

CCTV Policy – The use of closed circuit television (CCTV) to comply with the GDPR

Version 1: January 2019

1. The images obtained from the system which include recognisable individuals are personal data and are covered by the applicable Data Protection legislation. This Policy should therefore be read in conjunction with the Hornbeam Data Protection Policy.
2. CCTV systems are operated throughout Hornbeam sites, recording dedicated areas defined by a CCTV layout and following a specific 'Brand Standard'.
3. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need. This includes giving confidence to staff and visitors that they are in a safe and secure environment, protecting the integrity of the site by deterring criminals and to provide evidence to assist with the detection and prosecution of criminal offences.
4. When deciding to use CCTV in a certain area Hornbeam must take into account its effect on individuals and their privacy and perform regular reviews to ensure its use remains justified.
5. Hornbeam will be transparent in the use of a surveillance camera system, provide a CCTV notice to publicise a contact point for access to information and complaints in line with our Data Protection Policy.
6. Hornbeam is the Data Controller for the Personal Data captured by our CCTV systems.
7. The CCTV systems which are under Hornbeam's control are managed and operated by the Property Team. The recordings are confidential and available only to those directly connected with operating the system. Copies of recorded information are strictly controlled and only made in relation to incidents under specific restrictions and require the approval described in point 10.
8. The Data Controller will produce and communicate clear rules and procedures with regards to operating, processing and releasing CCTV images.
9. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
10. Access to retained images and information should be referred to info@hornbeamltd.co.uk and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes. And always require previous written approval of the Data Controller.
11. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
12. There should be effective and periodic review mechanisms to ensure legal requirements, policies and standards are complied with in practice and to ensure that the system is working properly and produces the required images.