if necessary, invoke disciplinary measures against any employee found to be involved in bribery and take prompt action to remedy the breach and prevent any repetition in line with disciplinary procedures. Such measures may include dismissal, reporting of the matter to the relevant authorities or, in the case of suppliers and other business partners, termination of the business relationship.

The Policy is based on five key principles of a fraud, bribery and money laundering risk management process:

- **Principle 1**: A policy based on risk has been written to convey to employees the expectations of the Group Board regarding managing and responding to fraud, bribery and money laundering risks.

- **Principle 2:** Related risk exposure is assessed by the Group to identify specific potential events and risks that it needs to mitigate.

- **Principle 3:** Prevention techniques and controls to avoid potential key fraud, bribery and money laundering risk events are established, where feasible, to mitigate potential impacts to the Group.

- **Principle 4:** Detection methods and controls to uncover fraud, bribery and money laundering events when preventative measures fail.

- **Principle 5:** A response process, including reporting, in relation to potential fraud, bribery and money laundering events and a coordinated investigation approach which is used to ensure potential fraud, bribery and money laundering events are dealt with in a timely manner.

It is the responsibility of the subsidiary boards to establish controls and procedures to prevent and detect fraud, bribery and money laundering and, therefore, safeguard the assets of the Group. This responsibility is delegated to management to apply and enforce on a day-to-day basis.

2. Who does this policy apply to?

This Policy applies to the Group, each of its subsidiaries and all other parties who are given access to the Group's information and premises.

This Policy covers all persons whether:

- Group employees and employees of the subsidiary companies.
- Board/committee members.
- Temporary agency staff or volunteers; and Consultants, contractors and agents (whether employed on a casual or freelance basis or otherwise).
- All other such persons acting for and on behalf of the Group.

If the action taken by the Group includes disciplinary action in relation to a member of staff, the relevant disciplinary procedures must be followed.

3. What is bribery?

Bribery is the giving or receiving of gifts, money, hospitality or other advantage in connection with the improper performance of a position of trust, or a function that is expected to be performed impartially or in good faith.

The Bribery Act 2010 came into force on 1 July 2011, repealing and replacing the existing laws on bribery with a new comprehensive anti-bribery code. There are four main bribery offences under the Act:

- Active Bribery - offering, promising or giving bribes.
- Passive Bribery - requesting, agreeing to receive or accepting bribes.
- Bribery of a foreign public official.
- Failure of a commercial organisation to prevent bribery (also known as the "corporate offence").

The corporate offence can take place if an organisation fails to prevent bribery by any of its employees, subsidiaries, agents or service providers or other associated persons (defined as a person who "performs services" for or on behalf of an organisation, which may include employees, contractors, agents, service providers and subsidiaries). It will be a defence to the corporate offence if an organisation can show that it had "adequate procedures" designed to prevent bribery occurring on its behalf.

Please remember that the Bribery Act 2010 has a very wide territorial scope. The general bribery offences apply to acts of bribery committed anywhere in the world by companies incorporated in the UK as well as individuals who are British citizens or ordinarily resident in the UK.

There are serious criminal penalties for committing a bribery offence under the Act, including up to 10 years in prison or an unlimited fine for individuals. The Group may also have to pay a fine, the level of which is unlimited.

4. Facilitation payments

The Group specifically prohibits the making of facilitation or "grease" payments. Facilitation payments are usually described as unofficial payments made to secure or speed up routine actions, often by public officials. Such routine actions can include issuing permits, licences or consents, immigration controls, scheduling inspections associated with contract performance, providing services or releasing goods held in customs. The payment offered or requested may only be small, but it will still be considered a bribe unless it is permitted or required by written local law. Broadly speaking, 'public officials' include any person who works for or represents any state or local government organisation and any person who works for a business which is owned by the state or local government (e.g. airport, railway company).

5. Red Flags

The following (non-exhaustive) list indicates examples of behaviours and circumstances which are considered red flags under this Policy:

- The provision of cash or cash equivalent (such as gift cards, loans, securities, share-options, gold, other precious metals or gemstones, etc.);
- Gifts or hospitality that is unduly lavish or excessive;
- Unusual payment terms, frequent or unexplained changes to third-party bank account details and/or unusually high commission paid to third parties;
- Transactions involving a party with a poor business reputation or a reputation for unethical conduct, including previous reports of suspicious, unethical or unlawful conduct; and
- Anything that could be construed as a bribe or kickback, or intended to influence the recipient to carry out a job or official duty in an improper way.

Please note that the red flags outlined above apply to the use of corporate as well as personal funds. They also apply to cases of indirect contributions, payments or gifts made through consultants, advisors, suppliers, customers or other third parties.

6. What is fraud?

Fraud is broadly defined as:

- **Fraud by false representation -** where an individual dishonestly and knowingly makes a representation that is untrue or misleading.

- **Fraud by wrongfully failing to disclose information -** where an individual wrongfully and dishonestly fails to disclose information to another person when they have a legal duty to disclose it, or where the information is of a kind that they are trusted to disclose it, or they would be reasonably expected to disclose it.

- **Fraud by abuse of position –** where an individual who has been given a position in which they are expected to safeguard another person’s financial interests dishonestly and secretly abuses that position of trust without the other person’s knowledge.

The Fraud Act 2006 creates new offences of obtaining services dishonestly and of possessing, making and supplying articles for use in frauds. It also contains a new offence of fraudulent trading applicable to non-corporate traders.

For fraud to be committed under the Fraud Act 2006 there will need to be an identifiable intent by the individual to make a gain or to cause a loss or to expose another to the risk of loss.

7. What is money laundering?

Money laundering is the illegal process of concealing the origins of money so that proceeds of crime are “cleaned” and appear to come from a legitimate source. Although there is no set statutory definition in the UK, the relevant anti-money laundering offences may be committed under the following legislation:

- The Proceeds of Crime Act 2002 (POCA)
- The Terrorism Act 2000
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

The Group seeks to mitigate money laundering risks effectively through:

- Identifying our customers and knowing their ownership and control structure.
- Understanding our relationship with them.
- Applying suitable controls and protection when onboarding new clients.

Internal controls and monitoring systems are in place to alert staff should criminals try to use the Group for money laundering, try to purchase goods fraudulently or to engage in any other financial crime.

Once aware of any potential threat, the Group will take steps to prevent it and escalate as appropriate, in line with our Confidential Reporting Whistleblowing Policy. Please see the "Managing the risk" section below for further detail on preventative measures and existing controls in this area.

The Group and its employees must remain vigilant to new types of financial crime and amend its policies and procedures where necessary to respond to new threats.

8. Examples of fraud, bribery and money laundering

In the context of the Group, some examples of actions that could be considered to be fraud, bribery and money laundering are as follows, although the list is by no means exhaustive:

<u>Fraud</u>

- Theft of any company property.
- Theft of petty cash/bankings.
- Forgery or alteration of any document, for example a cheque.
- Destruction or removal of records.
- Falsifying expense claims.
- Receiving incorrect salary overpayments and not informing or reimbursing the Group.
- Use of the Group's assets and facilities for personal use.
- Fraudulent use of computer time and resources, including unauthorised personal browsing on the Internet.

These last two examples would obviously exclude any reasonable, occasional but limited personal use, for example phone calls when away on company business or personal use of the computer in accordance with the Group's IT Usage Policies.

Bribery

- Allocation of property without following approved allocations policies and procedures, in return for a reward.
- Offering employment without following approved recruitment policies and procedures, in return for a reward.
- Acceptance of goods and services as an inducement to giving work to any supplier.
- Disclosing confidential information to outside parties without authority for personal gain.
- The giving or receiving of "facilitation payments" or kickbacks (as discussed above).

Money Laundering

- Sudden changes in customer ordering, delivery and/or payment requests, or those who may agree to bear very high or uncommercial penalties or charges.
- Other irregularities and/or suspicious transactions both within the Group and in organisations with which the Company contracts with.

9. Managing the risk

Fraud, bribery and money laundering should be considered as a set of risks to be managed alongside other business risks and, therefore, need to be embedded into the Group's risk management process.

In this context, 'risk' is the vulnerability or exposure that the Group has towards fraud, bribery and money laundering irregularity. It combines the likelihood of fraud, bribery and money laundering occurring and the corresponding impact measured in monetary, legislative, customer/client or reputational terms.

Preventative controls and the right type of culture operating within the Group will reduce the likelihood of fraud, bribery and money laundering occurring while detective controls and effective contingency planning can reduce the size of any losses or damage to our reputation.

In broad terms managing the risk of fraud, bribery and money laundering involves:

- Assessing the Group's overall vulnerability to fraud, bribery and money laundering.
- Identifying the key risk areas most vulnerable to the risk of fraud, bribery and money laundering.
- Considering the likely impact of fraud, bribery and money laundering occurring in these key risk areas.
- Assessing the scale/likelihood of fraud, bribery and money laundering occurring in the key risk areas.
- Identifying and evaluating existing controls to prevent fraud, bribery and money laundering.
- Developing an action plan and assigning ownership (i.e. allocating responsibility for fraud, bribery and money laundering).
- Implementing revised controls to improve the Group's approach to fraud, bribery and money laundering.
- Reviewing, monitoring and evaluating the impact of revised controls.
- Measuring the effectiveness of the fraud, bribery and money laundering-risk approach.
- Communicating relevant policies and procedures throughout the Group, and to other agency staff, consultants and contractors.
- Training teams as appropriate on the specific fraud, bribery and money laundering risks they may face (as further discussed below).

Managing the risk of fraud, bribery and money laundering is the same in principle as managing any other business risk and the annual risk management cycle should, therefore, look to cover areas set out below:

9.1 Identifying the key risk areas

Managers should:

- Establish the areas most vulnerable to fraud, bribery and money laundering risk, through the responsible managers undertaking an overall review of their local areas of activity to identify those areas most vulnerable to fraud, bribery and money laundering, for example, cash handling, procurement, accounts payable, allocations, recruitment, asset protection and sensitive information.
- Identify patterns of loss, if applicable, and areas of potential loss so that vulnerable areas can be pinpointed.

9.2 Considering the impact of a potential fraud, bribery and money laundering

Managers assess the possible impact that any type of reported fraud, bribery and money laundering can have in a wide variety of areas including, for example:

- The overall reputation of the Group
- Potential financial loss
- Potential criminal and civil liabilities
- Loss of confidence in the organisation
- Effect on staff morale and productivity
- Potential increase in insurance costs
- Need to utilise resources in investigative work

9.3 Assessing the scale/likelihood of fraud, bribery and money laundering

Managers assess the possible scales and likelihood of fraud, bribery and money laundering to ensure that the anti-fraud, bribery and money laundering arrangements that are in place are adequate. This analysis considers:

- The impact of a potential fraud, bribery or money laundering both on the organisation as a whole and in relation to the specific operational area.
- Monitoring and review of national/local trends in relation to new and emerging fraud, bribery and money laundering and considering the potential impact on the Group

9.4 Identifying the adequacy of existing controls

Managers evaluate the adequacy of existing controls and establish what further controls or enhancements to existing controls are required to mitigate the risk. It is also the duty of each employee to apply existing controls and feedback any discrepancies or potential issues to their appropriate line manager.

Existing controls should include:

- Adequate segregation of duties between key control areas.
- Staff resources that are sufficient to provide adequate control and are organised in a structured manner.
- Published local schemes of delegation identifying levels of responsibility and authority.
- Regular reconciliation of budgets that are subject to independent review.
- IT security arrangements (including security systems and codes of conduct for IT usage).
- Asset control register (cash, fixed assets), inventories, asset marking, etc.
- Documented policies and procedures that are subject to regular review.

- Maintenance of adequate records of risk assessment procedures.
- Appropriate due diligence on vendors/customers to assess the relevant risk level.

9.5 Prevention and detection of risks

The Group has in place a framework of preventative measures, including internal controls, designed to prevent fraud, bribery and money laundering occurring in the first instance.

These consist of rules, regulations, policies and procedures within which employees, board/committee members, agency staff, consultants and contractors are expected to operate and include:

- Code of Conduct
- Registers of gifts and hospitality
- Disciplinary procedures for employees
- A confidential reporting Speak Up Policy
- Financial Principles and Regulations

It is the responsibility of managers, as well as employees, board/committee members, agency staff, consultants and contractors to actively deter, prevent and detect fraud, bribery and money laundering by maintaining and applying good control systems and ensuring that those around them are familiar with them.

The most common control weaknesses to be aware of include:

- Too much trust being placed in employees.
- Lack of proper procedures for authorisation.
- Lack of adequate segregation of duties.
- Lack of independent checks on employee activities.
- Lack of clear line of authority.
- Infrequent reviews of departmental authority.
- Inadequate documents and records (leading to a loss of a ‘management trail’).

Prevention is preferable to detection and, therefore, preventative controls should be applied as appropriate, bearing in mind, the risk of fraud, bribery and money laundering and the potential for loss to the Group. However, preventative controls may not be sufficient to guard against determined individuals and detective controls are therefore important. Detective controls are established to detect errors, omissions and fraud, bribery and money laundering after the event has taken place.

Management are alerted to the factors which might indicate that fraud, bribery and money laundering is taking place. These include:

- Opportunity (e.g. where there is a lack of separation of duties so that one person has control over all aspects of a transaction, for example, over a purchase order, purchase invoice and purchase payment authorisation).
- Over-ride (e.g. where a manager over-rides the normal control system/procedure. In practice this may be necessary, however, if done frequently it may be indicative of non-compliance).
- Situational pressure (e.g. personal factors, which may be indicative of a tendency/temptation to fraud/bribery/money laundering).

Staff need to be vigilant to the warning signs and indicators of fraud, bribery and money laundering. Please see the "Red Flags" section above for examples of warning signs to be aware of.

9.6 Risk register

It is the responsibility of Senior Management to assess and review the risk of fraud, bribery and money laundering in their area on a regular basis and to ensure that local line management and colleagues implement any action plans.

9.7 Gifts and hospitality

It is sometimes customary and appropriate, particularly in connection with product demonstrations or promotional events, to give and receive reasonable and proportionate gifts and/or hospitality.

However, if the giving or receiving of gifts or hospitality is in any way for the purposes of obtaining an inappropriate advantage or benefit, then this may amount to a bribe which is prohibited under this and other Group policies and by law.

Bribery is a criminal offence. The Group prohibits employees from offering, giving, or receiving bribes or personal inducements, or requesting others to do so on their behalf, for any purpose. The Group's approach is for all employees to ensure that their actions concerning Gifts and Hospitality are open, proportionate, in good faith, lawful and help to enhance and protect the reputation of the Group.

All employees shall ensure that any gifts or hospitality offered, given or received shall:

- Be in good faith, occasional, appropriate and reasonable, and comply with any applicable laws.
- Be for reasons related to the business of the Group and the specific individuals involved.
- Be within the financial limits set out in the Policy and never be lavish or extravagant.
- In respect of Government or public sector controlled customers, comply with their rules and regulations.
- Never be connected in any way to the obtaining of an inappropriate advantage or benefit.

Gift registers exist to log incoming and outgoing "gifts" and it is each person's responsibility to log items that are given or received in relation to work and business. Anyone found to be in violation of the relevant policy and procedure will be subject to disciplinary action.

9.8 Monitoring and Reporting Concerns

The Board and/or its assigned committee, will review this Policy on a regular basis and communicate the outcomes of such review to the persons to whom this Policy applies.

Any issues or concerns with the running of this Policy or related matters should be immediately flagged to the Group Company Secretary (wk.groenewald@bytesplc.com) so that appropriate action may be taken. You may also report any concerns anonymously by following our confidential reporting Speak Up Policy. Please note that those covered by this Policy will not suffer any detrimental effects by virtue of raising any concerns in good faith.

9.9 Training

Compliance with this Policy is mandatory and it is vital that all employees, board/committee members, agency staff, consultants and contractors know the rules and comply with them. Disciplinary measures may be taken against any employee found to be involved in fraud, bribery or money laundering.

We will provide appropriate training on the scope and application of the Policy at appropriate and regular intervals. New employees, board/committee members, agency staff, consultants and contractors will also receive training as part of the induction process.

9.10 Regulatory requirements

The Group will at all times ensure that it complies with all regulatory requirements relating to fraud, bribery and money laundering. The Group will provide assistance to relevant authorities where required in connection with any external investigations involving breaches under this Policy.

9.11 Record Keeping

All gifts and hospitality must be recorded in a Gifts register and written receipts kept for items gifted or hospitality provided. This does not apply to nominal value items. This Gifts register will be subject to review by the appropriate management team. In addition, written records of any breaches or investigations under this Policy will be kept by the relevant management in question in accordance with confidentiality reporting under the Speak Up Policy.

END

Policy Owner	Chief Financial Officer
Version	2.0
Approver	BTG Plc Board
Approval Date	15 August 2025