Data Protection & GDPR Policy

1. Data Protection

In order to operate effectively and fulfil its legal obligations, CSTM Services Ltd needs to collect, maintain and use certain personal information about current, past and prospective employees and other individuals with whom it has dealings. All such personal information, whether held on computer, paper or other media, will be obtained, handled, processed, transported and stored lawfully and correctly, in accordance with the safeguards contained in the Data Protection Act 2018 (DPA)- including GDPR.

2. Data Protection Principles

All personal data must be processed in accordance with the eight Data Protection Principles. The essence of these principles is set out below together with brief, non-exhaustive practical examples of when these principles may have relevance to you.

Personal data must:

- Be processed fairly and lawfully;
- Be obtained only for one or more specified or lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- Be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- Be accurate and, where necessary, kept up-to-date;
- Staff must notify changes of name, address, telephone number, bank and marital status to the HR Department soon as possible. The HR Department will endeavour, periodically, to ask staff to confirm that such personal data held by the Company is accurate. Staff should advise the Company of any changes to their contact details or to any other details that may be of relevance.
- Not be kept for longer than is necessary
- Be processed in accordance with the rights of data subjects.
    - For example, employees have a right of access to the information that the Company holds about them. Upon receipt of a written or email subject access request the Company shall disclose all the information that it is required to do so by law.
    - If any member of staff receives any letter from a customer, business contact, other employee, or any other third party requesting any information about them then they must pass the letter to the Data Protection Officer.
    - Employees should, if they are making a subject access request of the Company, send their access request to the Director.
    - Access to personal data must be restricted to authorised individuals for approved purposes

- Be protected by appropriate technical and organisational measures against unauthorised or unlawful processing, against accidental loss or damage.
    - The Company may take steps to put in place technical methods (i.e. firewalls, encryption, password protection, etc.) or organisational methods (hierarchy of access to personnel files, locking cabinets etc.) of protecting personal data where the importance of the personal data makes this appropriate.
    - All employees who have access to personal data controlled by the Company whether or not on computer, and whether in the office or at home or elsewhere, must take adequate precautions to ensure confidentiality so that neither the Company, nor any individual employed by the Company, becomes exposed to criminal or civil liability as a result of the loss, destruction or disclosure of personal data. All individuals must fully comply with all Company procedures and requirements in this regard.

- Staff should ensure the security of data at all times. Staff must not leave personal data on screen or on desk tops when they are not at their desks. Paper records should be stored securely unless under active consideration. A clear desk policy should be observed.

- Not be transferred to a country or territory outside the European Economic Area unless there is a clear legal basis in the Act for making the transfer.

3. Data Processing

Personal data provided by or about an individual to the Company will be processed in accordance with the Act. Data about an individual will only be processed for lawful and fair purposes. The Company is the legal person who determines the manner in which and the purposes for which personal data may be used. The Data Protection Officer who has the main responsibility internally for managing data protection issues and compliance in the Company is the Director. Personal data about an individual will be processed for various purposes which may include:

- to assess his/her application to become an employee;
- To administer the contractual sick pay system;
- To address any health and safety issues;
- To facilitate management decisions;
- To detect fraud;
- To administer any personal health insurance benefit or other similar benefit;
- To administer the employment relationship so that the Company may properly carry out its duties, rights and obligations to the employee. Such processing will principally be for HR, administrative, regulatory or payroll purposes.

4. Sensitive Personal Data

Certain personal data is given special status in data protection legislation. This personal data is called sensitive personal data. Sensitive personal data is personal data consisting of information as to:

- Racial or ethnic origin.
- Political opinions.
- Religious beliefs (or other beliefs of a similar nature).
- Trade union membership
- Physical or mental health
- Sex life
- Commission or the alleged commission of an offence.
- Proceedings for any offence, the disposal of such proceedings or the sentence of any Court in such proceedings.

Subject to the exceptions set out below and elsewhere in this procedure, sensitive personal data shall generally only be processed after the employee has given express consent. The Company may in certain situations process the data without your consent if it is necessary for processing taking place for one of the following purposes:

- Ensuring health and safety of employees;
- Ensuring a safe working environment;
- Maintaining records of statutory sick pay or maternity pay;
- Protecting the person and property of people entering on to the company premises or customer site;
- Carrying out any other obligation or enforcing any right under employment law;
- Participating in legal proceedings or obtaining legal advice.
- For the administration of justice.
- For medical purposes by a health professional.

Sensitive personal data relating to racial or ethnic origin may be processed without express consent in order to CSTM Services Ltd the effectiveness of the Company's Race Equality Policy and Procedure. The Company may also process such sensitive personal data about you without your explicit consent where it is otherwise entitled to do so by virtue of a condition under Schedule 3 to the Act.

5. Requests for Information

Employees about whom the Company holds personal data has the right to be:

- Told whether their personal data is being processed by or on behalf of the Company and, if so, to be given a description of:
  - The personal data held;
  - The purposes for which it is being processed and;
  - The recipients of the personal data

- Given a copy of the personal data in an intelligible format (unless to do so is disproportionate or the person has agreed to an alternative way of providing access)
- Given any information available regarding the source of the personal data

For any subject access request. Written requests should be directed to the Director. If you are a member of staff and you receive a written request, then you should forward this to the Director immediately. The request for information will be dealt with promptly and in any event within 30 days from the Company receiving:

- The written request for the personal data;
- Sufficient details to allow the Company to respond to it;
- Sufficient details to confirm the identity of the person making the request; and

Where the provision of information would reveal the identity of a third party, the information may not be provided unless either the consent of that third party is obtained or it is reasonable to proceed without their consent. All requests for access to personal data must be made in writing (which includes e-mails). You should be aware that where access requests are made via e-mail and the Company need not respond until it is satisfied as to the identity of the individual making the request. Personal information relating to employees cannot normally be disclosed to an unauthorised third party. These include family members (see Para 25 below), friends, local authorities, government bodies and the police. There are only certain circumstances when personal information can be given to such third parties and these include:

- Prevention or detection of a crime
- Apprehension or prosecution of offenders
- Prevention of serious harm to a third party
- Protection of the vital interests of the data subject, e.g. release of medical data where failure could result in serious harm or death
- Ensuring health and safety.

Employees have the right to expect documentary evidence to support such requests.

6. Management of Personal Data

Where we take any decision which significantly affects any member of staff exclusively upon the results of an analysis of his/her personal data carried out by automated means then we will provide that person with notice of this fact as soon as reasonably practicable thereafter. If the decision is connected with a contract entered into between the Company and another person or is taken for the purposes of considering whether to enter into or with a view to entering into such a contract, the other person will be allowed to make representations on the outcome of that decision (perhaps as part of a formal grievance procedure).

In the event of a potential intended or actual transfer of a business, the Company will take all reasonable steps to limit disclosure of personal data about employees to any of the third parties concerned by for instance, the omission of names or other identifying particulars. However, staff should be aware that some personal data such as name, address, position, salary levels may be transferred to a prospective operator (or other similar party) of any part of Company operations as part of a due diligence process. Where this happens, the Company will place contractual obligations on the prospective operator to keep the staff's information safe. The transferee shall cease to be a third party on the date of the formal transfer, except in respect of the personal data concerning certain rights and obligations such as those relating to pensions – not required under the Transfer of Undertakings (Protection of Employment) Regulations 2003 as amended by the Trade Union Reform and Employment Rights Act 1996.

7. Responsibilities

We expect all employees to use computers, email and the Internet responsibly and in accordance with the data protection principles. You should make yourself aware of the provisions contained in the Company's IT Policy. Employees are expected to adhere to this procedure and to ensure that those for whom they are responsible both adhere to this policy and protect computer systems and personal data from security risks. Where necessary, managers should seek advice from the IT Department to assist in these goals.

Employees must become familiar with the aims of this procedure and follow the guidelines set out. In particular Employees should:

- Seek advice from the Director where they have an doubts as to whether or not the processing of personal data that they require to carry out in the course of their employment complies with the Act;
- Not use personal information that they hold in the course of their employment for any reason other than the performance of their employment duties. To procure personal information from the Company and use it without its consent is likely to constitute a criminal offence under the Act;
- Provide all assistance to the Director in the conduct of any audit or preparing a response to a subject access request;
- Keep information that you process for the Company safe and secure in accordance with any procedures issued by the Company. Where no procedures are set out explicitly, you should exercise a degree of care over the personal data that you process by considering the harm that may result were the information to be disclosed unintentionally. Guidance on appropriate levels of security can be obtained from the Director.
- Not keep duplicate records relating to Employees or students for the purposes of our employment where a centralised filing option is available. Keeping your own records unnecessarily can complicate the process of responding to subject access requests.
- Notify the Director immediately should you detect any potential or actual breach of the Act.

8. Security

Any breaches of this Procedure in relation to personal data security will result in disciplinary action and, in serious cases, may result in the dismissal of an employee of the Company.

Employees will be authorised to gain access to certain computer systems, programs and data. No employee must attempt, alone or with others, to gain access to data or programs to which they have not been authorised to gain access. Employees must not disclose personal details of other Employees to unauthorised third parties where this information is personal data in respect of which the Company is the data controller.

9. Training

Employees will receive training on the importance of Data Protection during their induction training, and further reminders will be given during the monthly supervisor visits. This policy will be used to CSTM Services Ltd the employee's awareness of the Data Protection Act, so further training needs can be identified.

Signature	Position	Date