CLOSE CIRCUIT TELEVISION POLICY

Introduction

The purpose of this Policy is to describe the circumstances in which the Company conducts surveillance of its employees, workers and contractors using Close Circuit Television ('CCTV').

This Policy should be read in conjunction with relevant Company policies, including:

a. Data Protection Policy.

b. Biometric Data Policy.

This Policy complies with the Data Protection Code of Practice on surveillance cameras.

Purpose

The Company has installed fixed CCTV cameras on many of its construction sites, both inside and outside of buildings and other facilities. These cameras (including any casings) are not covered or hidden, and monitor activities on an ongoing and continuous basis (including the use of time-lapse images).

The CCTV cameras record and store information and create records (including reports) in relation to the following:

a. Movements throughout the construction site.

b. Access to secure Company facilities (including outside the perimeter of the site).

c. Movements at entry points of the site.

Collection, storage and use of the data

The Company will use the data collected to monitor its workplace, construction sites, access points and perimeter in order to:

- Ensure the security of the site.
- Monitor workplace performance including scheduling.
- The integrity, security and service delivery of its projects.
- Ensure the health and safety of its employees, contractors and workers.
- Use images from time to time for marketing and information purposes for clients and appropriate third parties.
- Comply with any legal obligations, such as reporting obligations to authorities.

Such monitoring involves the collection or storage of information, including the creation of records, in a routine and passive manner. It also includes routine review of that information or those records to ensure the integrity, security and service delivery of the Company. However, and for the avoidance of doubt, such monitoring does not involve actively investigating or keeping track of an individual or his or her activities.
The Company will not conduct CCTV surveillance in any changing room or toilet facility.

Secure data

Recorded material will be stored in a way that maintains the integrity of the information. This is to ensure that the rights of individuals recorded by surveillance systems are protected and that the information can be used effectively for its intended purpose. The data will be held within a secure network at all times. In the event that the data is stored within a cloud computing system, the Company will take all reasonable steps to ensure that the system is secure and if the Company has a contract with a cloud provider the provider will need to ensure the security of the information held.

The Company will undertake periodic deletion of the data held on the system. The frequency of deletion of data will depend upon the business needs for each project and whether the Company is required to supply any of the recorded information to a regulatory third party or law enforcement agency. The Data Protection Act does not prescribe any specific minimum or maximum retention

periods which apply to all systems or footage. Retention will reflect the Company's purposes for recording information and the project needs.

Authorisation

Only authorised personnel are allowed to access CCTV surveillance information including:

- The appointed IT employees whose normal duties include routine back up or restoration of data, conduct of audits, review of web filtering, email filtering, document retrieval or logs, or other activities relating to the Company's IT and Network systems.
- Site managers or other senior managers who have been specifically authorised to have access to review CCTV footage.
- Employees who are specifically given authority to view specific CCTV data under a project request. Such request to be made to the appointed IT employee who will allow access for a particular project purpose. Such access will be logged and recorded for each project.
- Authorised Human Resources personnel.
- Company Directors.
- Third Party personnel who have been authorised by a Company Director and who have responded and acknowledged our email disclaimer.

If any employee of the Company has a concern regarding the disclosure of any data, then they must seek authority from the person appointed by the Company to have overall responsibility of the CCTV data.

Notice of CCTV use

The Company also provides notice to employees, contractors and workers about CCTV use as follows:

a. Clear, visible and readable signage at site entrances to sites, on perimeter fences and within workplace areas containing details of the purposes of the surveillance and who to contact.

b. By obtaining a signed acknowledgement when an employee commences on the site

CCTV use involving general public

The only occasion when the Company may inadvertently take surveillance information which involves the general public is when CCTV cameras capture images on the perimeter of the Company sites (although CCTV footage may capture visitors to sites). It is accepted that this data may include images of individuals who are under the age of 18 years of age.

The Company ensures that signage for its CCTV cameras is checked on a regular basis in order that the use of CCTV cameras at these locations is clear to employees, contractors, workers and the general public.

Whenever the Company intends to use CCTV images for any of the purposes set out above it will ensure that images of the general public are where reasonably possible not released to a client or third party, unless such images involve personnel who either work or are present on the client site.

Before release of such images to a client or third party the Company will use reasonable endeavours to understand the purposes the client or third party needs the surveillance data for and ask the client or third party about the policies it has in place to cover the use of this data.

Where a client or third party is given full access to the images which may inadvertently include the general public the Company will require assurance from the client or third party that they have policies in place to cover the use of this data.

Review

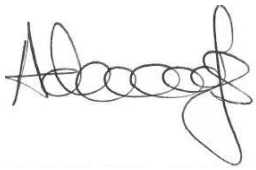
The Company will undertake a periodic review of the systems in place to safeguard the data and the data held on the system to ensure it is not held for any longer than reasonably necessary.

Disciplinary

The Company may take disciplinary action, up to and including termination of employment, for any breach of this Policy.

Signed: 

Francis Shiner – Managing Director

Signed: 

Adam Knaggs – Director

Signed: 

Martin Lowndes – Director

Signed: 

Craig Millar – Director

Signed: 

Gary Wykes – Director

Date: **January 2019**

Next Review Date: **January 2020**