CCTV Policy

Scope

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

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 employees and visitors to our premises, as well as helping to protect Firm property. However, we recognise that this may raise concerns about the effect on individuals and their privacy.

The images of individuals recorded by our CCTV cameras are personal data and therefore subject to data protection legislation. This policy is intended to address any privacy concerns individuals may have. It outlines why we use CCTV, where we use it 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. It covers all those working in Birketts' offices within scope and may also be relevant to visiting members of the public. The policy will be reviewed regularly to ensure it meets legal requirements, relevant guidance issued by the ICO, and industry standards.

This policy is also intended to help employees comply 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.

In this policy "employee" includes workers, contractors, self-employed consultants and agency workers.

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 controllers	are the people who, or organisations which, determine the way any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law;

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.
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;
Processing	means 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.

General

Images recorded by surveillance systems are personal data which must be processed in accordance with data protection laws. Birketts LLP are the data controller in respect of such data. We are committed to complying with our legal obligations and ensuring that the legal rights of individuals relating to their personal data are recognised and respected.

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

Where we are located in a multi occupied building with CCTV we will ensure the management company operates a suitable CCTV policy which is compliant with current data protection legislation.

Why and where we use CCTV

We currently use CCTV cameras to view and record individuals on and around our premises for the purpose of prevention and detection of crime, to monitor health and safety (including the safety of persons entering the building out of hours) and to protect Firm property.

Cameras are placed in internal and external common areas only (for example, communal landings, lift lobbies, reception areas, entrances, exits and car parking areas). Cameras are not placed 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.

Signs are displayed at the building entrances to ensure that everyone is aware that CCTV is in operation. The signs are clear and visible and contain our details and who to contact if required.

Image handling, storing and viewing

The screens in our reception areas display 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 areas cameras to provide assurance and safeguard against unauthorised personnel on the premises.

Copies of the recorded data can be downloaded to a PC and/or memory stick. Copies will only be made if required by a law enforcement agency in support of a crime and investigation, or in response to a subject access request, and not at any other time.

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

The system and any images recorded are securely stored, with only a limited number of Data users having access to a secure server. Recorded images will only be viewed by designated Data users. Conversations are not recorded.

Disclosure

We will only disclose images from CCTV to law enforcements agencies where a crime needs to be investigated or in response to a subject access request. In no other instances will disclosure be made.

Those handling requests for disclosure must obtain prior confirmation from the Risk & Compliance Team. All disclosures will be recorded centrally.

Retention of data

Images are held on a digital video recorder which automatically overwrites the images after 30 days. Images will not be kept for longer than 30 days unless required for an investigation into a crime. Regular checks are undertaken to ensure the retention period is being complied with.

Responsibilities and training

The building manager at each location is responsible for the operation of the system. Training for designated Data users is provided by the relevant installer/supplier.

Data users must at all times protect the data they handle in accordance with this policy, our Data Protection Policy, and as may be advised separately from time to time. We take compliance with this policy very seriously. Failure to do so may lead to disciplinary action under our procedures.

Subject access requests

Individuals requesting a copy of the data/images caught by our CCTV system may do so by making a subject access request to our Data Protection Officer, Sarah Ralph, by email at sarah-ralph@birketts.co.uk or by post to Providence House 141-145 Princess Street.

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.

Any 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. This will include dates and times and we may request a photograph to assist us. Images will be copied onto a USB device or equivalent.

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.

Unless the request is subject to exclusion under the UK GDPR, we will provide the requested information within one month of receiving the request.

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 image, but if this is not possible we may be unable to comply with the request.

Details of requests received and how they have been dealt with are recorded in a central log.

Monitoring compliance

The Risk & Compliance Director will ensure the standards are set and procedures are in place which comply with ICO guidance and legal obligations.

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.