# CCTV Policy

The monitoring, recording, holding and processing of images of distinguishable individuals constitutes personal data as defined by the Data Protection Act (1998). This Policy is intended to ensure that in its use of Closed Circuit Television (CCTV) Charles White LTD is fully compliant with the requirements of the Data Protection Act (1998).

**1. Responsibility**

Responsibility for implementing and monitoring the Charles White LTD CCTV Data Protection Policy sits with the CCTV Data Controller. The CCTV Data Controller is Envision Intelligent Solutions. Responsibility for the day-to-day management and use of authorised CCTV systems is delegated by the Data Controller to appropriately designated staff. Other GDPR responsibilities, out with the monitoring and management of CCTV, will remain with the Charles White Ltd, in house Data Controller.

**CCTV Data Controller;** Envision Intelligent Solutions, Innovation House, Silverwood Business Park, Craigavon BT66 6SY. **ICO number;** Z2972974.

This policy applies to CCTV installations which are managed and monitored by Envision and administered through Charles White Ltd. Neither Envision, nor Charles White Ltd, are able to accept the responsibility of Data Controller, or Data Processor under GDPR, for stand alone installations which are not managed and monitored through Envision.

**2. Purpose**

CCTV systems are employed on developments managed by Charles White LTD for the following specific purposes only:

- To deter and detect crime, including theft and criminal damage in the development common areas
- To enhance the safety and well-being of residents, visitors and members of the public within the development common areas.

Where, in carrying out these purposes, images are obtained of persons committing acts of an illegal nature
and/or acts which breach Charles White LTD policies and procedures, these may be used as evidence.

**3. Installation & Maintenance**

Charles White LTD installation of CCTV systems must comply with the following guidelines:

- Cameras are not hidden from view and are sited in such a way as to ensure that they only monitor spaces intended to be covered
- Signs are displayed so that everyone is aware that they are entering a premises that is covered by surveillance equipment
- Signs indicate the purposes for which cameras are installed
- The CCTV system is located in a locked cabinet in a secure area. Access to this cabinet is controlled by the CCTV Data Controller. Remote access is restricted to Envision as the CCTV Data Controller.
- Maintenance of the CCTV system will be carried out periodically by a party approved by the CCTV Data Controller.

**4. Processing Data**

Access to, and disclosure of, images is restricted and carefully controlled, in order to safeguard the rights of individuals and also to ensure that evidence remains intact should the images be required for evidential purposes. This will be controlled by the CCTV Data Controller. Members of the Charles White LTD team

are considered authorised staff for the purposes of accessing and disclosure of CCTV images when provided by Envision. This will be done under the strict guidance of the CCTV Data Controller. As the CCTV Data Controller under this policy, Envision will have the following responsibilities:

- Restricting access to those staff who need to have access to recorded images for the purpose(s) for which the system was installed
- Make practical arrangements for ensuring that recorded images are viewed only by authorised staff from Charles White LTD and Envision CCTV operating staff only on request of footage to be accessed via Envisions' Alarm Receiving Centre.
- Ensure that the CCTV log records all processing of data
- Maintain a list to the Data Controller (Envision CCTV operators) of staff who have access to recorded images
- At least 2 members of authorized staff must be present when the CCTV images are accessed for the purposes of a Subject Data Request. Details of the search must be written in the CCTV log records.
- Footage will be downloaded remotely and a downlink will be sent to the relevant parties regarding the request.
- A CCTV footage request form must be completed by the requester, signed off by authorised person from Charles White LTD.

Where footage is downloaded and sent to a Charles White Ltd member of staff, that member of staff will be recognised as a Data Processor under the General Data Protection Regulations. Data Processor's will only handle information as directed by the CCTV Data Controller. Charles White Ltd will ensure that information is not copied, stored or shared unless authorised by the CCTV Data controller.

**5. Access**

Residents who seek access to their personal data must submit a Subject Access Request form (QCF999). This form may be submitted through Charles White Ltd. The Data Controller must ensure that:

- All residents have the right to access images of themselves and the conditions under which access may be granted to them and to third parties
- All subject access requests are dealt with by CCTV LTD Data Controller in consultation with the other senior members of staff as appropriate
- Images are not to be disclosed to third parties without the permission of the Data Controller
- All requests from the police for access or disclosure are dealt with according to the principles of the Data Protection Act.
- Repeated subject access requests will incur a processing charge.

**6. Covert Monitoring**

Covert use of CCTV can only take place on the documented authorisation of two Company Directors. For these circumstances to occur, there must be reasonable suspicion that unauthorised or illegal activity is taking place, or is about to take place, or that a suspected breach of Charles White LTD policies and procedures is taking place, or is about to take place. Covert monitoring will be undertaken only for a limited and reasonable period of time consistent with the documented objectives. All decisions relating to the use of covert CCTV will be fully recorded.

**7. Documentation**

The CCTV system must have associated documentation (signage) listing the purposes for which the system has been installed and sited in an area of access to the premises. Documentation must also be available which includes details relating to means of access to images, extent of access, and must log requests to view, viewings themselves, any outcomes, repairs to cameras or re-siting of cameras. Those authorised to view images must provide a signature agreeing to abide by this Policy. The access log for the CCTV system will be reviewed and signed weekly by the CCTV Data Controller.

**8. Monitoring and Review**

This CCTV Policy will be kept under continuous review.