CCTV Policy - Lennox House

CONTENTS

CLAUSE

1. Policy Statement

1.1 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 following data protection laws. We are committed to complying with our legal obligations and ensuring that the legal rights of staff, relating to their data, are recognised and respected.

1.2 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

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

- **CCTV:** Fixed and domed cameras designed to capture and record images 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. It may also include static pictures such as printed screenshots.

CCTV Policy - Lennox House

- **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.
- **Controllers:** The people 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 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.
- **Data Processors:** Any person or organisation that is not a data user (or other employee of a 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 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 automatic number plate recognition (ANPR), body-worn cameras, unmanned aerial systems 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 cameras to view and record individuals on and around our premises. In particular, CCTV covers our entrances, sides of the building, yard, store and gaming areas (including private RPG Room), and internal office/store room areas. 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 practices. 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, directors, officers, consultants, contractors, freelancers, volunteers, interns, casual workers, zero-hours workers and agency workers and may also be relevant to visiting members of the public.

3.4 This policy is non-contractual and does not form part of the terms and conditions of any employment or other contract. We may amend this policy at any time without consultation. The policy will be regularly reviewed to ensure that it meets legal requirements, relevant guidance published by the ICO and industry standards.

3.5 A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

4. Personnel Responsible

4.1 The directors have 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 Robert Powell, Director. Day-to-day operational responsibility for CCTV cameras and the storage of data recorded is the responsibility of Robert Powell, Director.

4.2 Responsibility for keeping this policy up to date has been delegated to Robert Powell, Director.

5. Reasons for the Use of CCTV

5.1 We currently use CCTV in our entrances, yard and internal factory areas (not including the offices) as outlined below. We believe that such use is necessary for legitimate business purposes, including:

(a) To prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime. (b) For the personal safety of staff, visitors, customers, trade professionals and other members of the public and to act as a deterrent against crime. (c) To support law enforcement bodies in the prevention, detection and prosecution of crime, within safely documented and policy regards. (d) To assist in day-to-day management, including ensuring the health and safety of staff and others. (e) To assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings. (f) To assist in the defence of any civil litigation, including store theft, damage to private property, and employment tribunal proceedings.

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

6. Monitoring

CCTV Policy - Lennox House

6.1 CCTV monitors our entrances, yard, internal store areas, access ways, access points, fire doors, and passageways 24 hours a day, with this data continuously recorded to ensure comprehensive coverage.

6.2 Our camera locations are strategically selected to focus solely on areas relevant to the legitimate purposes of our monitoring. As far as practically possible, CCTV cameras will not be directed towards private homes, gardens, other private properties, or areas of privacy such as toilet facilities. Cameras are also not aimed into serviced let offices, though some overlap with door access may occur. Publicly accessible areas, including meeting rooms (when not booked), hot desks, kitchen areas, stairways, and chillout areas, are monitored to ensure security and safety.

6.3 Surveillance systems may be used to record sound.

6.4 Images are monitored by authorised personnel usually during working hours but may be monitored 24 hours a day, every day of the year.

6.5 Staff using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

6.6 Where CCTV cameras are placed in the workplace, we will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their images may be recorded. Such signs will contain details of the organisation operating the system, the purpose of using the surveillance system, and who to contact for further information, where these things are not obvious to those being monitored.

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

6.8 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, under the authority of the Data Controller - Robert Powell. Recorded images will only be viewed in designated, secure offices.

6.8b While our primary use of CCTV is for security purposes, we may occasionally stream events such as tabletop gaming, concerts, music events, banquets, special occasions, training sessions, festivals, tutorials, courses, and similar activities. These live streams may be broadcast on platforms such as Facebook and YouTube. Details regarding the live streaming setup include:

- The specific platform where the live stream will take place (e.g., Facebook, YouTube).
- Any restrictions on third-party embedding of the stream.
- The page or profile on which the stream will be broadcast.

- How the event will be advertised on the stream, including details about teams, venue, and participant names.
- Who will monitor the stream and for what purpose?
- The scheduled start and end times of the live stream.
- Post-stream information on where the footage may be published and/or stored.
- The storage location of consent forms.
- The process for individuals to withdraw their consent if they wish to do so.

These activities and the use of cameras for live streaming are governed by our Live Streaming Policy, which can be found separately. The CCTV policy remains dedicated solely to the safety and security of the building and its occupants.

7. Use of Data Gathered by CCTV

7.1 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.

7.2 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.

8. Retention and Erasure of Data Gathered by CCTV

8.1 Data recorded by the CCTV system will be stored on a local server. 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 21 days. We will maintain a comprehensive digital log of when data is deleted.

8.2 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.

9. Use of Additional Surveillance Systems

9.1 Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location, we will carefully consider if they are appropriate by carrying out a privacy impact assessment (PIA).

9.2 A PIA is intended to assist us in deciding whether new surveillance cameras 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. Any PIA will consider the nature of the problem that we are seeking to address and whether the surveillance system will be a justified and effective solution. It will also consider the effect that its use may have on individuals and whether better solutions exist which do not involve invasion of privacy.

10. Ongoing Review of CCTV Use

10.1 We will ensure that the ongoing use of existing CCTV cameras in the workplace is reviewed periodically to ensure that their use remains necessary and appropriate and that any legal requirements are met.

10.2 Regular audits will be conducted to ensure that the use of CCTV remains justified. These audits will include reviews of ongoing needs for the cameras and assessments of their performance.

11. Requests for Disclosure

11.1 Data gathered by CCTV will be retained for 31 days, except where the data is required for a specific incident. Disclosure of such data will be controlled and consistent with the purpose for which the system was established.

11.2 Disclosure of data gathered by CCTV will only take place in compliance with this policy and will be limited to:

- The police and other law enforcement agencies where the images recorded would assist in a specific criminal enquiry;
- Prosecution agencies, such as the Crown Prosecution Service (CPS);
- Relevant legal representatives of data subjects;
- Individuals whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings);
- Line managers or supervisory staff (in exceptional circumstances and where they have a legitimate need).

11.3 All requests for disclosure should be documented. If disclosure is denied, the reason should be recorded. Disclosures should be made by Robert Powell, Director, or any authorised personnel.

12. Subject Access Requests

12.1 Data subjects may make a request for disclosure of their personal data under data protection legislation. If you wish to make a subject access request, you should make the request in writing to Robert Powell, Director. Forms are available for this purpose.

12.2 We may ask for information to verify the identity of the person requesting before any information is disclosed.

12.3 We will respond to subject access requests within one calendar month unless the request is complex, in which case we will respond within three months. There will be no fee for processing such requests unless they are manifestly unfounded or excessive.

13. Complaints

13.1 If you have any concerns or complaints about the use of CCTV, you should contact Robert Powell, Director.

13.2 Complaints will be dealt with by our grievance procedure and may be escalated to the Information Commissioner's Office (ICO) if necessary.

14. Requests to Prevent Processing

14.1 Data subjects have the right to request the cessation of processing of their data if such processing is causing, or is likely to cause, substantial damage or distress to that individual or another. Any such requests should be made in writing to Robert Powell, Director.

14.2 Requests for the cessation of processing will be considered on a case-by-case basis, and we will endeavour to comply with such requests unless we have legitimate grounds for continuing to process the data.

This policy ensures that our use of CCTV and other surveillance systems is conducted in a manner that respects individuals' privacy while maintaining security and safety. For any further information or guidance, please get in touch with Robert Powell, Director.

Lennox House