The Burrows Cei Bach CCTV Policy

Version 1.1 (March 2024)

CCTV Policy

1. POLICY STATEMENT

1.1 We have assessed that security cameras, Closed-Circuit Television (**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 and audio 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 our visitors and staff, relating to their personal data, are recognised and respected.

2. DEFINITIONS

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

CCTV	fixed and domed cameras, smart doorbells, and any other recording equipment designed to capture and record images and audio of individuals and property.
Data	information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images with audio. It may also include static pictures such as printed screen shots.
Data subjects	all living individuals about whom we hold personal information as a result of the operation of our CCTV (or other surveillance systems).
Personal data	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	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	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 Privacy Policy.

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	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.
Surveillance systems	any devices or systems designed to monitor or record images and/or audio of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as body worn cameras, unmanned aerial systems, smart doorbells and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

3. ABOUT THIS POLICY

3.1 We currently use CCTV on and around our Property. This policy outlines why we use CCTV on our Property, 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 guests and visitors of the Property, our staff and contractors. It may also be relevant to visiting members of the public.

3.4 The policy will be regularly reviewed to ensure that it meets legal requirements, relevant guidance published by the ICO and industry standards.

4. PERSONNEL RESPONSIBLE

4.1 Michelle Romdhani has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy. Day-to-day management responsibility for deciding what information is recorded, how it will be used and to whom it may be disclosed has been delegated to on site managerial staff.

5. REASONS FOR THE USE OF CCTV

5.1 We currently use CCTV around our site 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 guests, staff, 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;

5.1.4 to assist in day-to-day management, including ensuring the health and safety of guests, staff and others;

5.1.5 in relation to employees and workers, to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings; and

5.1.6 to assist in the defence of any civil litigation, including employment tribunal proceedings.

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

6. MONITORING

6.1 CCTV monitors areas within the boundary of the Property 24 hours a day and this data is continuously recorded**.**

6.2 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 only cover entry and exit points, communal and public areas of the Property and will not focus on private spaces which are to be enjoyed by guests. Under no circumstances shall CCTV be installed in, or otherwise focus on, toilets, shower facilities, swimming pool areas, hot tubs, changing rooms, bedrooms or private offices or staff resting areas.

7. HOW WE WILL OPERATE ANY CCTV

7.1 Where CCTV cameras are placed at the Property, we will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their image may be recorded. The surveillance zone is the area that the CCTV covers only, not necessarily the whole property. Such signs will contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact for further information, where these things are not obvious to those being monitored.

7.2 Live feeds from CCTV cameras will only be monitored where this is reasonably necessary, for example to protect health and safety.

7.3 We will ensure that 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. This may include HR staff involved with disciplinary or grievance matters.

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 Given the large amount of data generated by surveillance systems, 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 will not be retained indefinitely but will be permanently deleted once there is no reason to retain the recorded information. Exactly how long that data will be retained for will vary according to the purpose for which they are being recorded. For example, where recordings are for the purpose of crime prevention purposes, data will be kept long enough only for incidents to come to light. We will maintain a comprehensive log of when data is deleted outside of our usual retention schedules.

9.2 At the end of their useful life, data in all formats 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. USE OF ADDITIONAL SURVEILLANCE SYSTEMS

10.1 Prior to introducing any new surveillance system, we will carefully consider if they are appropriate by carrying out a privacy impact assessment (PIA).

10.2 A PIA is intended to assist us in deciding whether new surveillance systems are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

10.3 Any PIA will consider the nature of the problem that we are seeking to address at that time and whether the surveillance is likely to be an effective solution, or whether a better solution exists. In particular, we will consider the effect a surveillance system

will have on individuals and therefore whether its use is a proportionate response to the problem identified.

10.4 No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in changing rooms) unless, in very exceptional circumstances, it is judged by us to be necessary to deal with very serious concerns.

11. COVERT MONITORING

11.1 We will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

11.2 In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of Michelle Romdhani. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent workers or customers will always be a primary consideration in reaching any such decision.

11.3 Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

12. ONGOING REVIEW OF CCTV USE

12.1 We will ensure that the ongoing use of existing CCTV cameras at the Property is reviewed periodically to ensure that their use remains necessary and appropriate, and that any surveillance system is continuing to address the needs that justified its introduction.

13. REQUESTS FOR DISCLOSURE

13.1 We may share data with other group companies and other associated companies or organisations, for example shared services partners where we consider that this is reasonably necessary for any of the legitimate purposes set out above in paragraph 5.

13.2 No recordings from our CCTV will be disclosed to any other third party, without express permission being given by Michelle Romdhani. Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.

13.3 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.

13.4 We will maintain a record of all disclosures of CCTV footage.

13.5 No CCTV footage will ever be posted online or disclosed to the media.

14. SUBJECT ACCESS REQUESTS

14.1 Data subjects may make a request for disclosure of their personal information and this may include CCTV images and, if captured, audio (data subject access request) in accordance with our Privacy Policy.

14.2 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.

14.3 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.

15. COMPLAINTS

15.1 If you have questions about this policy or any concerns about our use of CCTV, then they should speak to Michelle Romdhani in the first instance.

16. REQUESTS TO PREVENT PROCESSING

16.1 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 UK General Data Protection Regulation). For further information regarding this, please contact Michelle Romdhani.