CCTV Code of Practice 2023-24

Last review date	11/02/2020	Martin Hill
	27/02/2020	Approved by (Name) Michele Sarginson
Reviewed	02/04/2023	Martin Hill
	03/04/2023	Approved by Michele Sarginson

Contents

1. Introduction

The purpose of this code is to regulate the management, operation and use of the closed circuit television (CCTV) system at Aldern House, Peak District National Park hereafter referred to as 'PDNP'. The system comprises of a number of static and mobile cameras located around the PDNP site. The system is in use both externally at our car parks and internally in the following meeting rooms: Conference, Garden and Library along with the three interview rooms.

The use of CCTV has been considered in line with the following legislation; the Human Rights Act, the Regulation of Investigatory Powers Act 2000 (RIPA) and the General Data Protection Regulation 2016 and the UK Data Protection Act 2018.

The PDNPA are the data controller for the personal data contained in recorded footage. We are registered with the Information Commissioners Office (ICO), our registration number is Z7027992.

This policy and guidance follows the recommendations and principles set out in the ICO CCTV Code of Practice and the Surveillance Camera Code of Practice (updated 2022) issued by the Home Office.

2. Purpose of the CCTV scheme

- To protect PDNP buildings and their assets during and outside normal office hours
- To increase personal safety for staff, tenants, visitors and contractors
- To protect members of the public,staff and tenants when using designated meeting rooms
- To be a visible aid in crime prevention
- To assist in identifying, apprehending and prosecuting offenders.

3. Statement of intent

CCTV Cameras will be used to monitor activities within the PDNP, its car parks and other public areas to identify criminal acts in progress, anticipated, or perceived, and for securing the safety and wellbeing of PDNP staff, together with its visitors.

In planning and designing the system we have endeavoured to ensure that the scheme will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every single incident that might occur in the areas of coverage.

Materials or knowledge secured from the use of CCTV will not be used for commercial purposes. Backup and media copies may be released to the police for specific purposes related to law enforcement. Images may be released to the media, but only under instruction from a law enforcement agency.

4. Operation of the system

The CCTV system is owned by PDNP and designated members of staff have access: the scheme is overseen by the Corporate Property Team Manager, in accordance with the principles and objectives expressed in the code. During working hours the system is managed by the Facilities Manager and Facilities Assistant; out of hours and weekend the system is managed by First County Monitoring who are accredited as part of the National Security Inspectorate (NSI) scheme. PDNP IT Support Officer has access for the purposes of administering the system and providing network maintenance

- The CCTV system is fully operational for 24 hours each day, every day of the year, unless mitigating factors apply.
- Images are not actively monitored but may be reviewed for any of the purposes laid out in Section 2 of this policy
- Cameras sited on Authority premises that also take in neighbouring houses and gardens will have appropriate automatic pixilation to obscure those parts of images which would infringe the privacy of others
- Visitors to site are notified of use of CCTV by appropriate signage
- Live images are screened in the Property Support Team office only and on the personal computers of the designated key holders for the premises. Images from static cameras of the reception area and barrier entrance are displayed in the Customer Support Team office during working hours.
- Images are recorded on a rolling programme of 27 days. Unless required for providing evidence, this retention will automatically overwrite the oldest images.

5. Backup and additional media

In order to maintain and preserve the integrity of the media used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention will be strictly adhered to:

- Backup media will be uniquely identified.
- The controller will register the date and time of media.

- Image quality and checks on the correct operation of the equipment will be carried out by the Facilities Manager/Facilities Assistant on a regular basis
- A recording required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure, evidence store.
- If the recording is archived the reference must be noted and retention periods will apply.

6. Liaison

Liaison meetings may be held with all bodies involved in the support of the system and external agencies whereby there is a legitimate need to share the images recorded from the system and prior approval has been sought by the Corporate Property Team Manager or Facilities Manager.

7. Breaches of the policy (including breaches of security)

Any breach of the policy by PDNP staff will be initially investigated by the Data Protection Officer, who will co-ordinate an appropriate action plan.

8. Assessment of the scheme and code of practice

Performance monitoring, including random operating checks, may be carried out by the Facilities Manager, IT Systems Manager or Data Protection Officer.

9. Complaints

Any complaints about the PDNP's CCTV system should be addressed to the Director of Corporate Strategy and Development. Complaints will be investigated in accordance with Section 7 of this policy.

10. Access to Recordings / Images

Recordings may be viewed by the police and/or authorised officers of the Authority for the prevention and detection of crime upon receipt of appropriate authorisation and consent forms. A record will be maintained of the disclosure of recordings to the police or other authorised applicants and will only be disclosed on the clear understanding that the recording remains the property of PDNP. The PDNP also retains the right to refuse permission for the police to disclose the recording or other information contained within it to a third party

The individuals to whom 'personal data' relates have a right of access to data held about themselves, including those obtained by CCTV. Requests for access should be made by downloading and completing the form which is available on our website by using the following link: Subject Access Request Form. Alternatively a copy can be obtained from our Customer and Business Support Team by calling 01629 816200 or email customer.service@peakdistrict.gov.uk.

Applications received from outside bodies (for example solicitors) to view or release recordings should be referred to the Data Protection Officer. Recordings may be released where satisfactory documentary evidence is produced demonstrating that they are required for legal proceedings, as a verified subject access request or in response to a court order.

Summary of Key Points

- This policy will be reviewed regularly.
- The CCTV system is owned and operated by the PDNP.
- Liaison meetings may be held with the police and other bodies.
- Recordings will be properly indexed, stored and destroyed after appropriate use.
- Recordings may only be viewed by authorised PDNP staff and the police.
- Recordings required as evidence will be properly recorded witnessed and packaged before copies are released to the police.
- Recordings will not be made available to the media for commercial or entertainment.
- Digital storage media will be disposed of securely following the retention periods specified in PDNPs retention and records management policy.
- Any breaches of this code will be reported to and investigated by the Data Protection Officer.
- An independent investigation will be carried out for serious breaches.

Appendix 1 – Checklist for users of limited CCTV systems monitoring

The Authority has 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 visitors to our premises. It will not be used for other purposes. The following have been checked as part of the review process:

- The Authority is registered as a data controller with the ICO.
- The Authority's Corporate Property Team Manager is responsible for the system
- The system in place produces clear images that can be used by law enforcement agencies (usually the police) to investigate crime and these can be easily taken from the system when required
- Cameras have been positioned to avoid capturing the images of persons not visiting the premises
- Cameras have been sited so that they provide clear images
- There are visible signs showing that CCTV is in operation. Signage provides the name of the operator and contact details
- Images are securely stored, where only a limited number of authorised persons may have access to them
- The recorded images are only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated
- Images are not provided to third parties without completion of the appropriate documentation and authorisation.
- The system has been checked to ensure that it is working properly and produces high quality images.

Appendix 2: Log Files

Copied CCTV Images

Date Stored	Who By	ASB Log Number / Crime	Please State Why These Images Have Been Retained	Please State By Which Format These Images Are Being Stored (e.g CD Rom)	Please State The Date The Footage Was Destroyed, By Whom & Why

Appendix 3: 3rd Party Viewing

CCTV: 3rd Party Viewing

Date & Time Of Viewing	Name/s Of The Person/s Viewing The Image & Organisation Represented	State The Reasons For The Viewing	Images Viewed (please state location, date & time of original image/s)	The Outcome, If Any, Of The Viewing	Date & Time The Images Were Returned For Storage

Appendix 4 – 3rd Party Refusal Form

3rd Party Access Refusal Form

Further to your request for access to CCTV images, unfortunately your request has been refused. Details are provided below.

1) Identity of individual making the request:
Full Name:
Address:
Identification provided (if required)

2) Details of the footage requested:

3) Reason/s for refusing the request:

4) Manager's details:
Name:
Signature:
Service/Team:
Date: