CCTV SECURITY & DATA PROTECTION POLICY

1.0 Scope

1.1 Use of CCTV security cameras on the business premise for the purpose of crime prevention.

2.0 Legal Requirement

2.1 Where CCTV security cameras are in use on business premises for the purpose of crime prevention then the installation and data it produces is subject to the Data Protection Act 1998. It is required that:

(1) An assessment of the requirement for the company to operate CCTV is completed prior to installation
(2) That access to that stored information must be strictly controlled.
(3) Use of CCTV requires notification to the Information Commissioner's Office (ICO).

Note on Background to the Use of CCTV Camera Surveillance and Applicability of the Data Protection Act (taken from ICO website):

CCTV is used for maintaining 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, security organisations and persons making an enquiry.

3.0 Procedure

3.1 Appointment of Site Data Controller

3.1.1 The Managing Director will appoint a competent an individual to control the CCTV system and access to the images that are recorded. This person shall act as the Data Controller for the company. For ETS Group this role is held by Lucasz Lemieszonek, Contracts Supervisor.

3.1.2 All organisations that are using CCTV must understand the obligations of its use.

3.2 Registration of CCTV With ICO

3.2.1 Where the company uses CCTV then the company must register the system with the Information Commissioner. This is completed at the website below and must be completed every 12 months.

https://ico.org.uk/for-organisations/register/

3.3 Installation and Maintenance

3.3.1 Installation of CCTV Security Camera Systems is to be completed where a security Assessment of the site identifies that CCTV Security Cameras are a necessary action for crime prevention. All other security measures are to be considered before authorising the installation of a CCTV Security Camera System on business property.

3.3.2 The CCTV Security Camera System is only to be completed by competent, trained installers.

3.3.3 Each camera must be identified by a unique reference and serial number, linked to the relevant system.

3.3.4 Information on the security system is held by the Site Data Controller and the installing company.

3.3.5 In the event that there is a fault, or if the equipment is tampered with, the installer / maintainer must rectify any issue with the equipment.

3.3.6 In the event that any tampering or removal of any camera or equipment is identified, an investigation will take place. If involving employed individuals this may result in disciplinary proceedings taking place. For any tampering with the CCTV system the Managing Director and Site Data Controller will evaluate the need to inform the local Police service.

3.4 **Signage**

3.4.1 So to inform people that they are been monitored by CCTV signs will be displayed which are clearly visible and readable to all individuals that may be observed by the cameras.

3.4.2 Signage will contain the contact details of the company operating the system and the purpose for which the images are being recorded.

3.5 **Storage of Images**

3.5.1 Images (aka data) is stored within a secure location.

3.5.2 Access to this information will be controlled by the company Data Controller. Storage of the images and the retention period will be defined using the company form - *Annual Assessment of Use of CCTV Cameras within Company Premises*.

3.5.3 Images will be stored for 1 month which provides for sufficient retention of data for a crime or security incident to be detected, investigated and action taken to rectify.

3.5.4 The company will not allow disclosure images of identifiable people to the media Images released to the media to help identify a person will only be disclosed by the police.

3.5.5 The company will not allow captured images to be put on the internet.

3.5.6 The company may need to disclose CCTV images for legal reasons, for example crime detection. The only person authorised to do this is the company Data Controller or nominated deputy.

3.6 **Viewing Images**

3.6.1 Live footage of the premises will be displayed in the office for live management of site security purposes only.

3.6.2 The Data Controller (or nominated deputy) must vet who views all recorded footage. Should unauthorised viewing of the recorded footage occur the Data Controller shall escalate any concerns to the Managing Director. These concerns may also be escalated externally depending on the nature of the concern e.g. criminal proceedings.

3.6.3 Requests may also come from the company 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 to the Data Controller who will retain a copy of the request.

3.6.4 Prior to granting access the Data Controller 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.

3.6.5 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.

3.6.6 Images may also be used for training purposes of a deputised or replacement person. It is the responsibility of the Data Controller to ensure all such images exclude any personal identifiable data.

3.7 **Subject Access Requests**

3.7.1 In the event that a subject access request is received (a subject access request is a written request made by or on behalf of an individual for information involving themselves that he or she is entitled to ask for under the Data Protection Act 1998), this should be escalated to the company Data Controller in the first instance.

3.7.2 Individuals have the right to see CCTV images of themselves and to ask for a copy of them. The company will provide them within 40 calendar days of any request. The Data Controller will ensure that the requestor provides details to help the company to confirm the identity as the person in the pictures, and to help to find the images on their system.

3.7.3 A maximum fee of £10 can be imposed for the requested information and the 40 days will not commence until the fee has been received.

3.7.4 Upon receipt of a request, the Data Controller shall record the following:

(1) Date of request
(2) Requestor details
(3) Type of information requested

3.7.5 The Data Controller shall ensure that the record is updated throughout the processing of the request (date of correspondence sent/received, 40 day action date, action complete date, staff involved, and comments).

3.8 **External Requests**

3.8.1 In the event that a request is received from an external source eg the Police, this should be escalated to the company Data Controller in the first instance. The Data Controller will ensure that any information that is handed over will be handled by the receiver in accordance with the Data Protection Act 1998 prior to any information being provided.

3.9 **Compliance with this Policy**

3.9.1 Failure to comply with this policy will result in an investigation and may result in disciplinary action being taken, which may include summary dismissal.

3.9.2 Should any individual not understand any part pf this Policy they must discuss it with their line manager or the Site Data Controller.

3.9.3 Further advice can be obtained via the Information Commissioner 0303 123 1113.

APPENDIX A: GUIDANCE ON REGISTERING ON ICO DATA PROTECTION REGISTRAION WEBSITE

Have your company registration number, address and company credit / debit card to hand.

Go to https://ico.org.uk/for-organisations/register/

Part 1. About You

Organisation type: eg Limited company

Company Registration Number

Company Name

Organisation Address (as registered with Companies House)

Customer Enquiries Contact Details (Contact Name, Address, Email, Phone Number)

Part 2. Registration Details

Sector: If you are a construction company this is *Land or Property Services*

Nature of work: *Construction Company*

Scroll down and tick under Additional Reasons “CCTV for Crime Prevention”

Part 3. Other Obligations

The below list of questions is asked. The answer must be "*Yes*" to all of them,

1. Someone in my place of work is responsible for making sure we comply with the Data Protection Act **A: Yes**
2. Relevant people in my place of work have been trained in how to handle personal information **A: Yes**
3. When collecting personal information, we tell people how we will use it **A: Yes**
4. We have a process in place so we can respond to requests for the personal information we hold **A: Yes**
5. We keep records of people's personal information up to date and don't keep it longer than necessary **A: Yes**
6. We have measures in place to keep the personal data we hold safe and secure **A: Yes**

Part 4.

The information recorded will be confirmed, and you can then proceed to payment.

The ICO Registration Certificate to be shared to Management System/Records/Corporate Records with the expiry date set for 1 year.

For ETS Group

Mark Cole *Date: 16th July 2021*
Managing Director