Closed Circuit Television (CCTV) Policy

1.0 Ownership

J Coffey Construction ('the Company') operates a CCTV surveillance system ("the system") throughout the company's premises and divisional offices, with images being monitored and recorded centrally. The system is owned and managed by the J Coffey Construction Ltd with technical support provided by ADT Fire & Security.
The responsible person monitoring/reviewing footage will be the J. Coffey Plant Division Director.

2.0 Purpose

The Company's registered purpose for processing personal data through use of the system is crime prevention and/or staff monitoring. This is further defined as:
CCTV is used for maintaining public safety, the security of property and premises and for preventing and investigating crime, it may also be used to monitor staff when carrying out work duties. For these reasons the information processed may include visual images, personal appearance and behaviours. This information may be about staff, customers and clients, offenders and suspected offenders, members of the public and those inside, entering or in the immediate vicinity of the area under surveillance. Where necessary or required this information is shared with the data subjects themselves, employees and agents, services providers, police forces, court or tribunal, security organisations and persons making an enquiry in accordance with GDPR (refer to Company GDPR Policy.
The operators of the system recognise the effect of such systems on the individual and the right to privacy.

Full details of the Company's data protection registration are available on the Information Commissioner's Office website.

3.0 Compliance

Images obtained from the system which include recognisable individuals constitute personal data and are covered by the Data Protection Act & GDPR. This Policy should therefore be read in conjunction with the Company's GDPR Policy.
The appointed person for the Company is the J Coffey Plant Division Director (JCPDD) in conjunction with the Appointed Information Manager (AIM) who is responsible for ensuring compliance with the Act.
This policy has been drawn up in accordance with the advisory guidance contained within the Information Commissioner's CCTV Code of Practice and the Home Office Surveillance Camera Code of Practice.
Failure to comply with this policy may result in disciplinary action being taken, which may include summary dismissal. If there is anything in this policy that you do not understand, please discuss it with your line manager/departmental head.

4.0 Description

The system is intended to produce images as clear as possible and appropriate for the purposes stated. The system is operated to provide when required, information and images of evidential value.
Cameras are located at strategic points throughout the premises and divisional offices, principally at the perimeters, entrance and exit points of buildings and public and non-public spaces.
Signage is prominently placed at strategic points on the estate to inform staff, visitors and members of the public that a CCTV installation is in use and includes contact details for further information.

5.0 Operation

Images captured by the system are recorded continuously and may be monitored in the Control Room. Images displayed on monitors are not visible from outside the Control Room and access to the Control Room is strictly limited.
All Security staff working in the Control Room are made aware of the sensitivity of handling CCTV images and recordings. The Senior Controller will ensure that authorised staff are fully briefed and trained in all aspects of the operational and administrative functions of the system.

6.0 Information Retention

No more images and information shall be stored than is required for the stated purpose. Images will be deleted once their purpose has been discharged. Information used as a reference database for matching purposes will be accurate and kept up to date.

7.0 Access

All access to recorded images is recorded in the Control Room daily log. Access to images is restricted to those who need to have access in accordance with this policy, the SOPs and any governing legislation.
Disclosure of recorded material will only be made to third parties in accordance with the purposes of the system and in compliance with the Data Protection Act & GDPR
Anyone who believes that they have been filmed by the system can request a copy of the recording, subject to any restrictions covered by the Data Protection Act & GDPR. Right of access requests must be in writing and issued on the appropriate 'Right of Access' request form. There should be a clear responsibility on all employees to pass on anything which might be a 'Right of Access' to the appropriate person without delay.
Data subjects also have the right to request that inaccurate data be corrected or erased and to seek redress for any damage caused. Procedures are in place to ensure all such access requests are dealt with effectively and within the law.
Requests may come from the business for access to images due to reasonable suspicion that they may reveal evidence of an unlawful act, including instances where there may be a breach of code of conduct. All such requests must be submitted in writing by a Senior Manager or above to the JCPDD or AIM, who will retain a copy of the request.

Prior to granting access the JCPDD or AIM shall review the requested image, to ascertain if there is clear visible evidence consistent with the request, prior to release of the image to the requestor.

All who have been granted access for viewing images are responsible for ensuring that the viewing of images is undertaken where they cannot be copied or seen by unauthorised personnel.
In the event that the viewer experiences feelings of anxiety due to the nature of the image, this is to be escalated to HR who will make arrangements to have a one to one with the individual.

93/95 Greenford Road, Harrow Middlesex HA1 3QF

Refer to our GDPR policy situated on the K drive or on our website.

8.0 Covert Recording

Covert cameras may be used only in very limited circumstances. This requires written authorisation of the JCPDD and, where this may involve members of staff, the Head of Human Resources. (HR)
Covert surveillance may be carried out in cases of suspected specific criminal activity only where the objective of making the recording would be seriously prejudiced should the individual(s) concerned be informed of such surveillance.
Any authorisation to use covert surveillance must include a justification of the need to use such methods to obtain evidence of suspected criminal activity in a specific case; an assessment of alternative methods of obtaining such evidence and a statement of how long the covert monitoring should take place. The authorisation must be reviewed every 28 days and consider whether that should continue or be closed. Any decision to use covert surveillance for

any reason must be fully documented and records of such decision retained securely.

9.0 Annual Review

This policy was approved by the GDPR Committee on the 17th July 2018. It will be reviewed annually by the same committee and if there is any change in relevant legislation that might affect this policy to ensure that the purpose still applies.

This policy applies to all employees and other personnel engaged in J Coffey Construction operations:

Signed: E. Barrett (Original Signed Date: 14.01.2022

Eddie Barrett

Group Managing Director

On behalf of J Coffey Construction