

## HEGARTY LLP CCTV POLICY – ALL OFFICES

### 1. POLICY STATEMENT

- 1.1 We believe that CCTV has a legitimate role to play in helping to maintain a safe and secure environment for all staff and visitors. However, we recognise that this may raise concerns about the effect on privacy. This policy is intended to address such concerns. Images recorded by CCTV are personal data which must be processed in accordance with data protection laws. We are committed to complying with our legal obligations and ensuring that staff and visitors the legal rights are recognised and respected.
- 1.2 This policy is also intended to assist staff in complying with their own legal obligations when working with personal data. In certain circumstances, misuse of information generated by CCTV could constitute a criminal offence.

### 2. DEFINITIONS

- 2.1 For the purposes of this policy, the following terms have the following meanings:

**CCTV:** means fixed and domed cameras designed to capture and record images of individuals and property.

**Data:** is information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

**Data subjects:** means all living individuals about whom we hold personal information as a result of the operation of our CCTV.

**Personal data:** means data relating to a living individual who can be identified from that data (or other data in our possession). This will include video images of identifiable individuals.

**Data controllers:** are the people who, or organisations which, determine the manner in which any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law. We are the data controller of all personal data used in our business for our own commercial purposes.

**Data users:** are those of our employees whose work involves processing personal data. This will include those whose duties are to operate CCTV cameras to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy and our Privacy Standard.

**Data processors:** any person or organisation that is not a data user (or other employee of a data controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

**Processing:** is any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring personal data to third parties.

### **3. ABOUT THIS POLICY**

- 3.1 We currently use CCTV cameras to view and record individuals internally within our reception and third floor waiting room areas and externally in the car parking areas of our Peterborough Office and internally within meeting room three and externally in the front and rear car parking areas at our Oakham Office. This policy outlines why and how we use CCTV and how we will process data recorded by CCTV cameras to ensure we are data protection compliant.
- 3.2 We recognise that information that we hold about individuals is subject to data protection legislation. Images of individuals recorded by CCTV cameras are personal data and therefore subject to the legislation. We are committed to complying with all our legal obligations and seek to comply with best practice suggestions from the Information Commissioner's Office (ICO).
- 3.3 This policy covers all employees, directors, officers, consultants, contractors, freelancers, volunteers, interns, casual workers and agency workers and will also be relevant to clients and other visitors to our premises.
- 3.4 This policy will be reviewed when necessary to ensure that it meets all relevant requirements and industry standards.

### **4. PERSONNEL RESPONSIBLE**

Our Data Protection Lead, Sean Rowcliffe (DPL) has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy.

### **5. REASONS FOR THE USE OF CCTV**

- 5.1 We currently use CCTV on and around our premises as outlined below. We believe that such use is necessary for legitimate business purposes, including:
  - 5.1.1 to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
  - 5.1.2 for the personal safety of staff, clients, visitors and other members of the public and to act as a deterrent against crime;
  - 5.1.3 to support law enforcement bodies in the prevention, detection and prosecution of crime; and
  - 5.1.4 to assist in day-to-day management, including ensuring the health and safety of staff and others.

5.2 This list is not exhaustive and other purposes may be or become relevant.

### **6. MONITORING**

- 6.1 CCTV monitors the exterior of the building within the car park area 24 hours a day and is motion sensitive. Data is recorded once the CCTV cameras have been activated.

- 6.2 Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring.
- 6.3 CCTV will not be used to record sound.
- 6.4 Images are monitored by authorised personnel normally during working hours unless specific monitoring is necessary for crime detection/health and safety purposes.
- 6.5 Where necessary, staff using CCTV will receive appropriate training to ensure they understand and observe the legal requirements related to processing data.

## **7. HOW WE WILL OPERATE ANY CCTV**

- 7.1 Where CCTV cameras are placed, we will ensure that signs are displayed to alert individuals that their image may be recorded.
- 7.2 Live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such data. Recorded images will only be viewed in designated, secure offices.

## **8. USE OF DATA GATHERED BY CCTV**

- 8.1 In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the data, where it is possible to do so.
- 8.2 We may store video footage using a cloud computing system. We will take all reasonable steps to ensure that any cloud service provider maintains the security of our information, in accordance with industry standards.
- 8.3 We may engage data processors to process data on our behalf. We will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data.

## **9. RETENTION AND ERASURE OF DATA GATHERED BY CCTV**

- 9.1 Data recorded by the CCTV system will be stored [digitally using a cloud computing system]. Data from CCTV cameras will not be retained indefinitely but will be permanently deleted once there is no reason to retain the recorded information. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded. For example, where images are being recorded for crime prevention purposes, data will be kept long enough only for incidents to come to light. [In all other cases, recorded images will be kept for no longer than 90 days. We will maintain a comprehensive log of when data is deleted.
- 9.2 At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

## **10. REQUESTS FOR DISCLOSURE**

- 10.1 No images from our CCTV cameras will be disclosed to any other third party, without express permission being given by the DPL. Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.
- 10.2 In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.
- 10.3 We will maintain a record of all disclosures of CCTV footage.
- 10.4 No images from CCTV will ever be posted online or disclosed to the media.

## **11. SUBJECT ACCESS REQUESTS**

- 11.1 Data subjects may make a request for disclosure of their personal information and this may include CCTV images (**data subject access request**). A data subject access request is subject to the statutory conditions from time to time in place and should be made in writing, in accordance with our Privacy Policy available on request.
- 11.2 In order for us to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual. We reserve the right to obscure images of third parties when disclosing CCTV data as part of a subject access request, where we consider it necessary to do so.

## **12. COMPLAINTS**

If anyone has any questions about this policy or any concerns about our use of CCTV, please contact the DPL in the first instance.

## **13. REQUESTS TO PREVENT PROCESSING**

We recognise that, in rare circumstances, individuals may have a legal right to object to processing and in certain circumstances to prevent automated decision making (see Articles 21 and 22 of the General Data Protection Regulation). For further information regarding this, please contact the DPL.