Policy – data protection

We take seriously our duties, and the duties of our employees, under the Data Protection Act 1998 (the DPA). This policy sets out how we deal with employees' personal data and employees' obligations in relation to any personal data that they handle.

The Data Protection Manager is responsible for ensuring compliance with the Act and with this policy. That post is held by the HR Manager. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Manager,

Frequently used terms in this policy

Personal data means data kept electronically or in a structured paper file and relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual or it can be an opinion or statement of intention in relation to the individual.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings.

Data protection compliance

We will process personal data to comply with the eight principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully
- Processed for limited purposes and in an appropriate way
- Adequate, relevant and not excessive for the purpose
- Accurate
- Not kept longer than necessary for the purpose
- Processed in line with data subjects' rights
- Secure
- Not transferred to people or organisations situated in countries without adequate protection

How we are likely to use your personal data

We need to keep information on file about you for normal employment purposes. The information we hold is for our management and administrative use only. We will keep and use this information to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately, from the time you first apply for a job, whilst you are working for us, at the time when your employment ends and after you leave. This includes using information to enable us to comply with our contractual obligations and to protect our legal position in the event of claims against us. Much of the information we hold will have been provided by you, but some may come from other internal sources, such as your manager or, in some cases, external sources, such as referees. You may ask to see your personal file kept by the HR Department.

The sort of information we hold about you

The sort of information we hold includes:

- your application form and references
- your contract of employment/statement of employment particulars and any amendments to it
- correspondence with or about you, for example letters to you about a pay rise or, at your request, a letter to your mortgage company confirming your salary
- information needed for payroll, benefits and expenses purposes
- contact and emergency contact details
- records relevant to your right to work in the UK
- records of holiday, sickness and other absences
- records relating to your career history, such as training records, appraisals, other performance measures and, where appropriate, disciplinary and grievance records
- information about some of your protected characteristics for monitoring purposes only

Of course, you will also inevitably be referred to in many company documents and records which are produced by you and your colleagues in the course of carrying out your duties and the business of the company.

Where necessary, we may keep information relating to your health. This information might include reasons for any absences and doctor's reports and notes and will be used for the following:

- to comply with our health and safety and occupational health obligations
- to manage sickness absence and to consider how your health affects your ability to do your job and whether any adjustments to your job might be appropriate
- to administer and manage statutory and company sick pay

We monitor computer and telephone/mobile telephone use, as detailed in our electronic communications policy.

A CCTV system monitors all areas of the site inside and out, including the back car park, the Go-Kart car park, Liverpool Street and some areas of Heath Mill Lane. Images are recorded and retained for a limited period of time. This is primarily for security purposes, although in rare cases we may use CCTV footage in investigations into allegations of misconduct by employees, for example if a fight or vandalism is alleged to have taken place outside the building.

We keep records of your hours of work by way of our clocking on and off system, as detailed in

section 7a of the employee handbook.

When we give information about you to third parties

We may disclose information about you to third parties, for example:

- if we are legally obliged to do so
- to comply with our contractual duties to you
- to contractors who carry out some of our functions, such as our payroll functions, pensions and life insurance.
- where we transfer information about you to other group companies or to group head office for purposes connected with your career or the management of the company's business
- upon your request

Transferring information outside the European Economic Area

Sometimes we may need to transfer some information about you to our parent company which is based in the USA. The purpose of this data transfer is to ensure that legislative and corporate requirements are met, in both the UK and USA.

Accurate data

We will keep the personal data we hold about you accurate and up to date. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data. Please notify us if your personal details change or if you become aware of any inaccuracies in the personal data we hold about you.

Data retention

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

For guidance on how long certain data is likely to be kept before being destroyed, contact the HR Manager.

Disposal of data

All hard copy personal data and IT equipment including hard drives are disposed of in a secure manner by an approved waste disposal contractor and relevant waste transfer notes obtained.

All hard copy personal data is either securely shredded on site or disposed of off site via secured facilities. Hard drives are shredded at an off site facility.

Processing in line with your rights

We will process personal data in line with your rights, in particular your right to:

- Request access to personal data we hold about you
- Prevent the processing of your data for direct-marketing purposes.

- Ask to have inaccurate data amended
- Prevent processing that is likely to cause damage or distress to yourself or anyone else.
- Object to any decision that significantly affects you being taken solely by a computer or other automated process.

Data security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. All paper records are locked in a secure area, data transferred to/from a third party (such as payroll, pension, hearing screening) are password protected, any information shared electronically is password protected.

We have put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a third party if it agrees to comply with those procedures and policies, or if it puts in place adequate measures itself.

We will maintain data security by protecting the confidentiality, integrity and availability (for authorised purposes) of the personal data.

Hard copy personal data, whether related to our employees, suppliers or customers is held in secure cabinets with access restricted to limited staff. This personal data is not routinely carried in transit however where is it required to be transported, it will be held securely.

Third party access to ICT systems

With the exception to our primary IT support partner, access to the company systems is restricted and can only be accessed as agreed with the system administrator. All 3rd party providers are bound by confidentiality and security clauses within service level agreements agreed.

Accessing your personal data

If you wish to access personal data we hold about you under the DPA's subject access provisions, you should make a request in writing to HR Manager.

Your obligations regarding personal data

Everyone has rights with regard to the way in which their personal data is handled. During the course of the company's activities, we will collect, store and process personal data not only about our employees but also about our customers, suppliers and other third parties.

Employees are obliged to comply with data protection law and the data principles set out above when processing personal data on our behalf (including that of other employees). In particular they are obliged to comply with the following provisions and/or any other guidelines produced by the company relating to personal data and/or any other management instructions.

If you are in any doubt about what to do with personal information, you should seek advice from the

HR Manager.

Any breach of these obligations may result in disciplinary action.

If you acquire any personal data in the course of your duties, you must ensure that the use of the information is for a relevant purpose and that it is not kept longer than necessary.

For further guidelines on the retention of data and the company's standard retention periods, see/contact the HR Manager.

If you acquire any personal data in the course of your duties, you must ensure that the information is accurate and up to date, insofar as it is practicable to do so.

See the company's policies (data protection policy, electronic data protection policy, handbook and annual code of business conduct and ethics) for your obligations in relation to document security. In particular, you should ensure that you:

- Use password-protected and encrypted software for the transmission and receipt of emails containing personal data.
- Lock files in a secure cabinet
- Do not take any company information away from the company's premises, or access such information on personal devices, except where you have obtained the prior consent of a Senior Manager
- Do not leave your laptop, other device or any hard copies of documents in a public place and that you take care when observing the information in hard copy or on-screen that such information is not viewed by anyone who also has the right to that information.

Where information containing personal data is disposed of, you should ensure that this is done securely. This may involve:

- permanent removal of information from the server (so that it does not remain in your inbox or trash folder)
- shredding hard copies of confidential information

If you receive personal information in error by whatever means, you must inform the HR Manager immediately.

Status of this policy and new instructions

This policy does not give contractual rights to individual employees. The company reserves the right to alter any of its terms at any time, although we will notify you in writing of any changes.

Please sign either Statement A or Statement B below

Statement A

I have received and understand the contents of this policy. I give my consent for Cerro EMS to collect, process and retain my personal data.

Signed Print

Date

Statement B

I would like to withdraw my consent for Cerro EMS to collect, process and retain my personal data. I understand the consequences of withdrawing this consent.

Signed Print

Date