GDPR POLICY

GDPR Policy

One Creative Environments Ltd. ('the Company') is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR) and all other data protection legislation currently in force. The Regulation applies to anyone processing personal data and sets out the principles to be followed and gives rights to those whose data is being processed.

To this end, the Company endorses fully and adheres to the Data Protection Principles listed below. When processing data we will ensure that it is:

- processed lawfully, fairly and in a transparent way ('lawfulness, fairness and transparency');
- processed no further than the legitimate purposes for which that data was collected ('purpose limitation');
- limited to what is necessary in relation to the purpose ('data minimisation');
- accurate and kept up to date ('accuracy');
- kept in a form which permits identification of the data subject for no longer than is necessary ('storage limitation');
- processed in a manner that ensures security of that personal data ('integrity and confidentiality'); and
- processed by a controller who can demonstrate compliance with the principles ('accountability').

These rights must be observed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the Company will:

- observe fully the conditions regarding having a lawful basis to process personal information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information only to the extent that is necessary to fulfil operational needs or comply with any legal requirements;
- ensure the information held is accurate and up to date;
- ensure that the information is held for no longer than is necessary;
- ensure that the rights of people about whom the information is held can be fully exercised under the GDPR (i.e. the right to be informed that processing is being undertaken, to access personal information on request; to prevent processing in certain circumstances and to correct, rectify, block or erase information that is regarded as incorrect information);
- take appropriate technical and organisational security measures to safeguard personal information; and
- ensure that personal information is not transferred outside the EU, to other countries or international organisations without an adequate level of protection.

Personal Information of Employees

Throughout employment and for as long as is necessary following termination of employment, the Company will need to process data about you. Data likely to be processed by the Company includes:

- any references obtained during recruitment;
- details of terms of employment;
- payroll details;
- tax and national insurance information;
- details of job duties;
- details of health and sickness absence records;
- details of holiday records;
- information about performance;
- details of any disciplinary and grievance investigations and proceedings;
- training records;

- contact names and addresses; and
- correspondence with the Company and other information that you have given the Company.

The Company believes that those records used are consistent with the employment relationship between the Company and yourself and with the data protection principles. The data the Company holds will be for management and administrative use only but the Company may, from time to time, need to disclose some data it holds about you to relevant third parties (e.g. where legally obliged to do so by HM Revenue and Customs, where requested to do so by yourself for the purpose of giving a reference or in relation to maintenance support and/or the hosting of data in relation to the provision of insurance).

In some cases the Company may hold sensitive data, which is defined by the legislation as special categories of personal data, about you. For example, this could be information about health, racial or ethnic origin, criminal convictions, trade union membership, or religious beliefs. This information may be processed not only to meet the Company's legal responsibilities but, for example, for purposes of personnel management and administration, suitability for employment and to comply with equal opportunity legislation. Since this information is considered sensitive, the processing of which may cause concern or distress, you will be asked to give express consent for this information to be processed, unless the Company has a specific legal requirement to process such data.

Access to data

You have the right to obtain a copy of the information that is held about you. This is known as a 'subject access request'. Whilst there is no fee, a reasonable fee may be charged where the request is manifestly unfounded or excessive to cover the administrative costs of complying with the request.

You may, within a period of one month of a written or verbal request, inspect and/or have a copy, subject to the requirements of the legislation, of information held in your personnel file and/or other specified personal data and, if necessary, require corrections should such records be incorrect. Should you wish to do so, you must make a written or verbal request to your line manager in the first instance.

Data Security

You are responsible for ensuring that any personal data that you hold and/or process as part of your job role is stored securely.

You must ensure that personal information is not disclosed either orally or in writing, via web pages, or by any other means, accidentally or otherwise, to any unauthorised third party.

You should note that unauthorised disclosure may result in action under the disciplinary procedure, which may include dismissal for gross misconduct. Personal information should be kept in a locked filing cabinet, drawer, or safe. Electronic data should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

When travelling with a device containing personal data, you must ensure both the device and data is password protected. The device should be kept secure and where possible should be locked away out of sight. At no time should the device be left in a car. You should avoid travelling with hard copies of personal data where there is secure electronic storage available. When it is essential to travel with hard copies of personal data this should be kept securely in a bag and where possible locked away out of sight.