Safety / Health / Environment and Quality Policy HSP-01

Inner City Traffic Management Ltd (hereon ICTM) aims to achieve the highest standards of Safety, Health, Environment and Quality (SHEQ); the company's certification to ISO9001: 2015 compliant with national Highways Sector Scheme 12D, and implementation of ISO14001: 2015 provides evidence of this commitment.

All Management are responsible for delivering the ethos of this policy; in doing so we have identified the health and safety of its employees, contractors and visitors, maintaining the satisfaction of its interested parties, and protect the environment as essential requirements, we shall ensure the entire organisation is oriented towards achieving these goals openly and transparently.

SHEQ management and risk assessment fundamentals are integrated in all business processes.

ICTM are committed to training all our employees in the appropriate use of the management systems in place as appropriate, and ensure professional, managerial skills and 'on the job' skills are updated when needed.

Nothing is more important than the health and safety of everyone who works for us and uses our products or services. All injuries and work-related illnesses can and must be prevented. Working safely is always a condition of employment.

Adopting strong Safety, Health, Environment and Quality principles in everything we do is our main competitive advantage; and we recognise the need to satisfy the requirements and expectations of interested parties.

Commitment to preventing pollution and minimizing the environmental impact of our operations is always a fundamental requirement of our activities, and where appropriate we shall make the most efficient use of natural resources and energy.

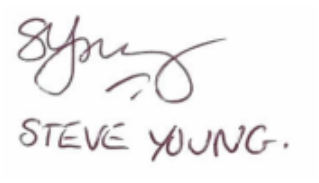
We recognise the importance of implementing this policy throughout our management systems, covering the entire supply chain from suppliers to customers and the proper and efficient use of our services in accordance with their agreed specifications. ICTM commits to comply with all applicable compliance and legal requirements to which it subscribes.

We shall communicate this policy throughout the organisation and engage them in the regular setting, measuring and revision of objectives.

We are committed to developing a long-term sustainable business, by improving and investing in all areas of the business; this is achieved by identifying and reviewing objectives, risks, and opportunities annually at each Management Review.

We will undertake to keep this policy updated, to implement and maintain our management system, and continuously improve our performance in all areas of our business activity.

Signed



Managing Director
Date: 24/11/2023

CONSULTATION- HSP-02

We accept our duty under the current edition of the Health and Safety (Consultation with Employees) Regulations to consult you on health and safety matters, particularly regarding:

- Any measures that may substantially affect your health and safety.
- Our arrangements for obtaining the assistance of a competent person to help us manage health and safety.
- Information about risks to your health and safety and preventative measures.
- The planning and organisation of any health and safety training that you will need to work safely.
- The health and safety consequences of the introduction of new technologies into the workplace.

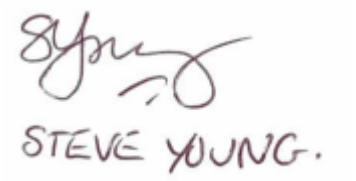
We will be consulting you directly.

You will be provided with such information as is necessary to enable you to participate fully and effectively in the consultation. Such information will be provided by the means most appropriate to the matters and circumstances concerned. The main means of consultation is the Foreman/Operatives meeting. Representatives from the company's various activities will attend the meetings.

Other means of consultation may include, but will not be limited to, the following: -

- Conversations with individuals.
- Information displayed on notice boards.
- Letters attached to payslips.

We encourage all employees to take an active interest in health and safety matters and welcome positive suggestions for improvement. If you would like to raise a matter for discussion, you should bring this to the attention of the Contract Director.



Managing Director
Date: 24th November 2023

Equal Opportunities Policy-HSP-03

Statement of policy and purpose of policy

1. Inner City Traffic Management (the **Employer**) is committed to equal opportunities for all staff and applicants.

2. It is our policy that all employment decisions are based on merit and the legitimate business needs of the organisation. The Employer does not discriminate on the basis of race, colour or nationality, ethnic or national origins, sex, gender reassignment, sexual orientation, marital or civil partner status, disability, religion or belief, age or any other ground on which it is or becomes unlawful to discriminate under the laws of England and Wales (referred to as **Protected Characteristics**).

3. Our intention is to enable all our staff to work in an environment which allows them to fulfil their potential without fear of discrimination or harassment. The Employer's commitment to equal opportunities extends to all aspects of the working relationship including:

    - recruitment and selection procedures.
    - terms of employment, including pay and benefits.
    - training, career development and promotion.
    - work practices, conduct issues, allocation of tasks, discipline, and grievances.
    - work-related social events; and
    - termination of employment and matters after termination, including references.

4. This policy is intended to help the Employer achieve its diversity and anti-discrimination aims by clarifying the responsibilities and duties of all staff in respect of equal opportunities and discrimination.

5. The principles of non-discrimination and equal opportunities also apply to the way in which staff treat visitors, clients, customers, suppliers, and former staff members.

6. This is a statement of policy only and does not form part of your contract of employment. This policy may be amended at any time by the Employer, in its absolute discretion.

Who is responsible for equal opportunities?

7. Achieving an equal opportunities workplace is a collective task shared between the Employer and all its staff. This policy and the rules contained in it therefore apply to all staff of the Employer irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants, and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers or interns (referred to as **Staff**).

8. The board of directors of the Employer has overall responsibility for this policy and for

equal opportunities and discrimination law compliance in the workplace and the MR S Young has been appointed as the person with day-to-day operational responsibility for these matters.

9. All Staff have personal responsibility to ensure compliance with this policy, to always treat colleagues with dignity and not to discriminate against or harass other members of Staff, visitors, clients, customers, suppliers and former staff members. In addition, Staff who take part in management, recruitment, selection, promotion, training and other aspects of career development (referred to as **Managers**) have special responsibility for leading by example and ensuring compliance.

10. Managers must take all necessary steps to:

- promote the objective of equal opportunities and the values set out in this policy.
- ensure that their own behaviour and those of the Staff they manage complies in full of this policy;
- ensure that any complaints of discrimination, victimisation or harassment (including against themselves) are dealt with appropriately and are not suppressed or disregarded.

What is discrimination?

11. Discrimination occurs in different ways, some more obvious than others. Discrimination on the grounds of any of the Protected Characteristics is prohibited by law, even if unintentional, unless a particular exception applies.

Direct discrimination

12. Direct Discrimination is less favourable treatment because of one of the Protected Characteristics. Examples would include refusing a woman a job as a chauffeur because you believe that women are not good drivers or restricting recruitment to persons under 40 because you want to have a young and dynamic workforce.

13. Direct discrimination can arise in some cases even though the person complaining does not actually possess the Protected Characteristic but is perceived to have it or associates with other people who do. For example, when a person is less favourably treated because they are (wrongly) believed to be homosexual or because they have a spouse who is Muslim.

Indirect discrimination

14. Indirect discrimination arises when an employer applies an apparently neutral provision, criterion, or practice which in fact puts individuals with a particular Protected Characteristic at a disadvantage, statistically. To show discrimination the individual complaining also must be personally disadvantaged. An example would be a requirement for job candidates to have ten years' experience in a particular role, since this will be harder for young people to satisfy. This kind of discrimination is unlawful unless it is a proportionate means of achieving a legitimate aim.

Victimisation

15. Victimisation means treating a person less favourably because they have made a complaint of discrimination or have provided information in connection with a complaint or because they might do one of these things.

Harassment

16. Harassment is:

- unwanted conduct which is related to a Protected Characteristic, and which has the purpose or effect of violating a person's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for them: or
- unwanted conduct which is of a sexual nature, and which has the purpose or effect of violating a person's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for them (**Sexual Harassment**); or
- less favourable treatment because of the rejection of or the submission to Sexual Harassment.

17. Harassment can arise in some cases even though the person complaining does not actually possess a Protected Characteristic but is perceived to have it or associates with other people who do. For example, when a person is harassed because they are (wrongly) believed to be homosexual or because they have a spouse who is Muslim.

18. Harassment may include:

- use of insults or slurs based on a Protected Characteristic or of a sexual nature or other verbal abuse or derogatory, offensive or stereotyping jokes or remarks.
- physical or verbal abuse, threatening or intimidating behaviour because of a Protected Characteristic or behaviour of a sexual nature.
- unwelcome physical contact including touching, hugging, kissing, pinching or patting, brushing past, invading personal space, pushing grabbing or other assaults.
- mocking, mimicking or belittling a person's disability, appearance, accent or other personal characteristics.
- unwelcome requests for sexual acts or favours; verbal sexual advances, vulgar, sexual, suggestive or explicit comments or behaviour.
- repeated requests, either explicitly or implicitly, for dates.
- repeated requests for social contact or after it has been made clear that requests are unwelcome.
- comments about body parts or sexual preference.
- displaying or distributing offensive or explicit pictures, items or materials relating to a

Protected Characteristic or of a sexual nature.

- shunning or ostracising someone, for example, by deliberately excluding them from conversations or activities.
- 'outing' or threatening to 'out' someone's sexual orientation (ie to make it known);
- explicit or implicit suggestions that employment status or progression is related to toleration of, or acquiescence to sexual advances, or other behaviour amounting to harassment.

19. Other important points to note about harassment:

- a single incident can amount to harassment.
- behaviour that has continued for a long period without complaint can amount to harassment.
- it is not necessary for an individual to intend to harass someone for their behaviour to amount to harassment.
- it is not necessarily for an individual to communicate that behaviour is unwelcome before it amounts to harassment; and
- the onus is on each individual to be certain that their behaviour and conduct is appropriate and is not unwanted and in the case of doubt, you must refrain from such conduct.

Disabled persons

20. Any Staff member who considers that they may have a disability is strongly encouraged to speak with the Steve Young, so that appropriate support can be provided, if needed. For these purposes, disability includes any physical or mental impairment which substantially affects your ability to perform day to day activities and has lasted (or is likely to last) more than 12 months. Disclosure of this information will be treated in confidence, if you wish it to be, so far as is reasonably practicable and we will do our best to handle matters sensitively and to ensure that you are treated with dignity and with respect for your privacy. We will consult with you about whether adjustments are needed to avoid you being disadvantaged and may ask you to see a doctor appointed by us, to advise on this. We will seek to accommodate your needs within reason.

21. Managers with responsibility for managing a member of Staff who they know or think to be disabled should speak to Steve Young to ensure that all relevant duties are complied with.

Making employment decisions fairly

22. As noted above, the Employer will recruit employees and make other employment decisions concerning promotion, training, dismissal, and related issues. based on objective criteria.

23. Managers should only stipulate criteria or conditions for employment decisions (including job selection, promotion, and redundancy) which are based on a legitimate business need and which do not go further than is needed to satisfy that need. If you are in any doubt about whether particular criteria or conditions are indirectly discriminatory or justifiable, then please speak to Steve Young.

Recruitment

24. Managers involved in recruitment must:

- specify only recruitment criteria that are relevant to the job, reflect genuine business needs and are proportionate. More than one person should be involved in short-listing of applicants wherever practicable.
- ensure that vacancies are advertised to a diverse audience and try to avoid informal recruitment methods that exclude fair competition. In very rare cases, it may be legitimate and necessary to restrict recruitment to a particular role to certain groups, but it is essential that this is discussed with the MR S Young so that appropriate steps can be taken to ensure legality.
- review job advertisements carefully to ensure that stereotyping is avoided and that particular groups are not unjustifiably discouraged from applying.
- not ask applicants about health or disability before a job offer is made (other than in exceptional circumstances).
- not ask candidates about current or future pregnancy, childcare, or related matters nor, in general, about matters relating to any Protected Characteristic; and
- not make assumptions about immigration status based on appearance, accent, or apparent nationality.
- so far as reasonably practicable, keep a written record of their reasons for relevant decisions.

25. The Employer is legally required to verify that all employees have the right to work in the UK. Prior to starting employment, all employees must produce original documents to the Employer's satisfaction, irrespective of nationality. Information about the documents required is available from the Mr S Young.

26. The Employer monitors applicants'

- Sex
- Ethnic group
- Disability
- Age

as part of our recruitment process. We do this to assess the effectiveness of our measures to promote equal opportunities and to help us identify and take appropriate steps to avoid discrimination and improve diversity. Provision of this information is voluntary and the information is kept in an anonymised format solely for the purposes stated here. The information will not be used as part of any decision-making process relating to the recruitment or employment of the person providing the information.

Staff training, career development and promotion

27. Training needs may be identified during the normal appraisal process. Appropriate training to facilitate progression will be accessible to all staff.

28. All promotion decisions will be made based on merit and according to proportionate criteria determined by legitimate business need.

29. Staff diversity at different levels of the organisation will be kept under review to ensure equality of opportunity. Where unjustified barriers to progression are identified, these will be removed.

Conditions of service

30. Access to benefits and facilities and terms of employment will be kept under review to ensure that they are appropriately structured and that no unlawful barriers to qualification or access exist.

Discipline and termination of employment

31. Access to benefits and facilities and terms of employment will be kept under review to ensure that they are appropriately structured and that no unlawful barriers to qualification or access exist.

32. Any redundancy selection criteria and procedures that are used, or other decisions taken to terminate employment, will be fair and not directly or indirectly discriminatory.

What to do if you encounter discrimination

33. If you believe that you have been the victim of discrimination, you should follow the Employer's Grievance Procedure.

34. Every member of Staff has a responsibility to combat discrimination if they encounter it. Staff who observe or are aware of acts that they believe amount to discrimination directed at others are encouraged to report these to the Steve Young.

35. Any grievance or report raised about discrimination will be kept confidential so far as this is practicable. We may ask you if you wish your complaint(s) to be put to the alleged discriminator if disciplinary action appears to be appropriate. It sometimes may be necessary to disclose the complaint or act even if this is not in line with your wishes, but we will seek to protect you from victimisation and, if you wish, we will seek to protect your identity. You should be aware that disciplinary action may be impossible without your co-operation or if you refuse to allow relevant information to be disclosed.

36. Staff who raise a complaint about or report discrimination in good faith will be protected from retaliation or victimisation. If you act in good faith, the fact that you have raised a

complaint or report will not affect your position within the Employer, even if the complaint is not upheld. Any member of Staff who attempts acts of retaliation or victimisation may be subject to disciplinary action up to and including summary dismissal for gross misconduct.

37. If you make a complaint, it may be necessary to ask you to stay at home on paid leave while investigations are being conducted and the matter is being dealt with through the appropriate procedure. This may particularly be necessary in cases of alleged harassment.

Non-compliance with equal opportunities rules

38. Any breach of equal opportunities rules or failure to comply with this policy will be taken very seriously and is likely to result in disciplinary action against the offender, up to and including immediate dismissal.

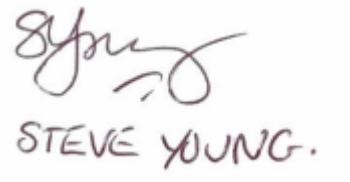
39. Staff should also note that:

- in some cases, they may be personally liable for their acts of discrimination and that legal action may be taken against them directly by the victim of any discrimination; and
- it may be a criminal offence intentionally to harass another employee.

Review of this policy

40. The board of directors of the Employer will keep this policy under review.

41. The Employer encourages Staff to comment on this policy and suggest ways in which it might be improved by contacting Steve Young.



Managing Director
Date: 24th November 2023

Corporate Social Responsibility HSP 04

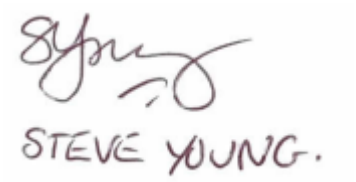
Our Code of Conduct

Our Code of Conduct provides a common behavioural framework for all Inner City TM employees irrespective of their specific job, direct employer or location and is based around these key values

- Comply with the law and are committed to the highest standards of governance.
- Always behave with honesty and integrity.
- Have regard for the views of our clients and employees alike.
- Are committed to the safety and health of our employees, our contractors, our suppliers, our clients and the general public we interact with.
- Value the rights and dignity of the individual, always ensuring that our words and actions demonstrate our belief in treating people with fairness and respect.
- Value diversity and a diverse workforce.
- Compete fairly and will not engage in corrupt practices.
- Communicate in an open and timely manner.
- Are committed to sustainable development and to achieving exemplary environmental performance.
- We shall not hire children who do not reach the legal age for work.
- No form of human trafficking, forced, bonded or compulsory labour shall be used.
- Wages, including overtime and benefits, shall comply with local law, including those relating to minimum wages, overtime hours and legally mandated benefits. Working hours shall comply with applicable local laws.
- Harassment or discrimination in any form is not acceptable.
- We encourage open communication with management regarding working conditions without fear of reprisal, intimidation, or harassment. We believe that maintaining an environment for dialogue between associates and management will deepen free, open-minded, and two-way communication, making it possible to build a stronger relationship of mutual trust. In addition, associates shall, in accordance with local laws, have the right to associate freely, and join—or choose not to join—labour unions or workers' council.

Commitment to Principles

In adhering to the above principles, we seek to communicate its commitment to its customers, associates, suppliers, dealers, and other business partners, and to the communities in which we live and work. Further, we expect that any party conducting business with us will embrace and uphold these principles to the best of their ability.



Managing Director. 24th November 2023

ANTI-BRIBERY POLICY HSP 05

Introduction

One of the Company's core values is to uphold sound, responsible and fair business operations. It is committed to promoting and maintaining the highest possible ethical standards in relation to all its business activities. The Company's reputation for maintaining lawful business practices is of paramount importance to it and this policy is designed to preserve these values. The Company therefore has a zero-tolerance policy towards bribery and corruption and is committed to acting fairly and with integrity in all of its business dealings and relationships wherever it operates and implementing and enforcing effective systems to counter bribery.

Purpose and scope

This policy sets out the Company's position on any form of bribery and corruption and provides guidelines aimed at:

- Ensuring compliance with anti-bribery laws, rules, and regulations, not just within the UK, but also in any other country within which the Company may carry out its business or in relation to which its business may be connected.
- Enabling employees and persons associated with the Company to understand risks associated with unlawful conduct and to enable and encourage them to be vigilant and to effectively recognise, prevent, avoid and report any wrongdoing, whether by themselves or others.
- Providing suitable and secure reporting and communication channels and ensuring that any information that is reported is properly and effectively dealt with.
- Creating and maintaining a rigorous and effective framework for dealing with any suspected instances of bribery or other unethical conduct.

This policy applies to all permanent and temporary employees of the Company (including any of its intermediaries, subsidiaries, or associated companies). It also applies to any individual or corporate entity associated with the Company or who performs functions in relation to, or for and on behalf of, the Company, including, but not limited to, directors, agency workers, casual workers, contractors, consultants, seconded staff, agents, suppliers, and sponsors ("associated persons").

All employees and associated persons are expected to adhere to the principles set out in this policy.

Legal obligations

The key UK legislation on which this policy is based is the Bribery Act 2010 and it applies to the Company's conduct both in the UK and abroad.

A bribe is an inducement or reward offered, promised, or provided to gain any commercial, contractual, regulatory or personal advantage.

It is an offence in the UK to:

- Offer, promise or give a financial or other advantage to another person (i.e., bribe a person) whether within the UK or abroad, with the intention of inducing or rewarding improper conduct.
- Request, agree to receive or accept a financial or other advantage (i.e., receive a bribe) for or in relation to improper conduct.
- Bribe a foreign public official.

You can be held personally liable for any such offence.

It is also an offence in the UK for an employee or an associated person to bribe another person in the course of doing business intending either to obtain or retain business, or to obtain or retain an advantage in the conduct of business, for the Company. The Company can be liable for this offence where it has failed to prevent such bribery by associated persons. As well as an unlimited fine, it could also suffer substantial reputational damage in connection with this offence.

Policy

All employees and associated persons are required to:

- Comply with any anti-bribery and anti-corruption legislation that applies in any jurisdiction in any part of the world in which they might be expected to conduct business.
- Act honestly, responsibly and with integrity.
- Safeguard and uphold the Company's core values by operating in an ethical, professional, and lawful manner always.

Bribery of any kind is strictly prohibited. Under no circumstances should any provision be made, money set aside, or accounts created for the purposes of facilitating the payment or receipt of a bribe.

The Company recognises that industry practices may vary from country to country or from culture to culture. What is considered unacceptable in one place may be normal or usual practice in another. Nevertheless, a strict adherence to the guidelines set out in this policy is always expected of all employees and associated persons.

If in doubt as to what might amount to bribery or other unethical conduct or might constitute a breach of this policy, you should refer the matter to your line manager.

The giving of business gifts to clients, customers, contractors, and suppliers is not prohibited provided the following requirements are met:

- The gift 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.
- It complies with local laws.
- It is given in the Company's name, not in the giver's personal name.
- It does not include cash or a cash equivalent (such as gift vouchers).
- It is of an appropriate and reasonable type and value and given at an appropriate time.
- It is given openly, not secretly.
- It is approved in advance by a Director of the Company.

Essentially, it is not acceptable to give, promise to give, or offer, a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given, or to accept a payment, gift or hospitality from a third party that you know or suspect is offered or provided with the expectation that it will obtain a business advantage for them.

For the avoidance of doubt, any payment or gift to a public official or other person to secure or accelerate the prompt or proper performance of a routine government procedure or process, otherwise known as a "facilitation payment", is also strictly prohibited. Facilitation payments are not commonly paid in the UK, but they are common in some other jurisdictions.

Responsibilities and reporting procedure

It is the contractual duty and responsibility of all employees and associated persons to take whatever reasonable steps are necessary to ensure compliance with this policy and to prevent, detect and report any suspected bribery or corruption in accordance with the procedure set out in the Company's Public Interest Disclosure Policy. You must immediately disclose to the Company any knowledge or suspicion you may have that you, or any other employee or associated person, has plans to offer, promise or give a bribe or to request, agree to receive or accept a bribe in connection with the business of the Company. For the avoidance of doubt, this includes reporting your own wrongdoing.

The duty to prevent, detect and report any incident of bribery and any potential risks rests not only with the Directors of the Company but applies equally to all employees and associated persons.

The Company encourages all employees and associated persons to be vigilant and to report any inappropriate or unlawful conduct, suspicions or concerns promptly and without undue delay so that investigation may proceed, and any action can be taken expeditiously. For example, if a client or potential client offers you something to gain a business advantage with the Company or indicates to you that a gift or payment is required to secure their business.

If you wish to report an instance or suspected instance of bribery, you should follow the steps set out in the Company's Public Interest Disclosure Policy. Confidentiality will be maintained during the investigation to the extent that this is practical and appropriate in the circumstances. The Company is committed to taking appropriate action against bribery or other unethical conduct. This could include either reporting the matter to an appropriate external government department, regulatory agency, or the police and/or taking internal disciplinary action against relevant employees and/or terminating contracts with associated persons.

The Company will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken. It is also committed to ensuring nobody suffers any detrimental treatment because of refusing to take part in bribery or corruption, or because of reporting in good faith their suspicion that an actual or potential bribery or corruption offence has taken place or may take place in the future.

All employees and associated persons must ensure that any contract or agreement entered into by them for or on behalf of the Company contains an appropriate clause aimed at ensuring that any third party to the contract is aware of and agrees to adhere to the contents of this policy and further, that the contract expressly sets out the consequences of non-compliance including, where appropriate, clear provision for terminating the contract in the event of non-compliance or the commission of any relevant bribery offence.

Record-keeping

All accounts, receipts, invoices and other documents and records relating to dealings with third parties must be prepared and maintained with strict accuracy and completeness. No accounts must be kept "off the record" to facilitate or conceal improper payments.

Sanctions for breach

Breach of any of the provisions of this policy will constitute a disciplinary offence and will be dealt with in accordance with the Company's disciplinary procedure. Depending on the gravity of the offence, it may be treated as gross misconduct and could render the employee liable to summary dismissal.

As far as associated persons are concerned, breach of this policy could lead to the suspension or termination of any relevant contract, sub-contract, or other agreement with the associated person.

Monitoring compliance

The Company has lead responsibility for ensuring compliance with this policy and will review its contents on a regular basis. They will be responsible for monitoring its effectiveness and will provide regular reports in this regard to the Directors of the Company who have overall responsibility for ensuring this policy complies with the Company's legal and ethical obligations.

Training

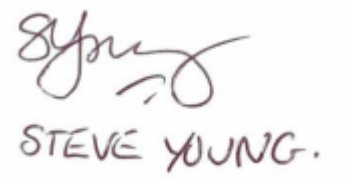
The Company will provide training to all employees to help them understand their duties and responsibilities under this policy.

The Company's zero tolerance approach to bribery will also be communicated to all business partners at the outset of the business relationship with them and as appropriate thereafter.

Examples of potential risks

The following is a non-exhaustive list of possible issues which may raise bribery concerns and which you should report in accordance with the reporting procedure set out above:

- A third party insists on receiving a commission or fee before committing to signing a contract with the Company or carrying out a government function or process for the Company.
- A third-party requests payment in cash or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made.
- A third party requests an unexpected additional commission or fee to facilitate a service.
- A third party demands lavish, extraordinary, or excessive gifts or hospitality before commencing or continuing contractual negotiations or provision of services.
- You are offered an unusually lavish, extraordinary, or excessive gift or hospitality by a third party.
- You receive an invoice from a third party that appears to be non-standard or extraordinary.
- The Company is invoiced for a commission or fee payment that appears large given the service stated to have been provided.



Managing Director
Date: 24th November 2023

Information Security & Cyber Policy HSP -006

1 Introduction

This document sets out Inner City Traffic Managements (ICTM) Information Security Policies and Procedures, and the responsibilities of everyone using ICTM systems and IT. Information security is of great importance, ensure compliance with legislation and demonstrate that the ICTM understands the process to recording, storing, processing, exchanging, and deleting information. Should this not be achieved ICTM can risk, breach of individual and commercial confidentiality and subsequent financial penalties from the regulator, the Information Commissioner.

There are three main principles to this policy:

- All staff must consider the sensitivity of the information they handle.

- All staff must protect information in proportion to its sensitivity by ensuring that information, whatever its format, is secured by physical means (such as locking paperwork away or appropriately archiving it when no longer current) or by using approved electronic means.
- Managers must ensure this policy is applied within their areas of work and should also lead by example.

This policy is mandatory. Any breach of the policy may result in disciplinary action being taken under ICTMs Disciplinary Procedure.

Any breaches of security (non-compliance with this Policy) must be reported to a director at ICTM or email admin@innercitytm.co.uk at the earliest opportunity. This is to safeguard ICTM and limit potential damage from information loss.

2 POLICY STATEMENT

It is the policy of ICTM to ensure that all information systems operated by the ICTM are secure and aspire to comply with the requirements of the Data Protection Act, the Computer
Misuse Act and (at the level of principles). It is also the aim of the ICTM that all staff must be fully aware of the need to maintain secure systems and fully understand their responsibilities as outlined in this document.

All staff are responsible for ensuring that they understand and abide by this policy. Failure to do so will be viewed as a serious matter and may result in disciplinary action.

It is the policy of the ICTM to ensure:

- Information is protected against unauthorised access.
- Confidentiality of information is maintained.
- Information is not disclosed to unauthorised persons through deliberate or negligent action. The integrity of information is maintained by protection from unauthorised modification.

- Information is available to authorised users when needed.
- Regulatory and legislative requirements are met.
- Contingency plans are produced and tested as far as is practicable to ensure business continuity is maintained.
- Information Security training is provided for all staff where relevant.
- All breaches of information security and suspected weaknesses are reported, investigated and appropriate action taken.
- Sharing of information with other organisations/agencies is permitted providing it is done within the remit of a formally agreed information sharing protocol.
- That there is a fair and consistent approach to the enforcement of standards of conduct expected from employees when using social media sites.

3 APPLICABILITY

All employees of the ICTM, contractual third parties and any agency staff used by ICTM with access to equipment and information (electronic and paper records) are responsible for ensuring the safety and security of the ICTMs equipment and the information that they use or manipulate.

Where services are provided to the ICTM by outside organisations then the contracting officer shall ensure that the provisions of this policy are known to and accepted by that organisation as part of the contract.

4 REQUIREMENTS

For the avoidance of doubt, the Information Security and the Acceptable Use of ICTM Policy requires that.

- Individuals must ensure that as far as is possible no unauthorised person has access to any information held by ICTM.

- Individuals must ensure that physical security measures are properly used.

- Individuals must not deliberately or negligently corrupt, damage or destroy data, software or hardware belonging to the ICTM. This includes the proliferation of viruses or other similar computer programmes.

- Individuals will be given access passwords to certain computer systems. These must not be disclosed. They should not be written down and they should be changed regularly.

- Individuals must not load or download software packages onto ICTM PC/PHONE or TABLETS and under no circumstances should games software be loaded on to these.

- Any staff found to be storing large numbers of personal files, especially large files such as photographs or videos may be asked to remove them or in some circumstances be the subject of disciplinary action.

- Any files received on any media, brought or sent into the ICTM or files received by electronic mail must be virus checked before being loaded onto any ICTM equipment.

5.1.1 Network Security

- Only ICTM owned Laptops, Phones or Tablets are allowed to be connected to the ICTMS WIFI (Computer) network. Permission must be granted by the directors if a visit requires access.

5.1.2 Physical Security

- Access to data held on the ICTMs information systems is minimised by restricting physical.
  access to the ICTMs office.

- Where information is kept in the offices, access to buildings is restricted by ensuring that security doors are closed properly and that entry codes are kept secure and changed regularly.

- Doors and windows must be always secured at lunch times and overnight and when the office is left unattended.

- Visitors to ICTM buildings must be always accompanied and signed in and out of the premises on arrival and departure.

5.1.3 Computer Security

5.2 Data Storage

- All staff must abide by the rules of the Data Protection Act and the Computer Misuse Act.

- Storage of data on PC or Laptop's C: drive is discouraged, and all users are requested not to store files on PC or Laptop's C:\drives because in the event of failure, all data stored on the C: drive would be lost as it not backed up.

- All information related to ICTM business is to be stored on ICTM Drop Box

5.3 File Storage and Naming Conventions

- All documents and files should be given clear and descriptive titles that will help others to understand what is contained within them. All documents should have a date and version number clearly included.

- Information which is no longer required (in line with the directorate's document retention schedule) should be promptly disposed of by deletion or destruction. Unless an audit record of versions is explicitly required previous versions of documents should be destroyed when the new version is created.

5.4 Screen Locking

- Computers must not be left unattended with screen unlocked when logged in.
- Whenever staff move away from a workstation, they must ensure that they have logged off or locked the workstation.
- When leaving a place of work staff must ensure they have logged off and closed the workstation correctly.

5.5 Memory Sticks and removable media

- Only ICTM supplied encrypted memory sticks are to be used.

5.6 Passwords

- Passwords given to you are for your use only.
- Passwords should not be written down or given to others to use under **any** circumstances.
- Passwords must be a minimum of 7 case sensitive characters[1] and should be a combination of upper/lower/numeric/special characters. Ideally Passwords should also contain random characters such as **#@?!$&** etc. Passwords must include at least three different character types, or they will not be accepted.
- Passwords must be changed every 90 days as a minimum.

5.7 Viruses

- All files received on disc from outside the ICTM or received via electronic mail must be checked for viruses before being used on ICTM equipment. You must not intentionally introduce/send or download files or attachments which contain viruses.
- If a virus is suspected, the directors must be informed immediately. The infected equipment should not be used until given permission from the ICTM. Any

disks, CD ROMS, and USB memory sticks that have been used on the suspected infected workstation should be gathered and not used.

5.8 Party Network Connections

- All requests for external 3rd Party network connections must be processed by the ICTM.

5.9 Document Handling

- All paper documents should be securely locked away when no longer required, by being placed in appropriate secure containers.
- The clear desk policy requires that all information protectively and shall be put away and locked when the desk is unattended.

5.10 Printing

Staff must ensure adequate care is taken when printing information.

5.11 Scanning

Staff must ensure adequate care is taken when scanning documents and using ICTMs secure scanning solution. Checking the destination file or email address.

5.11.1 Clear Desk

- All manual files and paper records must be closed in files away before leaving the office.
- Where possible information must be held securely in locked containers, lockers, drawers and filing cabinets to prevent unauthorised access.
- Any sensitive waste shall be shredded or placed in the appropriate confidential containers for secure disposal.

5.11.2 Mobile Workers and Home Workers

5.12 Laptops

- Care must be taken to avoid being overlooked whilst using equipment in any public area.

- Laptops must be kept in a secure location when not in use.
- Laptops must not be left unattended during the normal working day unless it is on ICTMs premises where there is good physical security at entrances to the building.
- When using portable equipment on the move, or outside of office hours, reasonable care should be taken to secure it.

5.13 Manual Files

- Manual files processed outside of the ICTMs property must be kept with the individual completing this work.
- When left unattended, Manual Files must be in a locked in the office and out of view.
- Computer equipment or manual files that are travelling with an employee must be locked in the boot of the car or always kept with the individual when travelling by public transport.
- Computer equipment or manual files must not be left unattended on a train or bus or left in a vehicle overnight.

5.14 Mobile Telephones, Tablets and Smart Phones

- Staff issued with mobile phones, Tablets, Smart Phones or other Personal Digital equipment are responsible for safekeeping and security.
- Security lock and pin protection must be used where available to protect the device and any stored data.
- Smart Phones devices must be protected with a password.
- Mobile devices are provided for work-related purposes only.

5.15 Lost or stolen mobile devices.

 If a mobile device is lost or stolen, staff must.

1) Contact a Director of ICTM to report the loss and ask for the mobile device to be suspended so that it can no longer be used.
2) Notify the local Police station of the loss.

Please note that replacement of lost or stolen handsets is not covered by any insurance so the relevant department will need to pay for the replacement.

5.16 Leaving ICTM or moving into another role

- Staff who are issued with Laptops, or any mobile devices must ensure their safe return on termination of employment or acceptance of a different post within the ICTM which does not require the use of those devices.

Use of the Internet

5.17 Downloading of Information Resources

- Individuals must not download non-work-related information from the Internet. To reduce the likelihood of a virus infection, individuals must take care to ensure that the files are from a trustworthy source.
- Individuals requiring any new software, including any plug-ins, must make a formal request to ICTM.
- Software must not be downloaded and/or installed onto ICTM equipment unless it has been approved by ICTM and can be validated that it is licensed for current use.
- Individuals are reminded that copyright laws apply to the Internet and care must be taken should there be a need to re-use any information (including images) in any ICTM.

5.18 4.6.2Uploading Data / Information to the Internet

Any users who are responsible for uploading data / information to the Internet must be sure that the information being uploaded is suitable to upload.

5.19 E-MAIL USE

E-Mail is a useful tool that enables individuals to organise themselves and communicate with others. This policy sets out the expectations for all ICTM computer equipment users who are provided with access to Outlook. Outlook is provided as a business tool and should not be used for non-work-related matters.

5.20 4.7.1 Sending email

- Individuals must use the default settings and not make changes to the disclaimer.

- E-mail is set up by default to conform with ICTM branding and house style, and a corporate disclaimer is applied to all outgoing messages.

- All e-mails must have the subject line completed and should be checked for accuracy of spelling, punctuation and grammar. Bold text should only be used sparingly, and for emphasis, and underlining should only be used for links. The use of upper-case text should be avoided as this may be interpreted by recipients as shouting.

- To avoid information overload, individuals should consider carefully who needs to be included in any e-mail and whether face-to-face or telephone contact could be an alternative method. When sending OFFICIAL-SENSITIVE or OFFICIAL e-mail, individuals should be mindful of any delegate permissions that recipients may have set up.

- Individuals must not alter the text of any received messages, including when forwarding them to others. Similarly, individuals should not assume that a forwarded message matches what was originally authored.

- Individuals must not use other people's mail accounts nor attempt to impersonate someone else or appear anonymous when sending e-mail.

- All emails should be finished with an email signature that includes your name, title, service and contact details.

Agreements by email

 Individuals must take care not to enter into any agreements via e-mail that could constitute a
contract, and if in doubt must seek the advice of ICTMs legal and procurement advisors.

Distribution lists

 Mail distribution lists are provided to enable business communications to be made to groups of individuals, and each list must have a designated owner. Lists should only be used for related business purposes, and any queries related to their use or composition should be directed to the list owner in the first instance.

5.21 Mailbox management

- Individuals are expected to treat their mailbox like an electronic in-tray, ensuring that it is regularly checked and that messages requiring further action are dealt with promptly – including sending holding responses where appropriate.

- Individuals should only archive and retain messages that need to be kept and these should be selected in line with business needs and any corporate

retention schedules that may exist. All other e-mail that does not constitute a necessary record of business should be deleted once it is no longer required.

5.22 Misuse of email

- Individuals must not send or forward any abusive, threatening, defamatory or obscene messages. Likewise, individuals should avoid sending messages in the heat of the moment, taking time to reflect on drafts and how they may be interpreted before sending them.
- Staff must take care with any suspected malicious or nuisance e-mails received (e.g., chain email, hoax and spam e-mails) and delete them.
- Individuals must never open attachments to an e-mail of unknown origin as they may contain viruses and other malware.

5.23 Mail and absence

- An "Out of Office" notice must be used whenever an individual is away from their normal office base, and messages should clearly indicate a date of return and contact details for those who can deal with issues whilst the individual is away.

5.24 Attachments

- Attachments should not be included in any internal mails or meeting invites, wherever it is possible links to documents should be used instead.

6 SECURITY INCIDENT REPORTING

- Information Security Incidents must be reported within two Business days of occurring in accordance with the ICTMs Security Incident Policy which classifies the type of security incident and ensures appropriate notification of relevant parties.
- Loss of **any** piece of ICTM equipment (computer, laptop, tablet, mobile phone, USB storage device, is classed as a security incident and must be reported.
- Information Security Incidents should be reported to a director or ICTM.

7 MANAGERS RESPONSIBILITIES

- The directors give their full backing to all the guidelines and procedures as set out and agreed in this document.

- Managers must also take responsibility to ensure:

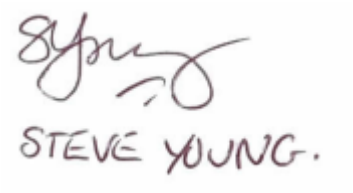
.

7.1 - Return of IT Equipment

- When an employee leaves ICTM, the directors must ensure all IT equipment is returned to the office.

- On the last working day, you must return any IT equipment and ensure it is returned to ICTM.

- Failure to comply with the requirements of this policy in relation to the return of ICTM equipment is regarded as a serious breach of this policy.



Managing Director
Date: 24th November 2023

Waste Management Policy HSP-007

1. Aims

Inner City Traffic Managements waste management policy is based on the following principles, which are in order or preference priority:

- *Reduction*
  Wherever possible reduce the purchase and use of single use items, examples include none-rechargeable batteries.

- *Re-use*
  Before discarding an item ensure that it is at the end of its useful life and that someone else cannot make use of it, examples include furniture & computers.

- *Recycling*
  Be aware of any Company initiatives; support them and encourage other suppliers to adopt good practice. Where practical, buy products made from recycled material in preference to first generation materials thereby helping to sustain a market.

- *Risk Minimisation*
  Minimise risks of immediate and future pollution or harm to human health.

2. Responsibilities

Inner City Traffic Management is committed to the protection of the environment through the implementation of an effective waste management programme that meets or exceeds all legislative and regulatory requirements placed on it.

All employees of Inner City Traffic Management have a personal responsibility for the way their conduct impacts on this policy and should take reasonable care to ensure that a responsible and approved disposal system is in place before undertaking any activity that results in the production of waste.

All employees of the Inner City Traffic Management should satisfy themselves that any disposal, for which they are responsible, is conducted in a manner approved by Inner City Traffic Management. Should there be any doubt contact should be made in the first instance with the directors who will either offer guidance or make the necessary introductions to ensure compliance.

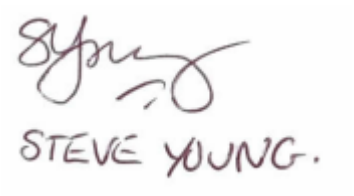
- *Office Waste*
  Prior to placing orders for waste removal or disposal, guidance should be sought from the directors regarding approved suppliers who have suitable environmental policies and practices in place.

  Responsibility for the disposal of general office waste, that is waste, which is a by-product of everyday office activities, rests with the Operations Director. The Operations Director is responsible for ensuring that the aims outlined above are known and achieved.

- *Confidential Waste*
  The disposal of confidential waste is the responsibility of the Operations Director and is to be undertaken in a manner approved by Inner City Traffic Management In disposing of confidential waste due reference should be made to the Data Protection Act and all required certificates must be obtained and retained. This responsibility cannot be delegated or passed to another department.

- *Chemical and Bio Waste*
  Written procedures for the purchase, use and proposed disposal of all hazardous chemicals, including by-products and waste materials should be drawn up as part of the obligatory COSHH assessment process.

- Under no circumstances should any hazardous substances be brought on to any Inner City Traffic Management site prior to the completion of a COSHH assessment.
- *Production Waste*
  The removal and disposal of waste resulting from Inner City Traffic Management is the responsibility of the Operations Director. This includes separating and segregating scrap waste, such as paper, steel, chemical products and general waste.



Managing Director Dated 24th November 2023

MODERN DAY SLAVERY ACT 2015 POLICY STATEMENT- HSP 08

Inner City Traffic Management recognises that slavery and human trafficking remains a hidden blight on our global society.

The aim of the Company is to identify our responsibility by alerting staff to the risks, however small, in our business and in the wider supply chain.

Staff are expected and encouraged to report concerns to management, where they are expected to act upon them.

We are committed to ensuring that there is no modern-day slavery or human trafficking in our supply chains or in any part of our business. Our Anti-slavery Policy Statement reflects our commitment to acting ethically and with integrity in all our business relationships and to implementing and enforcing effective systems and controls to ensure slavery and human trafficking is not taking place anywhere in our supply chains.

This Policy considers, and supports, the policies, procedures and requirements documented in our Management System, compliant with the requirements of ISO 9001.

The implementation and operation of this management system underlines our commitment to this policy statement. Formal procedures concerning slavery and human trafficking have been established, disciplinary procedures will be taken where they are breached.

The Company will achieve these aims by our initiative to identify and mitigate risk in the following.

Continually audit & review our practices for checking all employees are paid at least the minimum wage and have the right to work; • We encourage the reporting of concerns and the protection of whistle blowers. • The company will not knowingly support or deal with any business involved in slavery or human trafficking. • We have zero tolerance to slavery and human trafficking.

We expect all those in our supply chain and contractors comply with our values. To ensure a high level of understanding of the risks of modern slavery and human trafficking in our supply chains and our business, we provide training to relevant members of staff. All Directors have been briefed on the subject.

We use the following key performance indicators (KPIs) to measure how effective we have been to ensure that slavery and human trafficking is not taking place in any part of our business or supply chains: • Completion of Audits by Directors, Managers Safety managers and Safety Advisors.

This policy is in accordance with Section 54 of the Modern Slavery Act 2015 and constitutes our group's slavery and human trafficking statement. Modern Day Slavery Act 2015 Policy Statement For transparency the company will publish the Modern-Day Slavery & Trafficking Act 2015 Policy Statement on its website for the public, consumers, employees.

This policy applies to all those employed by Inner City Traffic Management Limited

Signed

Managing Director Dated 1st November 2023

Whistleblowing policy (confidential reporting) HSP-09

1. What is Whistleblowing?

In this policy ‘Whistleblowing’ means the reporting by employees of suspected misconduct, illegal acts, or failure to act within Inner City Traffic Management Ltd.
The aim of this Policy is to encourage employees and others who have serious concerns about any aspect of our work to come forward and voice those concerns.
Employees are often the first to realise that there may be something seriously wrong within the company. ‘Whistleblowing’ is viewed by ICTM as a positive act that can make a valuable contribution to the company’s efficiency and long-term success. It is not disloyal to colleagues or ICTM to speak up. ICTM is committed to achieving the highest possible standards of service and the highest possible ethical standards in public life and in all of its practices. To help achieve these standards it encourages freedom of speech.
If you are considering raising a concern, you should read this Policy first. It explains:

- the type of issues that can be raised
- how the person raising a concern will be protected from victimisation and harassment
- how to raise a concern, and
- what the ICTM will do

1.1 If you are unsure whether to use this Policy or want independent advice at any stage, you may contact the independent charity Public Concern at Work on 020 7404 6609. Their advisers can give you free confidential advice on how to raise a concern about serious malpractice at work.

2. What is the aim of the Policy and when does it apply?

3.1 Aims of the Policy

The Policy is designed to ensure that you can raise your concerns about wrongdoing or malpractice within ICTM without fear of victimisation, subsequent discrimination, disadvantage or dismissal.

It is also intended to encourage and enable you to raise serious concerns within ICTM rather than ignoring a problem or 'blowing the whistle' outside.

This Policy aims to:

- encourage you to feel confident in raising serious concerns at the earliest opportunity and to question and act upon concerns about practice
- provide avenues for you to raise those concerns and receive feedback on any action taken
- ensure that you receive a response to your concerns and that you are aware of how to pursue them if you are not satisfied
- reassure you that you will be protected from possible reprisals or victimisation if you have made any disclosure in good faith.

3.2. Scope of this Policy

This Policy is intended to enable those who become aware of wrongdoing in the company affecting some other person or service, to report their concerns at the earliest opportunity so that they can be properly investigated.

The Whistle Blowing Policy is not intended to replace existing procedures:

- If your concern relates to your own treatment as an employee, you should raise it under the existing grievance or harassment procedures
- If a client has a concern about services provided to him/her, it should be raised as a complaint to ICTM
- Complaints of misconduct by employees are dealt with under a separate procedure (for further information please contact Steve Young

3.3. Who can raise a concern under this Policy?

The Policy applies to all:

- employees of ICTM
- employees of contractors working for ICTM, for example, agency staff and drivers
- employees of suppliers
- those providing services under a contract or other agreement with ICTM in their own premises, and
- voluntary workers working with ICTM

3.4. What should be reported?

Any serious concerns that you have about service provision or the conduct of officers or members of ICTM or others acting on behalf of the ICTM that:

- make you feel uncomfortable in terms of known standards.
- are not in keeping with ICTM policies.
- fall below established standards of practice; or
- are improper behaviour.

These might relate to:

- conduct which is an offence or a breach of the law (a criminal offence has been committed or failing to comply with any other legal obligation)
- disclosures related to miscarriages of justice
- racial, sexual, disability or other discrimination
- health and safety of the public and/or other employees
- damage to the environment
- unauthorised use of public funds or other assets
- possible fraud and corruption
- neglect or abuse of clients, or
- other unethical conduct.

This list is not exhaustive.

4. Protecting the Whistleblower

4.1. Your legal rights

This policy has been written to take account of the Public Interest Disclosure Act 1998 which protects workers making disclosures about certain matters of concern, when those disclosures are made in accordance with the Act's provisions and in the public interest. The Act makes it unlawful for ICTM to dismiss anyone or allow them to be victimised on the basis that they have made an appropriate lawful disclosure in accordance with the Act. Rarely, a case might arise where it is the employee that has participated in the action causing concern. In such a case it is in the employee's interest to come into the open as

soon as possible. ICTM cannot promise not to act against such an employee, but the fact that they came forward may be considered.

4.2. Harassment or Victimisation

ICTM is committed to good practice and high standards and to being supportive of you as an employee.

ICTM recognises that the decision to report a concern can be a difficult one to make. If you honestly and reasonably believe what you are saying is true, you should have nothing to fear because you will be doing your duty to your employer, your colleagues and those for whom you are providing a service.

ICTM will not tolerate any harassment or victimisation of a whistleblower (including informal pressures) and will take appropriate action to protect you when you raise a concern in good faith and will treat this as a serious disciplinary offence which will be dealt with under the disciplinary rules and procedure.

4.3. Support to you

Throughout this process:
- you will be given full support from senior management
- your concerns will be taken seriously, and
- ICTM will do all it can to help you throughout the investigation

If appropriate, ICTM will consider temporarily re-deploying you for the period of the investigation.

For those who are not ICTM employees, we will endeavour to provide appropriate advice and support wherever possible.

4.4. Confidentiality

All concerns will be treated in confidence and every effort will be made not to reveal your identity if that is your wish. If disciplinary or other proceedings follow the investigation, it may not be possible to act as a result of your disclosure without your help, so you may be asked to come forward as a witness. If you agree to this, you will be offered advice and support.

4.5. Anonymous Allegations

This Policy encourages you to put your name to your allegation whenever possible. If you do not tell us who you are it will be much more difficult for us to protect your position or to give you feedback. This policy is not ideally suited to concerns raised anonymously.
Concerns expressed anonymously are much less powerful, but they may be considered at the discretion of ICTM. In exercising this discretion, the factors to be considered would include:

- the seriousness of the issue raised
- the credibility of the concern, and
- the likelihood of confirming the allegation from other sources

4.6. Untrue Allegations

If you make an allegation in good faith and reasonably believing it to be true, but it is not confirmed by the investigation, we will recognise your concern and you have nothing to fear.

If however, you make an allegation frivolously, maliciously or for personal gain, appropriate action that could include disciplinary action, may be taken.

5. Raising a Concern

5.1. Who should you raise your concern with?

This will depend on the seriousness and sensitivity of the issues involved and who is suspected of the wrongdoing. You should normally raise concerns with:

- Steve Young (MD)

The address for correspondence is The Beeches, Galley Hill, Waltham Abbey, EN9 2AJ
If, exceptionally, the concern is about the Directors your concern should still be raised with Steve Young who will decide how the investigation will proceed. This may include external investigation.

If you are unsure who to contact, you may call the independent charity Public Concern at Work on 0207 404 6609 for advice.

5.2. How to raise a concern

You may raise your concern by telephone, in person or in writing. The earlier you express your concern, the easier it is to act. You will need to provide the following information:

- the nature of your concern and why you believe it to be true
- the background and history of the concern (giving relevant dates)

Although you are not expected to prove beyond doubt the truth of your suspicion, you will need to demonstrate to the person contacted that you have a genuine concern relating to suspected wrongdoing or malpractice within ICTM and there are reasonable grounds for your concern.

You may wish to consider discussing your concern with a colleague first and you may find it easier to raise the matter if there are two (or more) of you who have had the same experience or concerns.

You may invite your trade union, professional association representative or a friend to be present for support during any meetings or interviews in connection with the concerns you have raised.

6. What the ICTM will do

ICTM will respond to your concerns as quickly as possible. Do not forget that testing your concerns is not the same as either accepting or rejecting them.
The overriding principle for ICTM will be the public interest. To be fair to all employees, including those who may be wrongly or mistakenly accused, initial enquiries will be made to decide whether an investigation is appropriate and, if so, what form it should take.

The investigation may need to be carried out under terms of strict confidentiality, i.e., by not informing the subject of the complaint until (or if) it becomes necessary to do so. In certain cases, however, such as allegations of ill treatment of others, suspension from work may have to be considered immediately. Protection of others is paramount in all cases.
Where appropriate, the matters raised may:

- be investigated by management, internal audit, or through the disciplinary/grievance process
- be referred to the police
- be referred to the external auditor
- be referred and put through established child protection/abuse procedures
- form the subject of an independent inquiry

Within ten working days of a concern being raised, the person investigating your concern will write to you:

- acknowledging that the concern has been received
- indicating how ICTM proposes to deal with the matter
- supplying you with information on staff support mechanisms
- telling you whether further investigations will take place and if not, why not.

The amount of contact between you and the officers considering the issues will depend on the nature of the matters raised, the potential difficulties involved and the clarity of your information. It is likely that you will be interviewed to ensure that your disclosure is fully understood.

Any meeting can be arranged away from your workplace, if you wish, and a union or professional association representative or a friend may accompany you in support.
ICTM will do what it can to minimise any difficulties that you may experience because of raising a concern. For instance, if you are asked to give evidence in criminal or disciplinary proceedings, we will arrange for you to receive appropriate advice and support.

You need to be assured that your disclosure has been properly addressed. Unless there are any legal reasons why this cannot be done, you will be kept informed of the progress and outcome of any investigation.

7. The Managing Director

The Managing Director has overall responsibility for the maintenance and operation of this Policy.

8. How the Matter can be Taken Further

This Policy is intended to provide you with an avenue within ICTM to raise concerns. We hope you will be satisfied with any action taken. If you are not, and you feel it is right to take the matter outside the company, the following are the ICTM's prescribed contacts:

- the External Auditor:
  Tony Crawley
  Statutory Auditor
  KPMG LLP
  St Nicholas House
  Park Row
  Nottingham
  NG1 6FQ
- your trade union
- the police
- other relevant bodies prescribed by legislation or Public Concern at Work will be able to advise you who you can contact

If you raise concerns outside of ICTM you should ensure that it is to one of these prescribed contacts. A public disclosure to anyone else could take you outside the protection of the Public Interest Disclosure Act and of this Policy.

You should not disclose information that is confidential to ICTM or to anyone else, such as a client or contractor of ICTM, except to those included in the list of prescribed contacts.
T
his Policy does not prevent you from taking your own legal advice.

9. Review of the Policy
The Directors will review this Policy annually.

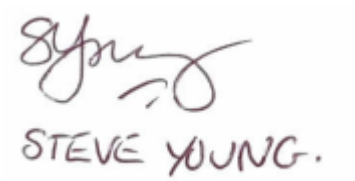
10. Corporate Recording and Monitoring

The Managing Director will maintain a corporate register containing all concerns that are brought to his attention. All persons allocated to investigate a concern must ensure the Managing Director is provided with sufficient details for the corporate register.

The Managing Director will review the corporate register and produce an annual report for Management Review. The report will include a summary of the concerns raised, to which department they related, the post to which the concerns related (if not confidential) and any lessons learned. The report will not include any employee names. The aim of this is to ensure that:

- ICTM and/or the relevant department learns from mistakes and does not repeat them, and
- consistency of approach across the departments

The corporate register together with the annual reports will be available for inspection by internal and external audit, after removing any confidential details.



Managing Director
Date: 24th November 2023 v3

CDM Policy HSP- 010

Inner City Traffic Management Ltd (hereon ICTM) is committed to creating safe and healthy working environments and to the implementation of good Health & Safety practice in the design, implementation and delivery of all projects falling within the scope of CDM.

ICTM will ensure that compliance with the requirements of CDM Regulations and associated Approved Code of Practice as a minimum and where possible, exceed those requirements in its duties as Designer and Principal Contractor.

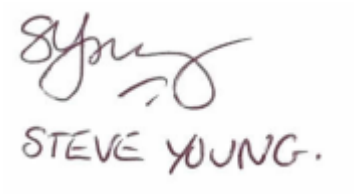
ICTM will ensure that all employees involved with the design and implementation of projects are trained in all aspects of the CDM Regulations appropriate to the nature of our work and, where necessary, specific training will also be provided relevant to a specific duty to ensure that employees have the experience and understanding necessary to ensure that their duties are carried out in a competent manner.

ICTM will ensure that all subcontractors and specialist consultants either directly employed or referred by a third party have been assessed to ensure that they have sufficient training, resources, and experience to demonstrate competency under the CDM Regulations prior to appointment.

When engaged as a Designer under the CDM Regulations, ICTM will review designs with the project team to ensure that design risks are identified and addressed in the most appropriate manner to avoid or reduce risks to Health & Safety at source.

Our staff will work with the project team to improve project safety and the Directors will take responsibility for co-ordinating and co-operating with the Project Team and CDM Co-ordinator.

The Managing Director is responsible for ICTM compliance with the CDM Regulations. However, all staff have responsibility for the implementation of this policy and ensure that Health & Safety is at the forefront of ICTM philosophy at all stages of a project.



Managing Director
Date: 24th November 2023

DATA PROTECTION POLICY HSP-011

Table of contents

1. Introduction

GDPR (General Data Protection Regulation) is one of the regulations affecting the way that organizations carry out their information-processing activities. It is the regulation that is designed to protect the personal data of European Union citizens. Fines are applicable for any form of breaching GDPR's rules and regulations. Hence, ICTM should ensure compliance with GDPR by establishing a Data Protection Policy (DPP).

2. Purpose

The purpose of this document is to describe ICTM's responsibilities regarding the protection of personal data.

3. Principles of Processing Personal Data

GDPR is based under several fundamental principles, such as:

a) Personal data should be processed with fairness, lawfulness, and transparency toward the data subject
b) Personal data should be collected for specified and legitimate purposes
c) Personal data should be accurate and kept up to date
d) Inaccurate personal data should be erased or rectified without delay
e) Personal data should be processed and secured against any unlawful or unauthorized processing

ICTM shall ensure compliance with all of the abovementioned principles.

3.1 Rights of the Data Subject

The rights of the data subject under the GDPR are:

a) The right of being informed
b) The right to access
c) The right to rectification
d) The right to erasure

e) The right to restrict processing
f) The right to data portability
g) The rights related to automated decision-making and profiling
h) The right to object

Data subject rights are supported by appropriate procedures within ICTM that allow the required action to be taken within the timescales stated under the GDPR.

The timescales for data subject requests are shown in the table below.

Data Subject Request
Time scale

The right of being informed.
Within one month (if the data is not supplied by the data subject)

The right of access
One month

The right to rectification
One month

The right to erasure
Without undue delay

The right to restrict processing.
Without undue delay

The right to data portability
One month

The rights related to automated decision-making and profiling.
Not specified

The right to object
On receipt of objection

3.2 Lawfulness of Processing

ICTM ’s policy specifies the appropriate actions that should be taken for documenting and processing a specific case of personal data. However, GDPR provides six alternative ways that can be used by ICTM, depending on the case.

Consent: Except in specific reasons that are stated as allowable under GDPR, ICTM should obtain consent from the data subject, prior to collecting and processing their data. For example, any case that involves children below the age 16 requires parental consent.

Contract performance: Explicit consent will not be required in cases where the collected and processed data are required for contract fulfilment, like cases when the contract cannot be finalized without the personal data. For example, if an address is missing in the delivery of a package, the delivery cannot be completed.

Legal obligation: Explicit consent will not be required in cases when the collected and processed data are required to comply with law. Taxation and employment can be examples of such cases.

Data subject's fundamental interests: A certain amount of data processing can be lawful under certain conditions (especially in the public sector), like cases when the data is needed to protect the subject's main interests or social care.

Carrying out tasks of public interest: The data subject's consent is not requested in cases where ICTM needs to perform a specific task that is of public interest.

Legitimate interests: Data processing is considered lawful in cases when the processing of personal data does not significantly affect the rights and freedoms of the data subject.

However, the taking of such actions should be justified properly and documented.

3.3 Data Protection by Design

ICTM should adopt the principle of data protection by design and ensure that the systems collecting personal data consider privacy issues. The systems should also successfully complete one or more data protection impact assessment.

The data protection impact assessment (DPIA) includes the following:

- Determine the purpose of processing the personal data
- Determine whether the processing of personal data is necessary
- Identify the necessary controls to address the risks and comply with the legislation

To respect personal data privacy and comply with GDPR, ICTM can use techniques, such as data minimization and pseudonymisation.

3.4 Processing Personal Data Contracts

Based on the requirements of GDPR, ICTM should ensure that all the personal data used are subject to a contract, i.e., the GDPR Controller-Processor Agreement Policy.

3.5 International Transfers of Personal Data

Before transferring any personal data outside of Europe, ICTM reviews and ensures that they are following GDPR regulations.

Therefore, to regulate the intra-group international data transfers, the Binding Corporate Rules (BCR) provide enforceable rights for data subjects.

3.6 Breach Notification

In any case related to breaches of personal data, ICTM is responsible for considering actions that should be taken and inform the affected parties.
In accordance with GDPR, if a breach of personal data occurs, the relevant authority should be informed within 72 hours. These cases should be managed based on the Information Security Incident Response Procedure, which provides the process of handling information security incidents.

Annex A (Data Protection Policy)
Summary of the policy

The data protection policy ensures an adequate level of security in terms of confidentiality, availability, and integrity of information assets and personal data of ICTM against all threats we could face. The organisation establishes, implements, operates, monitors, reviews, maintains, and improves processes and controls related to data processing and information security based on a risk approach.

Introduction ICTM ensures respect for the integrity, confidentiality, and availability of information generated within the processing of personal data.
ICTM shall ensure the protection of their information assets against internal, external, accidental, or deliberate threats.

Objectives Ensure continuity of critical business activities.
Ensure that all information processed, stored, traded, and released by ICTM has complete integrity.

Ensure that all information relevant to ICTM will be monitored and stored according to procedures for maintaining appropriate confidentiality.
Provide choice of appropriate and proportionate security controls to protect the assets and maintain interested parties' faith.

Principles ICTM shall establish, implement, operate, monitor, review, maintain, and improve their data protection and privacy framework based on a documented approach to risk activity and compliance with all of GDPR's requirements.

ICTM will take into account all legal, regulatory, and contractual requirements with regards to the processing of personal data in order to avoid breaching its legal statutory, regulatory, or contractual obligations, as well as its security requirements.

ICTM will establish and implement a risk management program documented in accordance with GDPR's requirements.

The criteria for evaluation and acceptance of risk must be established, formalized, and approved by the management.

The data protection policy has been approved by management and is subject to an annual review.

Responsibilities

The management has the responsibility to ensure that objectives and plans for compliance with GDPR are established and reviewed annually during the management review, the roles and responsibilities for the processing of the personal data and information security are defined, a security awareness program is implemented, an internal audit is conducted at least once a year, and the necessary resources to maintain and improve its compliance are provided.

The Director responsible for information security/data protection has the authority to intervene in all aspects of information security at ICTM. The Director of information security/data decides, in general, all the requirements for the effective compliance to GDPR by means of administrative directives, previously submitted to senior management.

Each executive has a responsibility to ensure that persons working under their control will protect information in accordance with ICTM's policies.

ICTM users (management, employees, contractors, and third party users) should be aware of the risks to information security and processing of personal data, their responsibilities, and the need to respect the policies and to ensure adequate protection of information.

Expected results

Appropriate and proportionate controls will be implemented to protect assets and give confidence to interested parties.

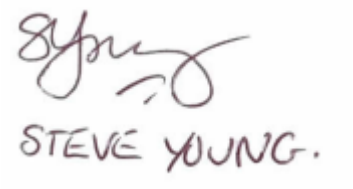
Decisions on matters of data protection will be based on an evaluation of risks faced by ICTM.

The legal, regulatory, and contractual requirements for ICTM will be met.

Related policies

Data protection policy
Human Resource Management policy
The policy on the personnel's training and skills development

Policy Approved By



Signed
Steve Young (MD) 24/11/2023

Tax Evasion Policy HSP – 012

Who must comply with the policy?

Our tax evasion policy applies to anyone working with us or anyone acting on our behalf, including all employees, directors, officers, agency workers, contractors, and external consultants.

Who is responsible for the policy?

The board of directors is responsible for ensuring the policy complies with all our

obligations, and that all others comply with the policy and are responsible for implementing the policy, monitoring its use and dealing with any queries.

The appointed company, Alywns LLP accountant are responsible for auditing related internal control systems and procedures. Finally, management at all levels are responsible for ensuring those reporting to them are fully aware and understanding of the policy.

What are tax evasion and facilitation of tax evasion?

Tax evasion means acting to cheat the public revenue or fraudulently evading UK tax,

with deliberate action or dishonest intent. It is a criminal offence.

Tax evasion facilitation means being knowingly involved in, or taking steps towards, the

fraudulent evasion of tax by another person. It also includes aiding, abetting, counselling.

or procuring the commission of that offence. When done deliberately and dishonestly, it

is a criminal offence.

Tax evasion is not the same as tax avoidance. Tax evasion involves deliberate and

dishonest conduct, while tax avoidance and involves taking steps to minimise tax payable

in line with current law and regulations

Prevention of Tax Evasion

Company accounts are submitted to company's house in a timely manner.

Managing director overseas all financial transactions and are recorded on Xero software.

All payments are only paid to a UK bank Account.

All bank accounts must reflect the name of the worker / invoice.

A payment cannot be made to person working for us or a third party has asked for payment to be made to a different person than the business providing the services, or to a bank account in a foreign country where the third party resides or conducts business.

No Cash payments are paid or received.

Bacs is the only transfer of money allowed.

No invoices can be amended to change the description of services in a way that may obscure the nature of original services provided.

You MUST:

Ensure you read, understand, and comply with this policy.

Avoid any activity that might lead to a breach of this policy.

Notify your line manager or the confidential Whistleblowing helpline as soon as possible if you suspect a conflict with the policy as occurred or might occur in the future.

What happens if the policy is breached?

If you breach the policy you'll face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

If any individuals or organisations working on our behalf breach the policy, we may terminate our contract with them.

Managing Director 24th November 2023

RIGHT TO WORK IN THE UK POLICY – HSP 013

This Document is for the use of Inner City Traffic Management Ltd Employees and their advisors only.

To comply with legislation, all employees must be eligible to work in the UK and as an employer we have a duty to carry out checks on all existing and potential employees. Managers have the responsibility for completing the check when recruiting a new member of staff.

An Immigration Officer can make a visit to ICTM at any time to make document checks to ensure that our employees legally have the right to work. You can be sent to jail for 5 years and pay an unlimited fine if you're found guilty of employing someone who you knew or had 'reasonable cause to believe' didn't have the right to work in the UK. This includes, for example, if you had any reason to believe that:

- they didn't have permission to enter or remain in the UK
- their permission had expired.
- they weren't allowed to do certain types of work or there is a cap on the total hours they can work.
- their papers were incorrect or false You can also be penalised if you employ someone who doesn't have the right to work and you didn't do the correct checks, or you didn't do them properly. Process You should check the eligibility to work in the UK of all prospective employees at interview stage, and then ask the successful candidate to bring both the original documents and copies of them with them on their first day. If they are unable to provide the required documentation for whatever reason, the offer of employment should not be made.

If the offer of employment proceeds without the required documentation in place this may lead to disciplinary action against the recruiting manager.

The Home Office provide a 'Right to Work Checklist'. A copy is shown at the end of this policy, for information. You must go through this 3-step checklist with all new starters. This should not take longer than a couple of minutes to complete unless they are not a citizen of the UK.

You must complete the form by ticking the corresponding box for:

(1) the document/s received
2) the checks you have completed, and
3) what copies were made, additionally to note if a follow up is required.

Step 1: Obtain Acceptable documents – page 1 (red section)

• The documents that may be accepted to establish a right to work are detailed in two lists – List A and List B.

You must obtain the document(s), specified in one of these lists.
You only need to tick one box to satisfy the right to work in either list.

- List A contains the range of documents which you may accept for a person who has a permanent right to work in the UK and no further checks are required.
– List B contains a range of documents which may be accepted for a person who has a temporary right to work in the UK, a follow-up checks on these documents will be required.

Responsibility for monitoring this lies with both the Directors. The most common documents received are from List A and are:

• Number 1 - which is a UK passport, and
• Number 8 - which is a full (not abbreviated) Birth Certificate (including parents/adoptive parent names) along with a separate official document detailing the National Insurance Number of the individual.

A Driving license does not provide evidence of Right to Work and should not be accepted. If you receive any other documents or have any questions on the documents, you receive please contact the People and Performance Administrator on 0131 335 4529 for further guidance.

Step 2: Check the Documents (top of page 2 – green section)

• When you are checking the validity of the documents, you must ensure that you do this in the presence of the holder. The responsibility for checking the document is yours.
• If you are given a false document, you will only be liable for a civil penalty if it is reasonably apparent that it is false.
• If someone gives you a false document or a genuine document that does not belong to them then this must be reported to your People and Performance consultant.
• For students who have limited permission to work during term-times, you must also obtain, copy and retain details of their academic term and holiday times covering the duration of their period of study in the UK for which they will be employed.

Step 3: Copy (middle of page 2 – purple section)

• We must retain a record of every document you have checked. This can be a hardcopy or a scanned and unalterable copy. Typically, this will be a photocopy however you can use a digital picture of the document providing this is in high resolution, ensuring the information and images are clearly visible.
• For ease of use, you can ask the applicant if they would capture a picture of their documentation should they have a camera phone, providing it meets the criteria above, and email this to the recruitment team at recruitment@Scotmid.co.uk. You will need to contact

the recruitment team to identify the individual who will then email a copy back to the store that you can then print off. Due to Data Protection please do not take pictures of anyone else's documents using your own mobile phone.

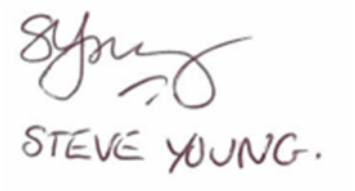
- Copies will be kept securely for the duration of the person's employment and for a further three years after they stop working for us.

- You must also make a record of the date on which you conducted your check. Simply inserting a date onto the copy is not enough. You must also record the fact that this is the date on which you conducted the check of documents. This can be done by making a dated declaration on the document copy as follows: 'I certify that this is a true copy of the original, the date on which this right to work check was made: [insert date]'.

- For ease, a template is available which includes a place for the document and the declaration wording. All you need to do is place the document in the relevant section and ask the applicant to take a picture or alternatively take a photocopy, is complete the declaration.

The completed checklist and dated copies of the documents should then be sent to the Directors along with the application form and Induction paperwork. If you are ever in any doubt about these procedures, please contact your People and Performance Consultant who will be happy to talk you through what documents are required.

Government Checklist Attached.



Managing Director 24th November 2023