Pagham Yacht Club

CCTV Policy (Final) April 2022

1. Introduction

1.1. Pagham Yacht Club ("PYC"), has in place a CCTV surveillance system ("the CCTV system"), across its sites. The system was installed in response to repeated thefts from PYC premises, despite other security measures being in place. It provides reasonable and proportionate protection to members and their property, particularly when PYC premises are unoccupied.

1.2. This policy details the purpose, use and management of the CCTV system at PYC and details the procedures to be followed in order to ensure that PYC complies with relevant legislation and the current Information Commissioner's Office CCTV Code of Practice.

1.3. PYC will have due regard to the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and any subsequent data protection legislation, and to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998. Although PYC is not a relevant authority, PYC will also have due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012 and in particular the 12 guiding principles contained therein.

1.4. This policy is based upon guidance issued by the Information Commissioner's Office, 'In the picture: A data protection code of practice for surveillance cameras and personal information'

1.5. This policy and the procedures detailed, applies to any part of the CCTV system which is capable of capturing images of identifiable individuals for the purpose of viewing and or recording the activities of such individuals. CCTV images are monitored and recorded in strict accordance with this policy.

2. CCTV System overview

2.1. The CCTV system is owned and managed by PYC, 1 West Front Road, Bognor Regis, PO21 4SY. Under current data protection legislation PYC is the 'data controller' for the images produced by the CCTV system. PYC is registered with the Information Commissioner's Office and the registration number is 808634. The CCTV system operates to meet the requirements of the Data Protection Act and the Information Commissioner's guidance.

2.2. The designated Security Officer is responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.

2.3. The CCTV system operates across PYC's Clubhouse and combined Car Park and Boat Park. Details of the number and location of cameras can be found at: http://www.paghamyachtclub.com/security/

2.4. Signs are placed at appropriate locations in order to inform members, visitors and members of the public that CCTV is in operation.

2.5. The Security Officer is responsible for ensuring that adequate signage is erected in compliance with the ICO CCTV Code of Practice.

2.6. Cameras are sited to ensure that they cover PYC premises as far as is possible. Cameras are installed at car parks, buildings, licensed premises, within buildings and externally in vulnerable public facing areas.

2.7. Cameras are not sited to focus on private residential areas. Where cameras might overlook residential areas, privacy filters will be applied.

2.8. Cameras are not sited in areas considered private, such as changing rooms or toilets.

2.9. Cameras capable of recording sound will only do so when recorded audio is appropriate for the declared use of the system. Audio will not normally be recorded where conversations are likely to be overheard.

2.10. The CCTV system is operational and is capable of being monitored for 24 hours per day, every day of the year.

2.11. The CCTV system is subject to a Data Protection Impact Assessment and any new CCTV Camera installation is subject to a privacy assessment.

3. Purposes of the CCTV system

3.1. The principal purposes of PYC's CCTV system are as follows:

3.1.1. for the prevention, reduction, detection and investigation of crime and other incidents;

3.1.2. to ensure the safety of members and visitors;

3.1.3. to assist in the investigation of suspected breaches of Club regulations by members and visitors.

3.2. The CCTV system will be used to observe PYC's facilities and areas under surveillance in order to identify incidents requiring a response. Any response should be proportionate to the incident witnessed.

3.3. PYC seeks to operate its CCTV system in a manner that is consistent with respect for individuals' privacy.

4. Monitoring and Recording

4.1. Cameras can be monitored remotely by approved individuals and at a password-protected workstation in the PYC loft. The Commodore and Security Officer are authorised to approve individuals to view cameras within their area of responsibility on a view-only basis.

4.2. Images are recorded on a server located at the loft workstation.

4.3. The cameras installed provide images that are of suitable quality for the specified purposes for which they are installed and all cameras are regularly checked to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate.

4.4. All images recorded by the CCTV System remain the property and copyright of PYC.

5. Compliance with Data Protection Legislation

5.1. In its administration of its CCTV system, PYC complies with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Due regard is given to the data protection principles embodied in GDPR. These principles require that personal data shall be:

5.1.1. processed lawfully, fairly and in a transparent manner;

5.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

5.1.3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

5.1.4. accurate and, where necessary, kept up to date;

5.1.5. kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed;

5.1.6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

5.2. PYC ensures it is responsible for, and able to demonstrate compliance with GDPR

6. Applications for disclosure of images

6.1. Applications by individual data subjects:

6.1.1. For requests by individual data subjects for images relating to themselves, a “Subject Access Request” should be submitted in writing to PYC Honorary Secretary together with proof of identification.

6.1.2. In order to locate the images on PYC’s system, sufficient detail must be provided by the data subject in order to allow the relevant images to be located and the data subject to be identified.

6.1.3. Where PYC is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual.

6.2. Access to and disclosure of images to third parties:

6.2.1. A request for images made by a third party should be made in writing to the Security Officer.

6.2.2. In limited circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation.

6.2.3. Such disclosures will be made at the discretion of the Security Officer, with reference to relevant legislation and where necessary, following advice from independent Information Compliance experts.

6.2.4. The Security Officer may provide access to CCTV images to approved Club Officers when sought as evidence in relation to discipline cases.

6.2.5. A record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requestor, authoriser and reason for the disclosure.

7. Retention of images

7.1. Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images will be retained for no longer than 30 days from the date of recording. Images will be automatically overwritten after this point.

7.2. Where an image is required to be held in excess of the retention period referred to in 7.1, the Security Officer or their nominated deputy, will be responsible for authorising such a request.

7.3. Images held in excess of their retention period will be reviewed on a three monthly basis and any not required for evidential purposes will be deleted.

7.4. Access to retained CCTV images is restricted to the Security Officer and other persons as required and as authorised by the Security Officer.

8. Complaints procedure

8.1. Complaints concerning PYC's use of its CCTV system or the disclosure of CCTV images should be made in writing to the Commodore at: commodore@paghamyachtclub.com

8.2. All appeals against the decision of the Commodore should be made in writing to the Club Trustees, via the Honorary Secretary: honsec@paghamyachtclub.com

9. Monitoring Compliance

9.1. All persons involved in the operation of PYC's CCTV System will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein.

9.2. All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to be familiar with data protection legislation, and undergo training where appropriate.

10. Policy review

10.1. PYC's usage of CCTV and the content of this policy shall be reviewed annually by the Security Officer with reference to the relevant legislation or guidance in effect at the time. Further reviews will take place as required.

APPENDIX A Assigned responsibilities and access

Approved CTTV access:

Role*	Rights	Areas
Security Officer	Local & remote Live & recorded. Data processing purposes. System access for maintenance.	All areas
Rear Commodore Buildings	Live, read-only, remote	PYC Club House
Rear Commodore Sailing	Live, read-only, remote	PYC Boat Park
Rear Commodore Angling	Live, read-only, remote	PYC Boat Park
Data Protection Officer (DPO)	Ad-hoc, as required for investigations	All areas
Commodore	Ad-hoc, as required for investigations	All areas

* Names and contact details on PYC website: http://www.paghamyachtclub.com

APPENDIX B CCTV Review Checklist

This CCTV system and the images produced by it are controlled by the PYC Security Officer 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.

We 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 members. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

Topic	Checked (Date)	By
Notification has been submitted to the Information Commissioner and the next renewal date recorded.		
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.		

Next review due 12 months after first item above. Date: _____

APPENDIX C References:

ICO Guidance: “Installing CCTV? Things you need to do first”
https://ico.org.uk/for-organisations/sme-web-hub/whats-new/blogs/installing-cctv-things-you-need-to-do-first/

ICO Guidance: “Guide to Data Protection”
https://ico.org.uk/for-organisations/guide-to-data-protection/

Data Protection Act 2018
https://www.gov.uk/government/collections/data-protection-act-2018

General Data Protection Regulation (GDPR)
https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

ICO Guidance: Guide to the UK General Data Protection Regulation (UK GDPR)
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Freedom of Information Act 2000
https://www.legislation.gov.uk/ukpga/2000/36/contents

ICO Guidance: What is the Freedom of Information Act?
https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

Protection of Freedoms Act 2012
https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted
https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

ICO Guidance: “In the picture: A data protection code of practice for surveillance cameras and personal information”
https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

ICO Guidance: “How to deal with a request for information: a step-by-step guide”
https://ico.org.uk/for-organisations/sme-web-hub/how-to-deal-with-a-request-for-information-a-step-by-step-guide/

APPENDIX D Data Protection Impact Assessment (DPIA)

Conducted October 2021 by Kevin Harris on behalf of Pagham Yacht Club

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
Operation & maintenance of small scale CCTV system for purposes of crime prevention and detection. Initiated by ICO advice to all organisations installing CCTV to have a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
Central unit (NVR) collects image and audio data from cameras for monitoring locally or remotely, and stores data for up to 30 days, after which it is automatically over-written by the system. It is unlikely these processes would present a high risk. Other data collection, storage or sharing would be exceptional and be in accordance with CCTV Policy.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
As above. Data will only be collected within PYC premises and peripheral areas, with privacy masks as required.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
There is nothing unusual in this context. People are familiar with CCTV and where people or property are to be protected, would expect CCTV to form part of this protection, provided it is used proportionately. The installed system uses current and standard technologies and techniques.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
The system provides a visible deterrent to potential criminals, and the data collected might identify individuals to the relevant authorities following a crime.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
The CCTV Policy will be published to the PYC website and feedback sought via the PYC members Blog.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
Only approved members will have access and only where relevant and proportionate to their role. Details will be provided in the CCTV Policy.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Innovative technology Denial of service Large-scale profiling Biometric data Genetic data Data matching Invisible processing Tracking Targeting of children/other vulnerable individuals for marketing, profiling for auto decision making or the offer of online services Risk of physical harm	All remote	Minimal	All low

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
None		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Commodore	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	None	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	PYC Security Officer	The DPO should also review ongoing compliance with DPIA