Penrith BID | CCTV Policy

Statement of intent

Penrith BID have installed Christmas Lights, including free standing installations into Penrith Town Centre. To ensure they are not damaged or vandalised we have installed a CCTV camera to monitor the town centre

The purpose of this policy is to manage and regulate the use of the CCTV system and ensure that:

• We comply with the GDPR, effective 25 May 2018. • The images that are captured are useable for the purposes we require them for. • We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation. This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

Taking action to prevent a crime • Using images of individuals that could affect their privacy

1. Legal framework

1.1. This policy has due regard to legislation including, but not limited to, the following:

• The Regulation of Investigatory Powers Act 2000 • The Protection of Freedoms Act 2012 • The General Data Protection Regulation • The Freedom of Information Act 2000 • The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 • The Equality Act 2010

1.2. This policy has been created with regard to the following statutory and nonstatutory guidance:

• Home Office (2013) 'The Surveillance Camera Code of Practice' • ICO (2017) 'Overview of the General Data Protection Regulation (GDPR)' • ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now' • ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'

2. Definitions

2.1. For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

• Surveillance – monitoring the movements and behaviour of individuals; this can include video, audio or live footage.

• Overt surveillance – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.

• Covert surveillance – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance. 2.2. Penrith BID does not condone the use of covert surveillance when monitoring the general public. Covert surveillance will only be operable in extreme circumstances.

2.3. Any overt surveillance footage will be clearly signposted around the angels.

3. Roles and responsibilities

3.1. The role of the data protection officer (DPO) includes:

3.2. Penrith B.I.D. Company Ltd as the corporate body, is the data controller. The governing body of BID therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

3.3. The board deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the data controller. 3.4. The role of the data controller includes:

• Processing surveillance and CCTV footage legally and fairly. • Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly. • Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection. • Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary. • Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.

4. Purpose and justification

4.1. The BID will only use surveillance cameras for the safety and security of the town centre Christmas lights installations.

4.2. Surveillance will be used as a deterrent for vandalism.

4.3. The BID will only conduct surveillance as a deterrent.

5. The data protection principles

5.1. Data collected from surveillance and CCTV will be:

• Processed lawfully, fairly and in a transparent manner in relation to individuals. • Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes. • Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. • Accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. • Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals. • Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6. Objectives

6.1. The surveillance system will be used to:

Deter criminal acts against property. • Assist the police in identifying persons who have committed an offence.

7. Protocols

7.1. The surveillance system will be registered with the ICO in line with data protection legislation. It is located on The George Hotel and forms part of their system.

7.2. The surveillance system is a closed digital system.

7.3. Warning signs have been placed where the surveillance system is active, as mandated by the ICO's Code of Practice.

7.5. The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

8. Security

8.1. Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

8.2. If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained.

8.3. Surveillance and CCTV systems will be tested for security flaws termly to ensure that they are being properly maintained at all times.

8.4. Surveillance and CCTV systems will not be intrusive.

8.5. Any unnecessary footage captured will be securely deleted from the system.

8.6 If the camera present faults will be repaired immediately as to avoid any risk of a data breach.

9. Privacy by design

9.1. The BID will ensure that the installation of the surveillance and CCTV systems will always justify its means.

10. Code of practice

10.1. The BID understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

10.2. CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

10.3. All surveillance footage will be kept for 1month for security purposes; the director in charge is responsible for keeping the records secure and allowing access.

10.5. The BID has a surveillance system for the purpose of the prevention and detection of crime

10.6. The surveillance and CCTV system is owned by the BID and images from the system are strictly controlled and monitored by authorised personnel only.

11. Access

11.1. Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

11.2. All disks containing images belong to, and remain the property of, the BID.

11.3. Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing.

11.4. The BID will verify the identity of the person making the request before any information is supplied.

11.5. A copy of the information will be supplied to the individual free of charge; however, the BID may impose a 'reasonable fee' to comply with requests for further copies of the same information.

11.6. Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.

11.7. Requests by persons outside the BID for viewing or copying disks, or obtaining digital recordings, will be assessed by the director, on a case-by-case basis with close regard to data protection and freedom of information legislation.

11.8. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

11.9. All fees will be based on the administrative cost of providing the information.

11.10. All requests will be responded to without delay and at the latest, within one month of receipt.

11.11. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

11.12. Where a request is manifestly unfounded or excessive, the BID holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

11.13. In the event that a large quantity of information is being processed about an individual, the BID will ask the individual to specify the information the request is in relation to.

11.14. It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

11.15. Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

• The police – where the images recorded would assist in a specific criminal inquiry • Prosecution agencies – such as the Crown Prosecution Service (CPS) • Relevant legal representatives – such as lawyers and barristers • Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

11.16. Requests for access or disclosure will be recorded and the director will make the final decision as to whether recorded images may be released to persons other than the police.

12. Monitoring and review

12.1. This policy will be monitored and reviewed every two years by the directors.

12.2. The Chair will be responsible for monitoring any changes to legislation that may affect this policy, and make the appropriate changes accordingly.

12.4. The scheduled review date for this policy is November 2021.