STATWIG GLOBAL PTE LTD

CORPORATE POLICIES

Contents

Dated 23rd August, 2021

POLICY OBJECTIVES

The safety and wellbeing of those we work with is of paramount importance to us. This includes staff, and the people we work with. We have a zero-tolerance approach towards all forms of unethical behaviour.

We also have a zero tolerance towards bribes, facilitation payments, tax evasion and money laundering. We will do all we can to prevent financing or the support of terrorist organisations and will not appoint or employ anyone that could reasonably be suspected to be connected to a terrorist group. We will abide by all the Laws in all matters including those related to modern slavery.

We require all staff and other people we work to refrain from any practices that could be counter to the above policy principles.

We request all those we work with to immediately raise any concerns relating to our work, whether concerns are suspected or confirmed, and whether specific or general in nature. Concerns are termed "incidents" and a full definition of these can be found below.

Anyone raising a concern should do so with the confidence that we will deal with all concerns as swiftly and professionally as possible, and protect them from detriment as a result, to the fullest extent that we can.

We will fulfill our legal, contractual and regulatory requirements in reporting incidents to relevant bodies, and assist the relevant external agencies with any investigations to the fullest extent that we can.

We will examine the policies and procedures of all organisations we deal with to ensure the principles of this policy also apply to them. Where necessary, we will include contractual requirements for third parties to implement these principles. We may refuse to work with, or stop working with, any party that does not abide by these principles.

WHAT IS AN INCIDENT

We regard an Incident as any actual or attempted:

- Acts of child abuse and exploitation, this includes physical abuse, neglect, emotional abuse, sexual abuse and wider exploitation (such as child labour and early marriage)
- Sexual misconduct
- Acts of modern slavery or human trafficking
- Acts causing harm or major detriment to a vulnerable group (as defined below)
- Acts of theft, fraud, bribery, money laundering, funding of terrorism, tax evasion and other forms of corrupt practice
- Instances where someone's health and safety is, or believed to be, in danger
- Any forms of illegal activities not covered above
- Undisclosed or emergent major conflicts of interest
- Attempts to cover up wrongdoing
- Data protection breaches

These include acts in relation to any work engaged by us.

Any concern or issue should be reported immediately to harsha@statwig.com

The above list is not intended to be exhaustive; any concerns that fall outside these categories but have caused harm, or have the potential to cause harm, should be reported.

SAFEGUARDING OF CHILDREN AND VULNERABLE GROUP

Definitions:

A vulnerable group is any identifiable group of individuals that could be at higher risk of harm or exploitation or are less likely to be able to defend themselves from harm or exploitation that results from the actions of Statwig or anyone we work with.

These groups will depend on the context. They may include (but are not limited to):

- People within different age ranges, especially children (defined as anyone of 14 years and under), young persons (who is 14 years of age or above but below the age of 16 years) and older people (anyone over the age of 50)
- People of a particular gender and/or sexual orientation
- People with disabilities or illnesses
- People with particular religious beliefs, or none
- People with a particular ethnicity, nationality, or geographical background
- People with a particular marital status
- People who are pregnant, or have recently had or adopted children
- People with particular political views, including members of political organisations
- People who are carers for people classed as vulnerable
- People who are refugees, internally displaced persons, or affected by a humanitarian crisis
- People of a particular economic class, or members of a particular trade or profession

"Harm" includes:

- physical, mental or sexual abuse
- the denial of fundamental rights
- the loss of financial, physical, sentimental or cultural assets

"Exploitation" is the unjust or unethical use of a power relationship in order to benefit from that relationship.

- According to the Children and Young Person Act (CYPA) 2001, a "child" is a person below the age of 14. A "young person" means a person who is 14 years of age or above but below the age of 16 years. A "juvenile" means a male or female person who is 7 years of age or above but below the age of 16 years. The Employment Act adopts the same definitions as the CYPA for a "child" and a "young person".

Policy Statement:

Statwig and those who work with us must not cause harm or allow harm to come to anyone who is a member of a vulnerable group through negligence.

Prevention with Employees:

We will use standard disclosure to vet all new employees in the Company for potential safeguarding risks (or similar services in the relevant countries if we employ people abroad). We will refuse employment to those deemed a risk to vulnerable groups.

We discourage those who may pose a safeguarding risk from applying for a role with us by including the following statement on all recruitment adverts:

"We are committed to the safeguarding and protection of children and vulnerable people in our work. We will do everything possible to ensure that only those who are suitable to work with children and vulnerable people are recruited to work for us. This post is subject to a range of vetting checks including a criminal records disclosure".

When employees visit projects, we will ensure wherever possible that the visit is not conducted alone. The itinerary for any trip must be agreed beforehand, and must not include a point where any Statwig employee is alone with a member of a vulnerable group

ANTI-BRIBERY AND ANTI CORRUPTION POLICY:

Definitions:

Gratification" includes —

(a) money or any gift, loan, fee, reward, commission, valuable security or other property or interest in property of any description, whether movable or immovable;

(b) any office, employment or contract;

(c) any payment, release, discharge or liquidation of any loan, obligation or other liability whatsoever, whether in whole or in part;

(d) any other service, favour or advantage of any description whatsoever, including protection from any penalty or disability incurred or apprehended or from any action or proceedings of a disciplinary or penal nature, whether or not already instituted, and including the exercise or the forbearance from the exercise of any right or any official power or duty; and

(e) any offer, undertaking or promise of any gratification within the meaning of paragraphs (*a*), (*b*), (*c*) and (*d*);

Policy Statement:

Statwig and those who work with us must not give, accept, offer or solicit gratifications, bribes or facilitation payments.

Statwig and those who work with us must not accept any gifts or hospitality unless they are freely given with no expectation of gain on behalf of the giver, and there is no potential to damage Statwig's reputation if it were accepted.

Statwig will not make payments if it thinks that such a payment could be construed as a gift, bribe or facilitation payment.

Statwig will not assist any person or organisation to evade tax legally payable anywhere in the world.

Prevention Internally:

All employees are encouraged to raise concerns about any issue or suspicion of malpractice at the earliest possible stage. If any of the employees are unsure whether a particular act constitutes bribery or corruption, or if you have any other queries, these should be raised with the General Manager immediately.

The General Manager will monitor and review the concerns regularly and any improvements identified will be made as soon as possible. Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in countering bribery and corruption.

ANTI MONEY LAUNDERING AND ANTI TERRORISM FINANCING

Definitions:

"terrorism financing offence" means —

(a) any offence under section 3, 4, 5 or 6 of Terrorism (Suppression Of Financing) Act;

(b) conspiracy to commit any of those offences;

(c) inciting another to commit any of those offences;

(d) attempting to commit any of those offences; or

(e) aiding, abetting, counselling or procuring the commission of any of those offences;

Money Laundering" is an action aimed at concealing the identity, source or destination of the proceeds of crime or other illicitly-obtained money.

"Terrorist financing" can occur where:

- Funds or assets are transferred for the benefit of a terrorist group
- A terrorist group seizes funds or assets by force

Policy Statement:

Statwig will not allow another organisation to use Statwig's bank accounts to channel funds on their behalf.

Statwig will not support any terrorist group. Statwig will not:

- Arrange meetings that encourage support for any terrorist group
- Make any direct or indirect payment or asset transfers to anyone where Statwig reasonably suspect is connected to terrorism, even if they are locally in a position of authority
- Appoint or employ anyone that could reasonably be suspected to be connected to a terrorist group

Prevention Internally:

Statwig employees should report any instances of individuals or organisations who wish to make donations or other payments to us in unusual circumstances or with unusual conditions attached. These could include:

- Unsolicited loans
- Grants or donations that are expected to be returned, at least in part, at a later date
- Grants or donations for a specific project where the donor insists on a particular implementing partner or supplier
- Monies given on condition that the donor gains some benefit from the donation or the project being funded
- Organisations treating Statwig's bank account as a conduit (e.g., money to be held by Statwig on behalf of another organisation and then either returned to the organisation or passed to another)
- Where we can reasonably believe that funds represent the proceeds of crime

Statwig employees should not proceed with any transaction that appears suspicious unless given permission to do so from the management team.

MODERN SLAVERY AND HUMAN TRAFFICKING:

Definitions:

- Slavery – Exercising powers of ownership over a person
- Servitude – Imposing an obligation to provide services through coercion
- Forced or Compulsory Labour – Exacting work or services under menace of a penalty, for which the person has not offered themselves voluntarily

Trafficking in persons

3.—(1) Any person who recruits, transports, transfers, harbours or receives an individual (other than a child) by means of —

(*a*) the threat or use of force, or any other form of coercion;

(*b*) abduction;

(*c*) fraud or deception;

(*d*) the abuse of power;

(*e*) the abuse of the position of vulnerability of the individual; or

(*f*) the giving to, or the receipt by, another person having control over that individual of any money or other benefit to secure that other person's consent,

for the purpose of the exploitation (whether in Singapore or elsewhere) of the individual shall be guilty of an offence.

Prevention Internally:

Our recruitment and employment procedures include appropriate pre-employment screening of all staff to determine the right to work.

Given the nature of our digital marketing business model, we consider the risk of modern slavery in the services is fairly low to be directly affected by modern slavery and/or human trafficking.

REPORTING AN INCIDENT (Whistleblowing Policy)

Definition:

A whistleblower is anyone who reports a suspicion of an incident to Statwig. This is therefore not limited to Statwig employees.

Any concern or issue should be reported immediately to harsha@statwig.com

Protection of Whistleblowers' Confidentiality:

We will protect the confidentiality of whistleblowers and prevent them from harm or detriment as a result of their report as much as it is in our powers to do so.

Any concerns or issues can be reported anonymously if the whistleblower feels this is the best course of action. We will respect their anonymity as best we can, however, any investigations may be at a disadvantage if we are unable to contact the whistleblower to discuss their concerns.

Treating all reports seriously:

Our policy is to treat all reports of incidents with the utmost seriousness and will respond to reports as soon as it is practicable to do so. This is normally within two working days of receiving a concern.

What whistleblowers' can expect:

We will acknowledge the report and may also request further information, if an investigation is appropriate. We cannot state exactly how long any investigation may take, as this will be determined by the context of the incident, but we will keep the whistleblower informed of progress as much as we are able to do so.

During the course of any investigation, it may not be possible to keep details entirely confidential, as we have legal duties to inform our donors and regulatory agencies of some types of incident. When this occurs, we will inform the whistleblower in advance, where we are allowed to do so, and work with them to prevent any harm or detriment.

During any investigation, it may not be possible to share all details that the investigation uncovers, however, we will keep the whistleblower informed of progress as much as we can.

Protection of Internal Whistle Blowers:

We will protect any employee that reports an incident, even if their suspicion turns out later to be false, as long as they had a genuine belief that the suspicion could be true. Employees will not be victimised in the workplace or suffer any detriment to their appraisals or career prospects. However, we do consider the malicious reporting of a suspicion that is known to be false from the start to be a disciplinary offence.

INCIDENT MANAGEMENT PLAN

Company's incident management policy aims at proactively safeguard the organization from external threats and operational inefficiencies.

We will detect the incident as soon as, or if possible, even before it happens and immediately notifying the relevant teams that can decisively deal with it before things get out of hand. After detecting an incident that is compromising company systems and operations, mitigation measures are put in action to restrict the threat. After all the relevant data is gathered, the incident is resolved and brought to a close. Once the incident has been resolved satisfactorily, business systems and operations are restored to their proper functioning.

Any concern or issue of any incidents should be reported immediately to harsha@statwig.com

*****