Burnham-on-Sea & Highbridge Town Council

Burnham Joint Burial Committee (BJBC)

Closed Circuit Television (CCTV) Policy

Adopted Minute No: 22/18/BJBC

Adopted: September 2018

There is a requirement for this policy to reviewed on annually
Next Review: September 2019

Burnham Joint Burial Committee (BJBC)
Closed Circuit Television (CCTV) Policy

Introduction

The BJBC has in place a CCTV surveillance system installed at Brent Road Cemetery. It was agreed at committee minute no. 38/17/BJBC that this was the most appropriate security measure to put in place. This policy details the purpose, use and management of the CCTV system and details the procedures to be followed in order to ensure that the BJBC complies with the new General Data Protection Regulation (GDPR).

This policy is based upon the guidance issued by the Information Commissioner's Office. The basic legal requirement is to comply with the Data Protection Act itself.

Purpose of the CCTV system

Images are being monitored and recorded for the purposes of prevention, reduction, detection and investigation of crime and other incidents. The CCTV will be used in order to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed. The BJBC seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy.

There is one sign placed at the vehicular entrance in order to inform all visitors that CCTV is in operation, covering the car park area and building and another sign on the building giving the purpose for using CCTV and who to contact about the system.

Monitoring, Recording and Retention

The CCTV system has four cameras. Three of these cameras are covering the car park and one camera is covering the entrances to the garage and office. The CCTV system is recording for 24 hours a day, every day of the year. The information is stored on a hard drive for 10 days and then is automatically deleted. The recorded information is viewed and monitored by the Caretaker in his office which is a secure area i.e. the door is always locked when the Caretaker is not present. Additional staff may be authorised by the Deputy Clerk when necessary to also view and monitor the recorded information.

For the purpose of law enforcement the recording would be transferred to a USB stick.

All requests for disclosure must be put in writing and the access authorised by the Deputy Clerk.

Monitoring Compliance

All staff involved in the operation of the CCTV will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with this policy. This policy will be reviewed annually.

Adopted Minute No: 22/18/BJBC

Date of next review: Sept 2019 See associated Appendix 1, 2 and 3

Appendix 1

The Data Protection Act 1998: data protection principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

(a) at least one of the conditions in Schedule 2 is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix 2

Checklist for users of limited CCTV systems monitoring small retail and business premises

This CCTV system and the images produced by it are controlled by the Deputy Clerk who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1998.
The BJBC have considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of customers. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

	Checked (date)	By	Date of next review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.	12.7.2018	L. Williams Clerk to Committee	Sept 2018
There is a named individual who is responsible for the operation of the system.			
The problem we are trying to address has been clearly defined and installing cameras is the best solution. This decision should be reviewed on a regular basis.			
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.			
Cameras have been sited so that they provide clear images.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, where only a limited			

number of authorised persons may have access to them.			
The recorded images will only be retained long enough for any incident to come to light (eg for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to third parties.			
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.			
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

Appendix 3

The guiding principles of the Surveillance Camera Code of Practice

System operators should adopt the following guiding principles:

- Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

- The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

- There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

- There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

- Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

- No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

- Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

- Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

- There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

- When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

- Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.