DAKOTA
HOTELS

CCTV POLICY

Contents

1. Introduction 2
2. Lawful Processing 2
3. Objectives 2
4. Roles and Responsibilities 2
5. Operation of the System 3
6. CCTV Control / Monitors 3
7. Citing of cameras 4
8. Covert Surveillance 4
9. Notification – Signage 4
10. Storage and Retention of Recorded Images 5
10.1. Storage 5
10.2. Retention 5
10.3. Accessing CCTV footage 6
11. Monitoring and Review 6

1. Introduction

The purpose of this procedure is to provide assistance in the operation, management, and regulation of the CCTV systems in place across Dakota Hospitality Ltd ("**Company**", "**we**", "**us**", and "**our**") and its hotels. These procedures follow the ICO "Code of Practice for Surveillance Cameras and Personal Data' and the Data Protection Act 2018 (DPA) guidelines.

2. Lawful Processing

The Company has a responsibility for the protection of its guests and employee's safety and security in which it utilises CCTV systems, associated monitoring and recording equipment to support these responsibilities.

The use of CCTV, associated images and any sound recordings is covered by the Data Protection Act 2018.

This procedure outlines the use of CCTV and how it complies with the Act, we have considered the privacy issues involved with using surveillance systems and have concluded that their use is necessary and proportionate to the needs we have identified as a business.

3. Objectives

The system compromises of fixed and roaming cameras located externally and internally for the purposes of capturing images.

- Protecting the companies' buildings and assets
- Increasing the safety and security of our guests and employees
- To act as a visual deterrent
- Support the police in a bid to deter and detect crime
- For the protection of our guests and employees.
- Ensure high levels of Health, Safety and food hygiene are being met.

4. Roles and Responsibilities

The Data Protection Officer (DPO) will be responsible for monitoring compliance with these procedures.

All authorised operators and employees with access to CCTV images will be made aware of these procedures prior to access being granted to CCTV systems, all operators have also received training in data protection responsibilities, they have been made aware of:

- How to handle information securely
- How to make a subject access request and where those requests should be submitted to.
- What to do if they receive a request for information from an official authority like the police.

CCTV monitoring in the interests of security will be conducted in an ethical, professional, and legal manner consistent with existing policies including the data protection policy.

Cameras will be used to monitor activities in all areas to identify criminal activity occurring, anticipated or perceived, and for the purpose of securing the safety and wellbeing of our

guests and colleagues. Cameras must not be used for the purposes of monitoring employees unless authorised by HR Director as part of an ongoing investigation with a legitimate reasoning to monitor.

Materials or knowledge secured because of CCTV will not be used for any commercial purpose, Data will only be released for use in the investigation of a specific crime and with written authority of the Police.

The planning and design has endeavoured to ensure that the surveillance scheme will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every single incident taking place in areas of coverage. Some Cameras operate off motion sensors trained on a specific area therefore may not capture events outside the trigger zone.

Warning signs, as required by the ICO Code of practice have been placed at all access routes to areas covered by CCTV.

Information obtained through the CCTV system may only be released when authorised by the Executive or senior team. Subject access requests should be made to gdpr@dakotahotels.co.uk.

Any requests for CCTV recordings / images from the police will be logged by the senior hotel team. If a law enforcement authority is seeking a recording for a specific investigation any such request made should be made in writing to gdpr@dakotahotels.co.uk

5. Operation of the System

- The CCTV system(s) life cycle will be managed by the principles and objectives expressed within these procedures.
- The day-to-day management will be the responsibility of the Hotel Manager who may delegate this to the Duty Manager or Security.
- The CCTV system will be in operation 24 hours a day, 7 days a week.

6. CCTV Control / Monitors

Viewing of live images on monitors is restricted to authorised personnel where it is necessary for them to see it e.g. to monitor public areas for security and health and safety purposes. Viewing of live images where there is an expectation of privacy is not authorised at any time.

Recorded images are reviewed in a restricted area and not shown or disclosed to unauthorised persons.

Access should be provided to authorised personnel based on the level of access to the system they require and to the parts of the system needed to perform their job role.

When playback equipment is not in use, the system should be logged out and computer locked to prevent unauthorised access. It is not acceptable to share log-on credentials with anyone else.

7. Citing of cameras

Cameras are in place in public areas and internal spaces such as offices, which do not intrude on a person's reasonable right to privacy. Cameras in place to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

CCTV video monitoring and recording of public areas may include the following:

- Protection of buildings and property - the building perimeter, entrances and exits.
- Employee-only areas such as offices, storage areas including cellars, high-risk areas for health and safety purposes including kitchens and plant rooms.
- Areas where there is the potential for crime to occur such as high footfall areas and cash handling points.
- Monitor and recording of all public areas including bedroom floors.

The following points were considered when the CCTV cameras were installed:

- Camera locations were chosen carefully to minimise viewing spaces that are not of relevance to the purposes for which we are using CCTV.
- The cameras have been sited to ensure that they can produce images of the right quality, considering their technical capabilities and the environment in which they are placed.
- Cameras are suitable for the location, bearing in mind the light levels and the size of the area to be viewed by each camera.
- We have checked that a fixed camera positioned in winter will not be obscured by the growth of plants and trees in the spring and summer.
- Cameras are sited so that they are secure and protected from vandalism.
- The system will produce images of sufficient size, resolution and frames per second.

8. Covert Surveillance

The Company will only consider covert surveillance in limited circumstances where required for a specific investigation in line with current legislation.

The Company will only undertake covert surveillance where it is needed to obtain evidence for an identified crime or internal investigation. Examples include –

- Gross misconduct has been identified or as part of an on going investigation.
- The need for covert rather than overt monitoring has been assessed and authorised by the Executive Team.
- There is an identified need for law enforcement purposes.

9. Notification – Signage

The Company is required to notify individuals when they are in an area where a surveillance system is in operation. The most effective way of doing this is by using prominently placed signs at the entrance to the surveillance system's zone and reinforcing this with further signs inside the area. Clear and prominent signs are particularly important where the surveillance systems are very discreet, or in locations where people might not expect to be under

surveillance. As a general rule, signs should be more prominent and frequent in areas where people are less likely to expect that they will be monitored by a surveillance system.

Adequate signage will be placed in each hotel to indicate CCTV is in operation. Signs will be clearly visible and readable, and be of an appropriate size (as shown to the right).

10. Storage and Retention of Recorded Images

10.1. Storage

Recorded material will be stored in a way that maintains the integrity of the information on the CCTV systems hard drive. This is to ensure that the rights of individuals recorded by surveillance systems are protected and that the information can be used effectively for its intended purpose.

The system is housed in a secure environment where access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV system is the responsibility of the IT Manager. The IT Manager may delegate the administration of the CCTV System to another employee. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

The Company will keep a record or audit trail showing how the information must be handled if it is likely to be used as evidence in court. Once there is no reason to retain the recorded information, it will be deleted. Exactly when we decide to do this will depend on the purpose for using the surveillance system. A record or audit trail of this process will also be captured.

CCTV images are digitally recorded, it is important that our information can be used by appropriate law enforcement agencies, if its required. In this event, a copy will be made onto a removable drive and handed to the Police.

10.2. Retention

The Data Protection Act 2018 does not prescribe any specific minimum or maximum retention periods which apply to all systems or footage. Rather, retention should reflect the organisation's purposes for recording information. The retention period should be informed by the purpose for which the information is collected and how long it is needed to achieve this purpose.

The Data Protection Acts states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained. Footage may be stored by the Company for up to 90 days in some areas to meet PCI Compliance requirements. Footage may only be kept longer than this specifically in the context of evidence in an accident, incident, investigation, or case. Camera footage that is not extracted is automatically overwritten after the retention period expires.

10.3. Accessing CCTV footage

CCTV footage can only be requested to be shared externally or exported in the following ways:

- Subject access request made via GDPR@dakotahotels.co.uk; or,
- Request made by the Police for footage via email, stating dates and times and area / subject of interest; or,
- Request for footage as part of an internal Compliance or HR investigation.

Once we have disclosed information to another body or party, such as the Police, they become the Data Controller for the copy they hold. It is their responsibility to comply with the DPA in relation to any further disclosures.

Internal procedure for exporting recorded events from CCTV System:

- Authorization is given by a member of the Executive Team or the Hotel Manager.
- Duty Manager, Security, or IT who have been assigned the task to access the system.
- Incident will be reviewed and observed from all possible angles across required time frame.
- Information requested such as times, dates and locations will be made in the form of an incident report which will be shared with the required internal employees.
- Any exported footage will be saved to the isolated computer or drive, and exported to flash drive as necessary.
- Footage may also be uploaded to the Company's compliance extranet if the footage forms part of an accident or H&S investigation in accordance with the Privacy Notice.
- Any footage requested via a subject access request will be reviewed by the Executive Team prior and after any post processing work has been completed to redact any footage in compliance with GDPR regulations.
- For subject access requests, requestor may request to
    - View footage on premises; or,
    - Have footage posted to them on an encrypted USB.

11. Monitoring and Review

Any suspected breaches to this policy must be reported to gdpr@dakotahotels.co.uk

Routine performance and random operating checks will be completed by IT, and these procedures will be regularly reviewed and periodically the Company may opt to have a 3rd party to complete a health check of the system and provide recommendations to improve performance, ensure compliance and ensure the system remains relevant.