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whatever its format, is secured by physical means (such as locking paperwork away or appropriately archiving it when no longer current) or by using approved electronic means.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:

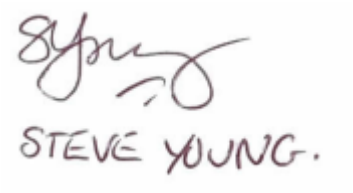
.

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