

## Report of Performance and Compliance Co-ordinator

---

### **Subject: CCTV Policy**

#### Purpose of the Report

This report seeks approval of the Authority's Closed Circuit Television (CCTV) policy.

#### Introduction

The policy replaces and updates the Authority's site-specific CCTV policies. This is in order to support a more co-ordinated approach to the management of CCTV systems across Authority sites by having one policy.

The purpose of this policy is:

- To ensure the PCNPA's approach to the operation of its CCTV systems at its sites is compliant with the relevant regulations and follows best practice.
- Set out the principles to be observed by PCNPA and its employees, involved in the operation, management and administration of relevant CCTV systems, as well as the hierarchy of responsibility which exists to ensure that these systems are operated in a compliant manner.
- Inform members of the public of the purposes for which CCTV is operated, and of the standards which will be met in relation to it.

The Asset Management Group and staff managing relevant sites have been involved with the development of the policy. The policy review process and creation of CCTV register has supported us to review retention periods and current signage with additional guidance being provided and new bilingual signage template created for site use. The CCTV register will be reviewed annually.

A data protection impact assessment has been carried out on all existing CCTV systems at sites and the policy has been reviewed by the Data Protection Officer. Updated wording for the Authority's privacy notice in terms of CCTV has been drawn up following the data protection impact assessment process.

The policy went to Leadership Team for comment on the 3/5/22, including review by Human Resources Manager.

A separate drone policy is currently being drafted.

## Financial Considerations

Breaches of this policy could lead to external action against the Authority, including the issuing of financial penalties by the Information Commissioner's Office.

## Risk Considerations

There is the potential for financial, safety, legal and reputational impact arising from the effectiveness of complying with surveillance and privacy related legislation.

The inclusion of CCTV register subject to annual review will help the Authority manage risk.

Clear lines of accountability have been included, with clear indication of when officers should seek Data Protection Officer advice or gain authorisation from Senior Management.

Policy indicates that it is a requirement for a data protection impact assessment to be carried out on installation of any future CCTV systems.

## Compliance

This policy plays a central role in ensuring the Authority complies with CCTV, privacy and surveillance legislation and regulations.

## Human Rights/Equality issues

Use of surveillance including CCTV cameras can raise concerns about the effect on individuals and their privacy. This policy is attended to address such concerns.

In doing so the policy takes account of the Human Rights Act 1998, [Surveillance Camera Code of Practice](#) and the 12 guiding principles and the ICO's [A data protection code of practice for surveillance cameras and personal information](#).

PCNPA will ensure its use of CCTV system does not produce unacceptable bias on any relevant ground or characteristic of the individuals whose images might reasonably be expected to be captured by it. PCNPA will take account of its obligations under the Public Sector Equality Duty in terms of its use of CCTV.

The policy sets out how people can complain if they have concerns about CCTV, including the field of vision or the siting of the camera.

Current CCTV systems have been subject to a data protection impact assessment, and the policy sets out when further data protection impact assessments would be needed.

## Welsh Language

CCTV signage will need to comply with Welsh Language Standards.

***Recommendation***

***Members are asked to consider and approve the CCTV Policy***

*(For further information, please contact Mair Thomas, Performance and Compliance Officer)*



## External and Internal

### Review

Version	Effective Date	Document Owner	Review Date Trigger
1		Performance and Compliance Co-ordinator	Every 3 years. Legislative or Organisational Changes. Appendix 1 – CCTV Register to be reviewed annually.

### Target Audience

Staff, Volunteers, Members, Visitors to Sites and General Public

### Consultations

Group	Date
Asset Management Group and Site Managers	February – April 2022
Data Protection Officer	February – May 2022
Leadership Team	3/5/22

### Approvals

This document requires the following approvals.

Approved by	Name	Date	Signature
National Park Authority			

## Contents

1. Policy Statement.....	3
2. Purpose and Scope.....	3
3. Legal Context.....	4
4. Purpose of Use of CCTV.....	4
5. Guiding Principles for Use.....	5
6. Cameras and Area Coverage .....	7
7. Roles and Responsibilities .....	8
8. Subject Access Rights and Sharing Footage.....	11
9. Data Retention.....	12
10 Use of CCTV Footage for Disciplinary Purposes .....	12
11 Complaints and Queries.....	13
12 Definitions .....	13
13 Related Policies and Procedures .....	14
Reference.....	14
Version History .....	14
Appendix 1 – CCTV Register.....	15

## 1. Policy Statement

Pembrokeshire Coast National Park Authority (PCNPA) recognises that Closed Circuit Television (CCTV) has a legitimate role to play in helping to maintain a safe and secure environment for all our staff, Members, volunteers, visitors and members of the public. However, we recognise that this may raise concerns about the effect on individuals and their privacy. This policy is intended to address such concerns. Any recorded images and audio files of individuals by surveillance systems are personal data. This will include, where appropriate other identifiable features, such as vehicle registration plates. PCNPA is committed to complying with our legal obligations and ensuring that the legal rights of staff, Members, volunteers, visitors and members of the public relating to their personal data, are recognised and respected.

The Authority's use of CCTV systems at its sites follows the requirements and principles of the Human Rights Act 1998, the Data Protection Act 2018 and UK General Data Protection Regulation, the Protection of Freedoms Act 2012 and the Surveillance Camera Code of Practice.

This policy is intended to assist staff in complying with legal obligations when working with personal data. In certain circumstances, misuse of information generated by CCTV could constitute a criminal offence.

## 2. Purpose and Scope

2.1 The purpose of this policy is:

- To ensure the PCNPA's approach to the operation of its CCTV systems at its sites is compliant with the relevant regulations and follows best practice.
- Set out the principles to be observed by PCNPA and its employees, involved in the operation, management and administration of relevant CCTV systems, as well as the hierarchy of responsibility which exists to ensure that these systems are operated in a compliant manner.
- Inform members of the public of the purposes for which CCTV is operated, and of the standards which will be met in relation to it.

2.2 This policy covers all overt CCTV systems in operation at PCNPA sites. Vehicle cameras or body cameras are not currently covered by this policy. PCNPA will only use covert cameras in relation to operations authorised to be carried out

under the Regulatory of Investigatory Powers Act 2000 or in exceptional circumstances relating to use for Disciplinary Purposes (see section 10 on Use of CCTV Footage for Disciplinary Purposes). The Authority has a separate Drone Policy in place *[Note: A separate drone policy is currently being drafted]*.

2.3 Definitions of terms used in this policy can be found in section 12.

### 3. Legal Context

3.1 Legislation relevant to this policy includes:

- Data Protection Act 2018 and UK GDPR
- Human Rights Act 1998
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Private Security Industry Act 2001

3.2 PCNPA will also take into account the [Surveillance Camera Code of Practice](#) and its 12 guiding principles. It will also take into account the ICO's [Guidance of Video Surveillance](#).

3.3 PCNPA officers should familiarise themselves in understanding what surveillance activities fall within the scope of the Regulation of Investigatory Powers Act 2000. Overt CCTV is not covered by this Act, but the Act sets out defining boundaries for overt/ covert activities.

### 4. Purpose of Use of CCTV

4.1 PCNPA acts as data controller for the CCTV Systems it operates and is registered with the ICO (Registration number: Z6010336.)

4.2 It is important that everyone and especially those charged with operating the CCTV systems on behalf of PCNPA understand exactly why each of the CCTV systems and cameras have been introduced and what the cameras should and should not be used for. Each CCTV system will have its own site objectives (specific objectives for each site are outlined in Appendix 1 – CCTV Register), these include:

- To protect staff, Members, volunteers, visitors and members of the public with regard to their personal safety

- Deterring violent or aggressive behaviour towards PCNPA staff
- To protect the Authority's buildings and equipment, and the personal property of, staff, Members, volunteers, visitors and members of the public.
- Preventing and detecting crime at its sites and retail facilities and assist in the identification and apprehension of offenders.
- To provide evidence of damage or loss to the Authority's insurance company.

#### 4.3 PCNPA will not use its CCTV:

- For monitoring the activities of PCNPA staff, volunteers, Members, visitors or members of the public in the ordinary course of their lawful business, unless circumstances are such that give rise to particular concerns for that person's safety.
- To intrude into the privacy of any individual unless in pursuit of one of the above authorised uses.
- For purposes of entertainment.
- For commercial purposes.

#### 4.4 PCNPA staff are not permitted to use CCTV systems to observe the working practices and time keeping of other PCNPA staff.

#### 4.5 PCNPA will ensure its use of CCTV system does not produce unacceptable bias on any relevant ground or characteristic of the individuals whose images might reasonably be expected to be captured by it. PCNPA will take account of its obligations under the Public Sector Equality Duty in terms of its use of CCTV.

## 5. Guiding Principles for Use

#### 5.1 The following guiding principles should be followed in relation to the installation of CCTV System and the use and management of data from them:

- **Transparent** – Adequate signage should be placed in prominent positions to inform staff, volunteers, Members, visitors and general public that they are entering a monitored area. Where possible these signs should include information on the presence of CCTV, the purpose for it and contact details for PCNPA as the data controller. PCNPA will notify people of its use of CCTV through its overarching privacy notice on its website.
- **For Legitimate and Specified Purpose** - Use of a CCTV system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need. Prior to establishing any



CCTV installation, it is necessary to establish a legitimate purpose for it. The appropriate balance is needed between the necessity of the CCTV and the privacy rights of individuals. The use of CCTV at a site should be subject to regular reviews to ensure its use remains justified.

- **Proportionate to that purpose** - The usage of CCTV cameras, including the field of vision and whether they can be controlled remotely, has to be proportionate to the identified need. Locations should be selected, that PCNPA reasonably believes require monitoring to address the purposes set out in section 4.
- **Accountability and Auditability** - All existing and proposed CCTV installations should be subject to a Data Protection Impact Assessment to identify what risks to personal data and privacy they pose and what controls can be applied to minimize these. There must be clear responsibility and accountability for all CCTV system activities including images and information collected, held and used. All staff actions which effect the operation of CCTV equipment should be captured in audit logs held on the devices or controlling applications. This includes any actions which change the field of vision, any downloads of footage and any deletion of footage. All CCTV equipment must be specified so as to provide accurate time and date stamping. All CCTV installations will be recorded on PCNPA's CCTV register (Appendix 1 of this policy.)
- **Subject to Senior Management Approval and Oversight** – Proposals to install CCTV must be approved by a member of the Senior Management Team and the Authority's Data Protection Officer. Approval is required prior to the procurement of CCTV equipment.
- **Data Retention and Minimisation** - No more images and information should be stored than that which is strictly required for the stated purpose of a CCTV system, and such images and information should be deleted once their purposes have been discharged. CCTV systems operated by PCNPA shall normally retain footage for no longer than 30 days. Where footage for a site is routinely retained for more than 30 days the reason for this should be outlined in the CCTV register (Appendix 1 of this policy). Where footage is required for the purposes of prosecution of an offence or to defend legal claims, a copy should be made and stored securely for this purpose.
- **Security and Access** - CCTV system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use. Access to retained images and information should be restricted and only accessed by authorised staff in relation to the purposes set out in Section 4. People have a right to request through subject access, a copy of footage in which they are captured, subject to exemptions within

the Data Protection Act 2018. The Authority may also get Freedom of Information Requests relating to footage captured. The police and other authorized agencies or bodies may apply for access to data collected via CCTV in order to carry out their statutory functions. All requests will be reviewed by PCNPA's Data Protection Officer and determined according to a process which ensures compliance with the law.

- **Maintenance and Quality** – PCNPA will consider any operational, technical and competency standards relevant to a CCTV system and its purpose and will work to meet and maintain those standards. Those with day-to-day management responsibility for CCTV will check and confirm on a regular basis that the system is properly recording, that cameras are functioning correctly and quality of footage is sufficient.

## 6. Cameras and Area Coverage

- 6.1 Care is taken to ensure that cameras are sited so that they are clearly visible.
- 6.2 No hidden cameras will be used unless in relation to authorised operations mounted under the Regulatory of Investigatory Powers Act 2000 or in exceptional circumstances relating to use for Disciplinary Purposes (see section 10 on Use of CCTV Footage for Disciplinary Purposes). Cameras shall not be directed in such a way as to amount to surveillance which is intrusive.
- 6.3 Clear signage is in place within the area which is being monitored in order to ensure that both the public are aware when they are in a monitored area and also that the maximum deterrent value is achieved. Signage will comply with Welsh Language Standards.
- 6.4 PCNPA CCTV systems do not record audio. If in the future PCNPA seeks to install CCTV with audio/voice recording any installation will only occur if it has been found to be proportionate following a Data Protection Impact Assessment. If it is found necessary to make voice recordings, signage will reflect this.
- 6.5 Camera positions are reviewed annually to ensure that they remain proportionate to their purpose. Where the purpose can no longer be justified against the intrusion on personal privacy, they will be removed or switched off.
- 6.6 In a limited number of cases camera's pickup in their line of site limited footage outside of PCNPA's boundaries. Where this is the case, it is noted in the CCTV register (Appendix 1). The Authority will monitor and respond to any concerns or

complaints that it receives relating to the positioning of cameras and their field of vision. Where the purpose can no longer be justified against the intrusion on personal privacy or property, they will be removed or switched off.

- 6.7 All viewing equipment shall only be operated by trained and authorised users.
- 6.8 Images will be viewed and/or monitored in a suitably secure and private area to minimise the likelihood of or opportunity for access to unauthorised persons. Access to footage that isn't viewed live is password protected.
- 6.9 Third parties, including community groups using PCNPA facilities will be notified that CCTV is in operation.

## **7. Roles and Responsibilities**

- 7.1 Centre Managers will have day to day management responsibility for CCTV at their sites. Responsibilities include:
  - Ensuring placement of clear and prominent signs at entry points to the CCTV zone and placement of additional within the zone.
  - Notifying third parties, including community groups using centre facilities that CCTV is in operation.
  - The Centre Manager is the staff member appointed to review non live recordings and only then for security purposes and in line with the purposes set out in Section 4. They may delegate this responsibility to the Site Warden where this is appropriate.
  - Ensuring access to footage is password protected.
  - To ensure the screen showing live pictures from CCTV cameras within the centre is restricted from viewing by the general public.
  - To seek approval from PCNPA's Data Protection Officer before showing footage, copying and sharing any data with internal and external third parties.
  - To contact PCNPA's Data Protection Officer if a subject access or freedom of information request from a staff, volunteer, visitor or member of the Public is received in relation to viewing and accessing footage captured by CCTV system.
  - Ensuring staff know what to do if a member of the public makes an enquiry about the CCTV system.
  - Ensuring that a data protection impact assessment has been completed for all CCTV systems on their site.
  - Ensuring the details of CCTV systems at their site is correctly recorded on the CCTV register (Appendix 1 of this document).

- Regularly checking that the equipment is in good working order and recording properly, including the quality of footage and ensuring maintenance and servicing arrangements are in place.
- To seek Senior Management Team and Data Protection Officer approval for any new installation of CCTV Systems or changes to existing CCTV Systems and ensuring a data protection impact assessment has been completed.
- Ensure data is deleted from old CCTV hard drive units prior to disposal when replaced by new system.

7.2 The Buildings Projects Manager will have day to day management responsibility for external and internal CCTV at Llanion. Responsibilities include:

- Ensuring placement of clear and prominent signs at entry points to the CCTV zone and placement of additional within the zone.
- The Buildings Projects Manager is the staff member appointed to review non live recordings and only then for security purposes and in line with the purposes set out in Section 4. They may delegate this responsibility to the Llanion Caretaker where this is appropriate.
- Ensuring access to footage is password protected.
- To ensure the screen showing live pictures from CCTV cameras within the reception is restricted from viewing by the general public.
- To seek approval from PCNPA's Data Protection Officer before showing footage, copying and sharing any data with internal and external third parties.
- To contact PCNPA's Data Protection Officer if a subject access or freedom of information request from a staff, Member, volunteer, visitor or member of the Public is received in relation to viewing and accessing footage captured by CCTV system.
- Ensuring staff at Llanion know what to do if a member of the public makes an enquiry about the CCTV system.
- Ensuring that a data protection impact assessment has been completed for all CCTV systems at Llanion.
- Ensuring the details of CCTV systems at Llanion is correctly recorded on the CCTV register (Appendix 1 of this document).
- Regularly checking that the equipment is in good working order and recording properly, including the quality of footage and ensuring maintenance and servicing arrangements are in place.
- To seek Senior Management Team and Data Protection Officer approval for any new installation of CCTV Systems or changes to existing CCTV Systems and ensuring a data protection impact assessment has been completed.
- Ensure data is deleted from old CCTV hard drive units prior to disposal when replaced by new system.

7.3 Site/ Warden Managers at Cilrhedyn Workshop or relevant Depot will have day to day management responsibility for CCTV at their sites. Responsibilities include:

- Ensuring placement of clear and prominent signs at entry points to the CCTV zone and placement of additional within the zone.
- The Site/ Warden manager is the staff member appointed to review non live recordings and only then for security purposes and in line with the purposes set out in Section 4. In relation to Cilrhedyn they may delegate this responsibility to the Woodland Supervisor when this is appropriate.
- Ensuring access to footage is password protected.
- To seek approval from PCNPA's Data Protection Officer before showing footage, copying and sharing any data with internal and external third parties.
- To contact PCNPA's Data Protection Officer if a subject access or freedom of information request from a staff, volunteer, visitor or member of the Public is received in relation to viewing and accessing footage captured by CCTV system.
- Ensuring staff know what to do if a member of the public makes an enquiry about the CCTV system.
- Ensuring that a data protection impact assessment has been completed for all CCTV systems on their site.
- Ensuring the details of CCTV systems at their site is correctly recorded on the CCTV register (Appendix 1 of this document).
- Regularly checking that the equipment is in good working order and recording properly, including the quality of footage and ensuring maintenance and servicing arrangements are in place.
- To seek senior management team and Data Protection Officer approval for any new installation of CCTV Systems or changes to existing CCTV Systems and ensuring a data protection impact assessment has been completed.
- Ensure data is deleted from old CCTV hard drive units prior to disposal when replaced by new system.

7.4 The Data Protection Officer is responsible for approving the showing of footage, copying and sharing of any data with internal and external third parties or those relating to subject access and freedom of information requests. The Data Protection Officer will consult with the Administration and Democratic Services Manager in cases that relate to Freedom of Information requests. Responses to request for sharing and use of footage for disciplinary purposes must be agreed by the Data Protection Officer. The Data Protection Officer will consult with the Human Resources Manager in terms of requests relating to sharing of footage which includes staff.

7.5 Members of the Senior Leadership Team and the Data Protection Officer are responsible for approving proposed new CCTV installations and any significant changes to existing ones. They will also check to see if there are any Security Industry Authority (SIA) licence implications.

- 7.6 In cases of a serious breach involving CCTV data, the Data Protection Officer is responsible for reporting the matter to the ICO. The Data Protection Officer will also assist teams with Data Protection Impact Assessments and investigate breaches.

## 8. Subject Access Rights and Sharing Footage

- 8.1 People have a right to request through subject access, a copy of footage in which they are captured, subject to exemptions within the Data Protection Act 2018 and also balanced against the rights and freedoms of others who may appear in that footage. PCNPA will require specific details including at least a time, date and camera location before it can properly respond to any such requests. Further information on Subject Access Requests can be found in PCNPA's [Data Protection Policy](#).
- 8.2 If a staff member receives a Subject Access Request relating to CCTV footage they should contact PCNPA's Data Protection Officer for advice and get their approval before providing footage to the requestor.
- 8.3 We cannot release CCTV footage following a Subject Access Request where third party individuals can be identified unless those parties have consented to the disclosure.
- 8.4 The police and other authorized agencies or bodies may apply for access to data collected via CCTV in order to carry out their statutory functions. CCTV footage may be subject to Freedom of Information requests. All requests will be reviewed by PCNPA's Data Protection Officer and determined according to a process which ensures compliance with the law.
- 8.5 The Data Protection Officer must satisfy themselves of the identity of any person wishing to view stored images or access the system and the legitimacy of the request.
- 8.6 The Data Protection officer may also consent to the sharing of footage
- to make a report regarding suspected criminal behaviour
  - To PCNPA 's insurance company where required in order to pursue a claim for loss or damage to insured property

- 8.7 Where images are disclosed as detailed above a record will be made in the system log book including the time of access, the reason for viewing the images, the details of images viewed and a crime incident number (if applicable).
- 8.8 Where images are provided to third parties, wherever practicable steps will be taken to obscure images of non-relevant individuals.

## **9 Data Retention**

- 9.1 CCTV systems operated by PCNPA shall normally retain footage for no longer than 30 days. Where footage for a site is routinely retained for more than 30 days the reason for this should be outlined in CCTV register (Appendix 1 of this policy). Where footage is required for the purposes of prosecution of an offence or to defend legal claims, a copy should be made and stored securely for this purpose.

## **10 Use of CCTV Footage for Disciplinary Purposes**

- 10.1 CCTV is not generally used to monitor staff covertly, however, in exceptional circumstances only, covert monitoring may be considered. Any request for covert CCTV to be installed as a result of genuine management concerns regarding staff conduct (where there is a suspicion of acts of Gross Misconduct including criminal activity), are to be discussed with the Human Resources Manager who will have a discussion with the CEO and Data Protection Officer as to whether this request is granted or not. In determining this, a Data Protection Impact Assessment must be completed. Where it is deemed appropriate, covert monitoring will be carried out for a specific time period and any footage collected will be used only for the purposes as set out in the DPIA.
- 10.2 Where there is an allegation of a breach in disciplinary rules as outlined in our Disciplinary Policy and Procedure or Code of Conduct, CCTV footage from overt or covert cameras may be considered during the investigatory stages of the disciplinary processes, and later used in formal disciplinary hearings, if relevant to the allegations raised against the employee.
- 10.2 Staff should be made aware that CCTV footage may be used for disciplinary purposes. If such CCTV footage is identified it will be presented to the employee during the investigation, pursuant to the Disciplinary Policy and Procedures. The employee will be given the opportunity to review the CCTV footage and explain

or challenge its content. The employee will also be permitted to refer to the CCTV footage in any subsequent disciplinary hearings if applicable.

- 10.3 Activity where CCTV can be provided after being requested by the Human Resources Manager may include:
- Acts which constitute Gross Misconduct in accordance with our Disciplinary Policy.
  - Practices which seriously jeopardise the health and safety of others.
  - Theft or damage to PCNPA property or aggressive behaviour towards PCNPA staff or members of the public.
- 10.4 PCNPA will not use its CCTV for monitoring the activities of PCNPA staff, in the ordinary course of their lawful business. PCNPA staff are not permitted to use CCTV systems to observe the working practices and time keeping of other PCNPA staff.

## 11 Complaints and Queries

- 11.1 If you have any further questions about PCNPA's CCTV system, or its use of CCTV, or requests for footage, please contact PCNPA's Data Protection Officer: [dpo@pembrokeshirecoast.org.uk](mailto:dpo@pembrokeshirecoast.org.uk).
- 11.2 People have a right to object to processing where they believe that the field of vision or the siting of the camera is disproportionate to the stated purpose of the camera. Where someone objects to processing, PCNPA will consider the objection and decide whether a lawful basis for processing can still be justified. A written response will be provided outlining the outcome. Objections can be raised by writing to: [dpo@pembrokeshirecoast.org.uk](mailto:dpo@pembrokeshirecoast.org.uk).
- 11.3 All other complaints relating to CCTV should be processed in line with our [Service Standards Complaints procedures](#).

## 12 Definitions

- 12.1 Definitions of the terms used in this policy:
- CCTV – Closed Circuit Television
  - Data Protection Officer (DPO) – A statutory role set out under the Data Protection Act with responsibility for ensuring that organisations are



compliant with personal privacy rights. Anybody can report a personal privacy concern about the Authority to the Data Protection Officer.

## 13 Related Policies and Procedures

13.1 This policy should be interpreted and applied in relation to other related policies and procedures:

- Data Protection Policy
- Data Retention Policy and Schedule *[Note: Currently under review]*
- ICT User Policy (External and Internal)
- Information and Data Security Policy (Internal)
- Safeguarding Statement (Internal)
- Service Standards – Comments and Complaints
- Freedom of Information Publication Scheme
- Privacy Notice
- Disciplinary Policy and Procedure and Code of Conduct
- Drone Policy *[Note: A separate drone policy is currently being drafted]*.
- Welsh Language Standards (Signage)

Reference		
1	<i>Surveillance Camera Code of Practice, Biometrics and Surveillance Camera Commissioner</i>	<a href="https://www.gov.uk/government/publications/upd-ate-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version">https://www.gov.uk/government/publications/upd-ate-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version</a>
2	<i>Guidance on Video Surveillance, ICO</i>	<a href="https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance/how-can-we-comply-with-the-data-protection-principles-when-using-surveillance-systems/">https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance/how-can-we-comply-with-the-data-protection-principles-when-using-surveillance-systems/</a>
3	<i>The employment practices code, ICO</i>	<a href="https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf">https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf</a>

Version History		
Version	Effective Date	Summary of Changes
1		The policy replaces and updates the Authority's site-specific CCTV policies and has been reviewed by PCNPA's Data Protection Officer.

## Appendix 1 – CCTV Register

Site	Carew Castle and Tidal Mill
Responsible PCNPA Officer	Visitor Services Manager South
Camera Locations	Castle Shop, Internal (1 unit with 3 cameras)
Monitor Location	Office attached to Castle Shop
Audio/ Images	Images only
Monitoring of General Public/ Public Areas/ Any other public or private land beyond PCNPA land	Yes – anyone who enters shop. Doesn't cover external public spaces and only captures National Park Authority Land.
Site Specific Objectives/ Purposes	<ul style="list-style-type: none"> <li>• Preventing and detecting crime at its sites and retail facilities and assist in the identification and apprehension of offenders.</li> <li>• To provide evidence of damage or loss to the Authority's insurance company.</li> <li>• To protect staff, volunteers, visitors and members of the public with regard to their personal safety</li> <li>• Deterring violent or aggressive behaviour towards PCNPA staff</li> <li>• To protect the Authority's buildings and equipment, and the personal property of, staff, volunteers, visitors and members of the public.</li> </ul>
Recording Retention Period (Justification if longer than standard 30 days)	30 days, automatically overwritten
Signage in Place	Signage in place on wall of the Castle Shop where the cameras are
Authorised to Access Footage	Visitor Services Manager South - Password Access. Live footage can be viewed by any staff working in the Castle Office.

Site	Castell Henllys
Responsible PCNPA Officer	Visitor Services Manager North
Camera Locations	1 unit located at shop, internal. 1 unit located reception (Public Area), internal. 1 unit located Reception (Public Area), internal.
Monitor Location	Reception
Audio/ Images	Images only

Monitoring of General Public/ Public Areas/ Any other public or private land beyond PCNPA land	Yes – anyone who enters shop and reception area. Doesn't cover external public spaces and only captures that is on PCNPA land.
Site Specific Objectives/ Purposes	<ul style="list-style-type: none"> <li>• Preventing and detecting crime at its sites and retail facilities and assist in the identification and apprehension of offenders.</li> <li>• To provide evidence of damage or loss to the Authority's insurance company.</li> <li>• To protect staff, volunteers, visitors and members of the public with regard to their personal safety.</li> <li>• Deterring violent or aggressive behaviour towards PCNPA staff.</li> <li>• To protect the Authority's buildings and equipment, and the personal property of, staff, volunteers, visitors and members of the public.</li> </ul>
Recording Retention Period (Justification if longer than standard 30 days)	30 days
Signage in Place	Yes – Signage on display on the door on the way into the building and at reception.
Authorised to Access Footage	Live images are monitored in reception by staff on duty. Visitor Services Manager North - Password Access.

Site	Oriel y Parc
Responsible PCNPA Officer	Visitor Services Manager West
Camera Locations	15 Colour Camera covering internal and external areas (Cameras 1-4 are external cameras)
Monitor Location	Reception desk and back office
Audio/ Images	Images only
Monitoring of General Public/ Public Areas/ Any other public or private land beyond PCNPA land	<p>Yes in terms of Public/ Public Areas.</p> <p>In terms of other public or private land beyond PCNPA land the only camera which has a view of other areas is 'Camera 3.' This camera covers the rear shutter doors of the centre as well as the rear staff entry, there is a very small amount of Bryn Road showing which is unavoidable, as we need to be able to see the rear staff entrance, so it takes in probably a meter of the road side.</p>
Site Specific Objectives/ Purposes	<ul style="list-style-type: none"> <li>• To protect staff, volunteers, visitors and members of the public with regard to their personal safety</li> <li>• Deterring violent or aggressive behaviour towards PCNPA staff</li> </ul>

	<ul style="list-style-type: none"> <li>• To protect the Authority's buildings and equipment, and the personal property of, staff, volunteers, visitors and members of the public.</li> <li>• Preventing and detecting crime at its sites and retail facilities and assist in the identification and apprehension of offenders.</li> <li>• To provide evidence of damage or loss to the Authority's insurance company.</li> </ul>
Recording Retention Period (Justification if longer than standard 30 days)	<p>Minimum of 3 months before footage is automatically overwritten – this is to be amended to 30 days.</p> <p>Amgueddfa Cymru/ National Museum Wales don't require PCNPA to hold onto recordings past 30 days.</p> <p><i>[To be Updated - Retention Period to be amended, hard drive is potentially being replaced and 30 days retention period will be a specification requirement for the new one].</i></p>
Signage in Place	Yes – Signage on entry to the café and inside the main visitor centre are in 2 different locations.
Authorised to Access Footage	<p>During opening hours, live images are displayed and monitored by staff on duty both at the reception desk and in the back office.</p> <p>Recorded Images – Visitor Services Manager West and Site Warden, Password Access.</p>

Site	Cilrhedyn Workshop and Depot
Responsible PCNPA Officer	Site Manager (Area Warden Manger North)
Camera Locations	<p>Camera 1 - unit eastern end of woodland warden shed (looks back over park trailers, diesel tank &amp; entrances into woodland warden store &amp; north warden store, external.</p> <p>Camera 2 - unit next to ranger store (covers yard and diesel tank), external.</p> <p>Camera 3 - pine end of main shed/building (covers main roller door, looks back up to site entrance &amp; yard in front of shed), external.</p>
Monitor Location	Mess Room
Audio/ Images	Images only
Monitoring of General Public/ Public Areas/ Any other public or private land beyond PCNPA land	<p>Yes.</p> <p>Camera 1 – trailer parking and diesel tank – can see over hedge into the field next door. It is a grazing field. It is not possible to change the field of view without reducing the area of the yard that we are trying to capture.</p> <p>Camera 3 – pine end of the main shed/ building – None PCNPA land is captured in footage as you can see cars passing on the road. However due to the</p>

	distance you would not be able to identify individuals and any person/ vehicle at the roadside entrance would be difficult to recognise. This limits the impact in terms of privacy.
Site Specific Objectives/ Purposes	<ul style="list-style-type: none"> <li>• To protect staff with regard to their personal safety</li> <li>• To protect the Authority's buildings and equipment, and the personal property of staff,</li> <li>• Preventing and detecting crime at its sites and assist in the identification and apprehension of offenders.</li> <li>• To provide evidence of damage or loss to the Authority's insurance company.</li> </ul>
Recording Retention Period (Justification if longer than standard 30 days)	30 days, automatically overwritten.
Signage in Place	Signage in Place
Authorised to Access Footage	Recorded Footage - Site Manager and Woodland Supervisor, Password Access

Site	Llanion HQ
Responsible PCNPA Officer	Buildings Projects Manager – Servicing and Maintenance
Camera Locations	<p>Internal:</p> <ul style="list-style-type: none"> <li>• Reception area front (Covers front door entry)</li> <li>• Reception area back</li> <li>• Blue meeting room</li> <li>• Yellow meeting room</li> <li>• Red meeting room</li> </ul> <p>External:</p> <ul style="list-style-type: none"> <li>• Rear courtyard</li> <li>• Century box, staff entrance</li> <li>• Access drive Camera (on corner of building)</li> <li>• Front Parking area (on corner of building)</li> <li>• Front Parking area (other side)</li> <li>• Main entrance</li> </ul>
Monitor Location	Reception.
Audio/ Images	Images only
Monitoring of General Public/ Public Areas/ Any other public or private land beyond PCNPA land	<p>Internal:</p> <p>Reception area front (Covers front door entry) and Reception area back monitor general public accessing reception area.</p> <p>External:</p>

	<ul style="list-style-type: none"> <li>• Rear courtyard - Small part of back garden of sheltered housing complex behind Llanion is captured in top corner of camera shot. Repositioning not possible as if turned further left would lose scope in terms of monitoring the courtyard.</li> <li>• Access drive Camera (on corner of building) – PCNPA Llanion car park. Adopted highway visible in top corner of camera shot. Not feasible to reposition camera as would then lose from shot the exit from the car park which is needed in terms of meeting site specific objectives.</li> <li>• Century box, staff entrance – PCNPA Llanion car park</li> <li>• Front Parking area (on corner of building) – PCNPA Llanion car park</li> <li>• Front Parking area (other side) – PCNPA Llanion car park</li> <li>• Main entrance – Public entrance way</li> </ul>
Site Specific Objectives/ Purposes	<ul style="list-style-type: none"> <li>• To protect staff, volunteers, visitors and members of the public with regard to their personal safety</li> <li>• Deterring violent or aggressive behaviour towards PCNPA staff</li> <li>• To protect the Authority's buildings and equipment, and the personal property of, staff, volunteers, visitors and members of the public.</li> <li>• Preventing and detecting crime at its sites and assist in the identification and apprehension of offenders.</li> <li>• To provide evidence of damage or loss to the Authority's insurance company.</li> </ul>
Recording Retention Period (Justification if longer than standard 30 days)	30 days, automatically overwritten.
Signage in Place	Signage in Place
Authorised to Access Footage	<p>Reception team can view live footage but cannot access recorded data.</p> <p>Recorded footage – Buildings Project Manager and Site Caretakers, password access.</p>