

## **GDPR/CCTV Policy and Code of Practice**

### **General Data Protection Regulation statement**

1. CCTV is installed for the purpose of staff, visitor and premises security.
2. Cameras are installed at various locations inside and outside the premises.
3. Images from the cameras are recorded.
4. The location of all cameras is known to staff.
5. Access to stored images is controlled on a restricted basis within the company.
6. Use of images, including the provision of images to a third party, will be in accordance with our GDPR policy which is available on request or can be downloaded from our website.
7. CCTV images may be used where appropriate as part of staff counselling or disciplinary procedures.
8. External and internal signage is displayed on the premises stating the presence of CCTV and indicating the name of the Data Controller and a contact number during office hours for enquiries.

### **Retention of Images**

Images from cameras are recorded. And are held in access-controlled secure storage. All data is automatically overwritten after 31 days.

### **Access to Images**

All requests for access by Data Subjects is dealt with by the Data Controller. This right of access is covered under GDPR.

All requests for access or for disclosure will be recorded. If access or disclosure is denied, the reason will be given and documented.

Access to recorded images is restricted to the Data Controller and Directors of the firm. The Data Controller will take advice on whether a request to access images by data subjects and/or third parties is valid. All requests for access must be directed to the Data Controller.

### **Viewing of Images**

Viewing of images will be documented as follows:

- The name of the person removing from secure storage or otherwise accessing, the recordings
- The date and time of removal of the recordings
- The name(s) of the person(s) viewing the images (including the names and organisations of any third parties)
- The reason for the viewing
- The outcome, if any, of the viewing
- The date and time of replacement of the recordings

### **Removal of Images for Use in Legal Proceedings**

In cases where recordings are removed from secure storage for use in legal proceedings, the following will be documented:

- The name of the person removing from secure storage or otherwise accessing the recordings
- The date and time of removal of the recordings
- The reason for removal
- Specific authorisation of removal and provision to a third party
- Any crime incident number to which the images may be relevant
- The place to which the recordings will be taken
- The signature of the collecting police officer, where appropriate
- The date and time of replacement into secure storage of the recordings

### **Access to Images by Third Parties**

Disclosure of recorded images to third parties will only be made in limited and prescribed circumstances. Release will be specifically authorised. Disclosure to third parties will be limited to the following:

- Law enforcement agencies where the images recorded would assist in a specific criminal enquiry
- Prosecution agencies
- Relevant legal representatives
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)

### **Procedures for Dealing with an Access Request by Data Subjects**

The Data Controller will determine whether actioning this request will involve releasing images of third parties are held under a duty of confidence. In all circumstances the firm's indemnity insurers will be asked to advise on the desirability of releasing any information.

The Data Controller will then locate the images requested and determine whether disclosure to the data subject would entail disclosing images of third parties.

If the request is valid and third-party images are not to be disclosed, the Data Controller will arrange for the third party images to be disguised or blurred. An editing company may be used to carry out this task. If an editing company is used, the Data Controller will ensure that there is a contractual relationship between MPACT Group Ltd. and the editing company, and:

- That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images
- The written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the Data Controller
- The written contract makes the security guarantees provided by the editing company explicit

The Data Controller will provide a written response to the data subject within 21 days of receiving the request setting out the Data Controllers' decision on the request. A copy of the request and response will be retained.

### Complaints

Complaints must be made in writing and addressed to the Data Controller. Where the complainant is a third party, and the complaint or enquiry relates to someone else, the written consent of the individual is required. All complaints will be acknowledged within 7 days and a written response issued within 21 days.

Signature:  \_\_\_\_\_

Date: 27/09/2019

Name: Mike McGuire

Job Title: Director