DATA PROTECTION & PRIVACY POLICY

GENERAL

The CDR Group is registered with the Data Protection Act 1998 and registration is renewed annually. Compliance with the Data Protection Act is considered to be of prime importance to the Company and all activities within the scope of the Act are closely monitored.

Responsibility for compliance with the Act rests with the Directors and Managers. Staff are made aware of the importance of complying with the Act as part of their induction procedure. During the course of their work, staff are regularly reminded that any personal details are to be treated as highly confidential and not to be divulged to any other party. Any contravention of this directive would be subject to the Disciplinary Procedure.

The Directors are fully supportive of this policy and expect all staff to conform to the Data Protection Act.

PRIVACY POLICY

This Privacy Policy describes CDR's current policies and practices with regards to personal data collection by CDR through is websites, (hereinafter referred to collectively as "CDR's websites"). The term "personal data" refers to personally identifiable information about you, such as your name, birth date, e-mail address or mailing address, and any other information that is identified with you personally.

Personal Data Collected Through CDR's Websites or Landing pages

The only personal data CDR currently collects through its websites is the information you voluntarily give us when you use our sites.

For example, you may use this site to contact CDR with questions and comments. When you fill out a form on our websites, you may provide your name and other contact information, including your company's name, your e-mail address, and your mailing address or the mailing address of your company or other personal information.

Use of Personal Data Collected Through CDR Websites

CDR uses the personal data information you provide to answer the query you will have posted through the site. CDR also use this information to help us improve the content and functionality of our websites, to better understand our customers and markets, and to improve our products and services. CDR may use this information to contact you in the future to tell you about products or services we believe will be of interest to you. If we do so, each communication we send you will contain instructions permitting you to "opt-out" of, or cancel the subscription.

Requirements and Criteria for Processing

CDR ensure that:

(a) personal data is processed fairly and lawfully;

(b) personal data is always processed in accordance with good practice;

(c) personal data is only collected for specific, explicitly stated and legitimate purposes;

(d) personal data is not processed for any purpose that is incompatible with that for which the information is collected

(e) personal data that is processed is adequate and relevant in relation to the purposes of the processing;

(f) no more personal data is processed than is necessary having regard to the purpose of the processing;

(g) personal data that is processed is correct and, if necessary, up to date;

(h) all reasonable measures are taken to complete, correct, block or erase data to the extent that such data is incomplete or incorrect, having regard to the purposes for which they are processed;

(i) personal data is not kept for a period longer than is necessary, having regard to the purpose for which they are processed.

Personal data may be processed only if:

(a) the data subject has given their consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for the compliance with a legal obligation to which CDR is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of an activity that is carried out in the public interest or in the exercise of official authority vested in CDR or in a third party to whom the data is disclosed: or

(f) processing is necessary for a purpose that concerns a legitimate interest of CDR or of such a third party to whom personal data is provided, except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject and in particular the right to privacy.

Anonymous Data Collected Through CDR Websites

In addition to the information you provide when you use our websites, CDR uses technology to collect anonymous information about the use of our websites. For example, we use technology to track how many visitors access our websites, the date and time of their visit, the length of their stay, and which pages they view. We also use technology to determine which web browsers our visitors use and the address from which they accessed our sites (for example, if they connected to a CDR website by clicking on one of our banner ads).

This technology does not identify you personally. It simply enables us to compile statistics about our visitors and their use of our sites and to better understand our customers and markets, and to improve our products and services.

Subject Access Policy

CDR will provide information in response to any reasonable subject access request. CDR will ensure data are kept in an accessible form to facilitate subject access.

CDR at the request of the data subject shall provide to the data subject, without excessive delay and without expense, written information as to whether personal data concerning the data subject is processed:

Provided that a request by the data subject as aforesaid shall only be made by the data subject at reasonable intervals.

Any such application shall be made in writing to CDR and is to be signed by the data subject.

If such data is processed CDR shall provide to the data subject written information in an intelligible form about:

(a) actual information about the data subject which is processed;

(b) where this information has been collected;

(c) the purpose of the processing;

(d) to which recipients or categories of recipients the information is disclosed; and

(e) knowledge of the logic involved in any automatic processing of data concerning the data subject.

CREDIT CARD TRANSACTIONS

Clients of the CDR Group may wish to pay for goods or services using a credit or debit card. This may be either a personal card or a company card. It is of prime importance that data relating to such cards is handled in a secure manner.

The following procedures for card transactions must be observed at all times:

- Clients should be strongly discouraged from transmitting card details by email, fax or post

- In the event that card details are received by email, fax or post then all paper documentation showing any information relating to the card must be securely shredded as soon as the card transaction has been completed. In addition, in the case of email, all email messages containing information relating to the card must be completely deleted as soon as the card transaction has been completed. This includes any copies of the message that may have been archived
- Card details received by telephone may be recorded on paper temporarily. The card transaction should be completed as soon as possible following the telephone call. The paper record must be securely shredded as soon as the card transaction has been completed
- Card transactions must only be carried out using the Sage Pay on-line terminal
- Card transactions must only be carried out using the designated PC to access the terminal
- Card transactions must only be carried out when the CDR Group's firewall and virus protection systems are fully operational
- Card transactions must only be carried out by a member of staff who has been trained in these security procedures and trained in the use of the terminal
- The full card details must not be displayed on any acknowledgement, receipt or invoice issued to the Client
- Telephone monitoring/recording systems must be turned off whilst card details are being relayed.
- The card details must not be recorded on any document or other media that will be retained by the CDR Group
- Employees must not communicate card details to any person by any means whatsoever

If any Employee has reason to believe that the security of card details, or of the designated PC, has been breached they must report this immediately to senior management.

Senior management will promptly report any perceived actual or potential breach of the security of card details to the card user, the card issuer and the Police. A written record will be maintained of all such reports. Senior management will thoroughly investigate the circumstances surrounding the perceived actual or potential breach of security, and will act promptly upon both the findings of that investigation and on any recommendation made by the card issuer or the Police.