CCTV POLICY

INTRODUCTION

CCTV is operated by Birketts LLP at our premises: Providence House, 141-145 Princes St, Ipswich, IP1 1QJ and Brierly Place, 160-162 New London Road, Chelmsford, CM2 0AP

1. POLICY STATEMENT

We believe that CCTV and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our staff and visitors. However, we recognise that this may raise concerns about the effect on individuals and their privacy. This policy is intended to address such concerns. Images recorded by surveillance systems 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 the legal rights of staff, relating to their personal data, are recognised and respected.

This policy is 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 or other surveillance systems could constitute a criminal offence.

2. DEFINITIONS

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 (or other surveillance systems).

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 and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy and our General Data Protection Policy.

Data processors: are any persons 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. GENERAL

The building manager at each location is responsible for the operation of the system.

3.1 We currently use CCTV cameras to view and record individuals on [and around] our premises. This policy outlines why we use CCTV, how we will use CCTV and how we will process data recorded by CCTV cameras to ensure we are compliant with data protection law and best practice. This policy also explains how to make a subject access request in respect of personal data created by CCTV.

3.2 We recognise that information that we hold about individuals is subject to data protection legislation. The images of individuals recorded by CCTV cameras in the workplace 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 and may also be relevant to visiting members of the public. The policy will be regularly reviewed to ensure it meets legal requirements, relevant guidance by the ICO and industry standards.

3.4 The system and any images recorded are securely stored, where only a limited number of individuals have access to a secure server.

3.5 The cameras have been placed in external and internal common areas only, not in individual offices or toilet and bathroom areas. Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras will not focus on private homes, gardens or other areas of private property.

3.6 For security purposes, the CCTV may be viewed over a fixed IP address by designated individuals to ensure the safety of persons entering the building out of hours, if they are called out for any reason.

3.7 The systems selected have been provided by ADT and Chubb, who have provided us with advice on a suitable system for our purpose and which also meets our insurers' requirements.

3.8 Where we are located in a multi occupied building we will ensure the management company operates a suitable CCTV policy under current data protection legislation.

4. IMAGE HANDLING, STORING AND VIEWING

4.1 Conversations are not recorded.

4.2 The screens in reception display the external area cameras only. The screen (Ipswich only) located in the back office has a split screen and displays the images from the other common area cameras to provide assurance and safeguard against unauthorised personnel on the premises.

4.3 Copies of the data recorded can be downloaded to a PC and or memory stick if required by a law enforcement agency in support of a crime and investigation. This is the **only** time that copies will be taken.

4.4 Recorded images will only be viewed by designated individuals.

5. DISCLOSURE

5.1 We will only disclose images from CCTV for our purposes of prevention and detection of crime to law enforcement agencies, where a crime needs to be investigated. In no other instances will disclosure be made.

5.2 Those handling requests for disclosure must obtain confirmation from the risk and compliance team. All disclosures will be recorded centrally.

6. RETENTION

6.1 Images will not be kept for longer than 30 days (Unless required for an investigation into a crime).

6.2 The images are held on a digital video recorder which automatically overwrites the images after 30 days.

6.3 Regular checks are undertaken to ensure the retention period is being complied with.

7. RESPONSIBILITIES

7.1 Signs are displayed at the entrance and all staffs and visitors are aware that CCTV is in operation.

7.2 The signs are clear and visible and they contain our details and who to contact if required.

8. SUBJECT ACCESS REQUESTS

8.1 Individuals requesting a copy of their images may do so by making a subject access request under the Data Protection Regulations to The Data Protection Officer, Providence House, 141-145 Princes St, Ipswich, IP1 1QJ.

8.2 The firm reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

8.3 An individual making a subject access request must provide details which allow us to identify them as the subject of the images and to locate the images on the system. Details of the date and time will be needed, and we may request a photograph of the individual to assist us. Images will be copied onto a USB device or equivalent.

8.4 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.

8.5 Unless the request is subject to exclusion under the General Data Protection Regulation, we will provide the requested information within one month of receiving the request.

8.6 We may not be able to release security images if by doing so we would be breaching the data privacy rights of a third party whose image has been captured at the same time. In such cases we will consider alternative solutions, such as blurring the other party's images, but if this is not possible, we may be unable to comply with the request.

8.7 A central log is kept to show those requests received and how they have been dealt with.

9. MONITORING COMPLIANCE

9.1 The Risk & Compliance Director will ensure the standards are set, procedures are in place and they comply with the code and legal obligations.

9.2 Checks will be made on an annual basis to ensure compliance and an annual review of the policy will be undertaken to review the system's effectiveness.

9.3 A checklist is completed, annually for all policy reviews, to evidence this and is retained by the Risk & Compliance Director. For further information refer to the CCTV code of practice, which can be found at www.ico.org.uk.

24 October 2018