CCTV (Closed Circuit Television) Policy

1. Introduction

The Company uses closed circuit television (CCTV) images to protect the Company's property and to provide a safe and secure environment for employees and visitors to the Company's business premises. This policy sets out the details of how the Company will collect, use, and store CCTV recordings and the obligations and/or rights of all employees, contractors, customers, visitors, and any other person/s on Company premises to which this policy is applicable.

We recognise that images of individuals recorded by CCTV cameras in the workplace are personal data and therefore subject to data protection legislation. We are committed to complying with all our legal obligations and seek to comply with best practice suggestions from the ICO (Information Commissioner's Office).

Unless there are exceptional circumstances, the Company will only record video (see covert recording below).

This policy is non-contractual and may be reviewed at any time and changed to meet the requirements of the business and/or requirements of any applicable legislation.

2. Scope

This policy applies to all employees, contractors, customers, visitors, and any other person/s on Company premises.

3. Definitions

- **CCTV** – closed circuit television. Fixed and domed cameras to capture recordings of individuals, property, and assets.
- **Surveillance Systems** – any device or systems designed to monitor and/or record images of individuals or information relating to individuals. This term generally refers to any systems that capture information of identifiable individuals or information relating to identifiable individuals.
- **ICO** – Information Commissioners Office.
- **Personal Data** – data relating to a living individual who can be identified from that data. In respect of CCTV, this will include video images of identifiable individuals. It may also include static pictures such as printed screen shots.

4. Aims

The Company aims as far as reasonably practicable to maintain a safe and secure environment for all our staff and visitors and to protect its property. The Company considers it necessary, proportionate, and legitimate to use CCTV in the management of its business including:

- The personal safety of employees and visitors, and to act as a deterrent against crime.
- The prevention or detection of crime or equivalent malpractice, and to protect buildings and assets from damage, disruption, and vandalism.
- Monitoring of the security of the Company's business premises.
- Ensuring compliance with Health and Safety rules and requirements and Company procedures.
- Identification of unauthorised actions or unsafe working practices.
- To assist in evidence and the effective resolution of disputes which may arise during the course of disciplinary and/or grievance investigation and processes.
- To support law enforcement bodies in the identification and prosecution of offenders.

This list is not exhaustive.

5. Location of cameras

Cameras are located at strategic points throughout the Company's business premises, principally at the entrance and exit points. The Company has positioned the cameras so that they only cover communal or public areas on the Company's business premises, and they have been sited so that as far as practicably possible they provide clear images. No camera focuses, or will focus, on toilets, shower facilities, or changing rooms. Cameras will only be placed in staff kitchen areas; staff break rooms or private offices if a specific need is identified.

All cameras (with the exception of any that may be temporarily set up for covert recording) are also clearly visible.

Appropriate signs are prominently displayed so that employees, clients, customers, and other visitors are aware they are entering an area covered by CCTV.

Cameras are not always active, and the business reserves the right to activate and de-activate cameras from time to time.

6. Recording and retention of images

Images produced by the CCTV equipment are intended to be as clear as possible so that they are effective for the purposes set out above. Maintenance checks of the equipment are undertaken on a regular basis to ensure it is working properly.

Images may be recorded either in constant real-time (24 hours a day throughout the year), or only at certain times, as the needs of the business dictate.

As the recording system records digital images, any CCTV images that are held on the hard drive of a PC or server are deleted and overwritten on a recycling basis. Once the hard drive has reached the end of its use, it will be erased prior to appropriate disposal.

Images that are stored on or transferred on to removable media such as external drives/USBs or which are stored digitally are erased or destroyed once the purpose of the recording is no longer relevant. In normal circumstances, this will be a period of 30 days. However, where a law enforcement agency is investigating a crime, or an internal process is ongoing, images may need to be retained for a longer period.

7. Access to, secure storage and disclosure of images

Access to, and disclosure of images recorded on CCTV is restricted to authorised members of staff only.

The images that are filmed are recorded centrally and held in a secure location. Access to recorded images is restricted to the operators of the CCTV system and to those managers who are authorised to view them in accordance with the purposes of the system. Requests to view recordings will be handled via the IT ticketing process. The request will be assessed by the Group Human Resources Director (Data Protection Lead) and the IT Manager. Authorised viewing of recorded images will take place in a restricted area to which other employees will not have access when viewing is occurring. If media on which images are recorded are removed for viewing purposes, this will be documented.

Disclosure of images to other third parties will only be made in accordance with the purposes for which the system is used and will be limited to:

- Third party data processors who provide professional services to us where we cconsider that this is reasonably necessary for any of the purposes set out above or CCTV service support providers.

- The police and other law enforcement agencies, where the images recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness.
- Prosecution agencies, such as the Crown Prosecution Service.
- Insurance bodies in the defence of claims.

A Board member (or another senior director acting in their absence) is the only person who is permitted to authorise disclosure of images to external third parties such as law enforcement agencies.

All requests for disclosure and access to images will be documented, including the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded.

8. Individuals' access rights

Under the UK's data protection laws, including the General Data Protection Regulation (GDPR), individuals may request a copy of the personal data that the Company holds about them, including CCTV images if they are recognisable from the image.

If you wish to request access any CCTV images relating to you, you must make a written request to the Human Resources Manager. The Company will usually not make a charge for such a request, but we may charge a reasonable fee if you make a request which is manifestly unfounded or excessive or is repetitive. Your request must include the date and approximate time when the images were recorded and the location of the particular CCTV camera, so that the images can be easily located, and your identity can be established as the person in the images.

The Company will usually respond promptly and in any case within one month of receiving a request. However, where a request is complex or numerous the Company may extend the one month to respond by a further two months.

The Company will always check the identity of the individual making the request before processing it.

The Group Human Resources Director (Data Protection Lead) will always determine whether disclosure of your images will reveal third party information, as you have no right to access CCTV images relating to other people. In this case, the images of third parties may need to be obscured if it would otherwise involve an unfair intrusion into their privacy. External expertise may be sought in this determination.

If the Company is unable to comply with your request because access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, you will be advised accordingly.

9. Covert recording

The Company is aware that covert recording can only be done in exceptional circumstances for example where the Company suspects criminal activity taking place. On this basis the Company will only undertake covert monitoring if it has carried out a data protection impact assessment which has addressed the following:

- the purpose of the covert recording.
- the necessity and proportionality of the covert recording.
- the risks to the privacy rights of the individual(s) affected by the covert recording.
- the time parameters for conducting the covert recording.
- the safeguards and/or security measures that need to be put in place to ensure the covert recording is conducted in accordance with the data protection laws, including the GDPR.

If after undertaking the data impact assessment the Company considers there is a proportionate risk of criminal activity, or equivalent malpractice taking place or about to take place, and if informing the individuals concerned that the recording is taking place would seriously prejudice its prevention or detection, the Company will covertly record the suspected individual(s).

In doing this the Company will rely on the protection of its own legitimate interests as the lawful and justifiable legal basis for carrying out the covert recording.

Before the covert recording commences the Company will ensure that a member of the Board (or another senior director acting in their absence) agrees with the findings of the data protection assessment and provides written authorisation to proceed with the covert recording.

Covert monitoring may include both video and audio recording.

Covert monitoring will only take place for a limited and reasonable amount of time consistent with the objective of assisting in the prevention and detection of particular suspected criminal activity or equivalent malpractice. Once the specific investigation has been completed, covert monitoring will cease.

Information obtained through covert monitoring will only be used for the prevention or detection of criminal activity or equivalent malpractice. All other information collected in the course of covert monitoring will be deleted or destroyed unless it reveals information which the Company cannot reasonably be expected to ignore.

10. Staff training

The Company will ensure that all employees handling CCTV images or recordings are trained in the operation and administration of the CCTV system and on the impact of the laws regulating data protection and privacy with regard to that system.

11. Responsibility and Implementation

The board of directors has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy. Day-to-day management responsibility for deciding what information is recorded, how it will be used and to whom it may be disclosed has been delegated to the Group Human Resources Director and Group IT Manager. Day-to-day operational responsibility for CCTV cameras and the storage of data recorded is the responsibility of IT Manager.

The Company's Data Protection Lead/Group Human Resources Director is responsible for the implementation and day to day compliance with this policy; they will conduct a regular review of the Company's use and processing of CCTV images and ensure that at all times it remains compliant with the laws regulating data protection and privacy.

Any complaints or enquiries about the operation of the Company's CCTV system should be addressed to the Human Resources Department.

12. Data Protection

The Company will process the personal data collected in connection with the operation of the CCTV policy in accordance with its data protection policy and any internal privacy notices in force at the relevant time. Inappropriate access or disclosure of this personal data will constitute a data breach and should be reported immediately to the Company's Data Protection Lead/Group Human Resources Director in accordance with the Company's data protection policy.

Breach of this policy and any reported data breaches will be investigated and may lead to sanctions under the Company's disciplinary procedure.

Document History

Rev	Section	Revision Detail	Author	Approver	Issue Date
1	All	New	M Percival	S Harris	24 May 2018
2	All	Rebranding to Autocraft Solutions Group	L Paukina	M Percival	26 June 2018
3	All	Major Update	T Pugh	B Barr	22 August 2024