Appendix to Data Protection Policy HR

CCTV POLICY

In this policy:

"the company" means The AFE Group Ltd trading under the business unit names of Mono Bakery Equipment, Millers Vanguard, Falcon Foodservice Equipment, Serviceline, Williams Refrigeration"
"the data controller" means the registered body responsible for the control of data access in compliance with this policy and associated acts
"CCTV" means closed- circuit television, or in vehicle camera device
"the system" means the CCTV System

The company's CCTV system will operate fairly, within the law, and primarily for the purposes of Crime Prevention, Site Security and Health & Safety as stated on signage located around the premises. The system operates 24 hours a day, 365 days a year. It is intended, within reasonable limits, to offer a balance between the objectives of CCTV and the need to safeguard an individual's right to privacy. There is no audio feed or audio recording on the system.

The key objective of the CCTV system is to detect, prevent or reduce the incidence of crime and the monitoring of health, safety, welfare and good conduct of those on the site premises, and in meeting vehicle insurance conditions for driver and road safety.

The aim of the CCTV system is to make the company a safe and responsible place to work. There will be no deliberate monitoring of people, or employees carrying out their legitimate business.

The CCTV system is registered with the Information Commissioners Office. The Company Data Controller is Mr Timothy Smith, Company Secretary. Each business unit will appoint a senior officer as its local data controller.

Access to the CCTV data is limited to a select number of CCTV operatives, these operatives will be required to sign to say they have read and understood the rules of this policy and agree to confidentiality over matters that may arise.

Access to the data will be controlled by a data request application made to the Data Controller who will validate the request and authorise data access, limited to the specific incident and associated recordings. If permission is given then this request will be logged. The log will include date of request, who made the request, why the request was made.

A data request must be very clear and precise in date, location and time to pinpoint the relevant recordings and enable the CCTV operatives to work efficiently and comply with Data Protection. Only the data that relates to the person or the issue will be released. Recorded images must only be viewed in a confidential area and only by the authorised staff who have access. If a request is made to release data to the Police or other Enforcement Body as part of an investigation process then this would be authorised by the Data Controller and logged accordingly.

Recorded data will be retained for a period of up to 30 days, after which this data will be overwritten. In accordance with the provisions of the above Act, all requests will be responded to within 30 days of receiving the required information. Any breaches of the above will be subject to an investigation and if proved will be treated as Gross Misconduct in accordance with the internal Disciplinary Procedures.

This policy has been prepared in conjunction with the CCTV Code of Practise as issued by the Information Commissioners Office.