**Cattewater Harbour Commissioners CCTV Policy**

## 1. Purpose and scope

1.1. Cattewater Harbour Commissioners ("**we**", "**us**" and "**our**") uses closed circuit television (CCTV) to provide a safe and secure environment for staff, visitors and customers, for enforcement of our statutory duties and powers, and to protect our property. This policy relates to the use and management of CCTV throughout our premises, operated slipways and supervised areas of the harbour.

1.2. This policy sets out the accepted use of the CCTV equipment and images to ensure compliance with relevant data protection and privacy laws.

1.3. This policy has been produced in line with the Information Commissioner's Office (ICO) CCTV Code of Practice and should be read alongside the Cattewater Harbour Commissioner's Privacy Policy.

## 2. Why we use CCTV

2.1. We have considered and determined that the purposes for which CCTV is deployed are legitimate, reasonable, appropriate and proportionate. CCTV systems are deployed at our premises where it is necessary:

2.1.1. for the exercise of official authority vested in us, to pursue parties who use our facilities without payment, including for civil enforcement or statutory seizure and sale of a vessel and/or goods; and

2.1.2. for our or a third party's legitimate interests (where we are not performing our tasks as a public authority), including monitoring security and health and safety at our premises.

Additionally we deploy CCTV systems as necessary for law enforcement purposes in our capacity as a competent authority in order to:

2.1.3. deter crime and assist in the prevention and detection of crime and/or serious breaches of policies and procedures; and

2.1.4. assist with the identification, apprehension and prosecution of offenders.

2.2. The CCTV system will NOT be used:

2.2.1. to record sound; or

2.2.2. for any automated decision taking.

2.3. We have:

2.3.1. assessed and documented the appropriateness of and reasons for using CCTV;

2.3.2. established and documented who is responsible for day-to-day compliance with this policy - the Harbour Commissioner; and

2.3.3. ensured signage is displayed to inform individuals that CCTV is in operation, except where CCTV is located in locations where such signage would not be visible, such as on navigation towers or cliffs.

2.4. Once installed, reviews will be regularly undertaken to ensure that the use of the CCTV systems and the processing of the personal data obtained through it remains justified.

## 3. Positioning cameras

3.1. We will make every effort to position cameras to ensure they only cover our premises, operated slipways and supervised areas of the harbour. Where possible, any cameras that have a field of view which includes private homes or gardens are modified so that the homes or gardens are automatically blocked-out and removed from view.

3.2. The installation of cameras in areas in which individuals would have an expectation of privacy will not be authorised under this policy, unless reasonable steps are taken to prevent intrusion, or there are exceptional circumstances, subject to approval by the Harbour Master.

3.3. Wherever possible we will clearly display signs in the vicinity of the cameras so that staff, visitors and customers/clients are aware they are entering an area covered by CCTV, however this will not always be possible where cameras are located in non-visible areas such as on cliffs or navigation towers.

3.4. Our CCTV signs will state:

3.4.1. that we are responsible for the CCTV recording; and

3.4.2. contact details for queries regarding the CCTV scheme.

3.5. We have taken reasonable steps to ensure no neighbouring domestic areas are included in the camera view, including a system for automatically blocking any such areas from the camera view.

**4. Image quality**

4.1. Images produced by the equipment must be as clear as possible so that they are effective. To achieve this:

4.1.1. the equipment must be properly installed, serviced, checked and maintained to ensure it works properly;

4.1.2. any recording media, if needed, will be of good quality and will be replaced if the quality of the images has begun to deteriorate;

4.1.3. where time/date of images are recordable the equipment will be set accurately;

4.1.4. cameras will be correctly positioned; and

4.1.5. cameras will be protected from vandalism so far as is possible.

**5. Data and image retention**

5.1. Images and recording logs must be retained and disposed of in accordance with our standard CCTV retention procedures to ensure that footage is not kept for any longer than is necessary.

5.2. For digital recording systems, CCTV images held on the hard drive of a PC or server will be overwritten on a regular basis, and unless authorised by the Harbour Master, will not be held for more than 28 days. Cameras are triggered by movement and so the retention period will vary, depending on the amount of movement and therefore amount of footage recorded by the particular camera.

5.3. If images are retained for longer than this, the reason(s) will be recorded. An example of where we may need to retain footage for longer than 28 days is where it is needed in connection with law enforcement.

5.4. Where a request to retain information is authorised, reasonable steps will be taken to safeguard any footage which would otherwise have been be deleted. If footage is shared on removable media this must be password protected.

5.5. Recordings will only be accessible within the management office or by remote app access. Physical access restrictions are in place within the office, including password protecting computer systems from which footage could be obtained or copied, and remote app access is also restricted via password.

**6. Access to images**

6.1. Staff images

6.1.1. Staff images will only be accessed if a serious event occurs, such as criminal activity, fraud, gross misconduct, or behaviour that puts others at risk.

6.1.2. Requests to access footage must be authorised by the Harbour Master before the necessary access arrangements are made.

6.1.3. Any request to view CCTV footage will have to be recorded for audit purposes on a CCTV register. The CCTV register should list:

6.1.3.1. the date and time of the request/disclosure;

6.1.3.2. whether or not the request has been authorised;

6.1.3.3. the reason for authorisation;

6.1.3.4. whether or not the footage is being removed from the CCTV system or secure storage i.e. downloaded onto removable media; and

6.1.3.5. a signature of the person that is accessing the footage.

6.2. Access to and disclosure of images to third parties

6.2.1. Access to and disclosure of images recorded on CCTV will be restricted and carefully controlled. This will ensure that the rights of individuals are protected, and also ensure that the images can be used as evidence if required. Images may only be disclosed in accordance with the purposes for which they were originally collected.

6.2.2. Disclosures to third parties will only be made in accordance with the purpose(s) for which the system is used and will be limited to:

6.2.2.1. police and other law enforcement agencies, where the images recorded could assist in a specific criminal enquiry and/or the prevention of terrorism and disorder;

6.2.2.2. prosecution agencies (such as the Crown Prosecution Service);

6.2.2.3. relevant legal representatives of people whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings);

6.2.2.4. individuals who have been caught on our CCTV in accordance with a request made such as one described at 8 below;

6.2.2.5. in exceptional cases, for others (such as insurers, local authorities or other statutory harbour authorities) to assist in identification of a victim, witness or perpetrator in relation to an incident; and

6.2.2.6. staff involved with our disciplinary processes.

6.3. If a police officer requests images from our CCTV system in relation to an investigation that has not been initially reported by the business, then please refer them to the Harbour Master. It may be that we are required to disclose the images or we have a discretion whether to do so.

**7. Disclosure**

7.1. The Harbour Master and Harbour Assistant are the only people who can authorise disclosure of information to the police or other law enforcement agencies. All requests for disclosure should be documented for audit purposes in the CCTV register. If disclosure is denied, the reason should also be recorded in the CCTV register.

7.2. Before any images are disclosed the following must be recorded in the CCTV register:

7.2.1. if the images are being removed from the CCTV system or secure storage to another area, the location to which they are being transferred;

7.2.2. any crime incident number, if applicable; and

7.2.3. the signature of the person to whom the images have been transferred.

**8. Subject access rights to individuals' own data**

8.1. The UK GDPR gives individuals the right to access personal data about themselves, including CCTV images and footage.

8.2. Where a request for access to CCTV images/footage is made, we should request confirmation of the following information in writing to enable us to identify the relevant personal data:

8.2.1. the full name and address of the person making the request (the 'data subject');

8.2.2. a description of the data subject and/or details of what they were wearing to ensure we can locate the individual, and only relevant images are disclosed;

8.2.3. the approximate date and time when the images were recorded to allow for searching; and

8.2.4. the location where the images were recorded.

8.3. The Harbour Master and Harbour Assistant will record and respond to such requests and decide whether the disclosure of footage is appropriate (which may involve seeking legal advice); this is unless the request is made by a member of staff, in which case it will be actioned by HR.

8.4. Before we disclose any footage it is important to determine whether disclosure of the images will reveal third-party personal information.

8.5. Particular care should be exercised when images of other people are included in the materials for disclosure. We will need to consider whether there would be an expectation that the third-party images would be released in such circumstances. If not, we need to consider whether obscuring the identity of third-parties is possible, or whether we can get their consent. If not, disclosure may not be appropriate. We could alternatively allow the data subject to review the footage under supervision on our premises to avoid disclosing a copy of third-party personal data outside of the organisation. Supervised viewings will only be appropriate in certain circumstances though and each request will need to be considered on a case-by-case basis.

8.6. The UK GDPR also gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data. The UK GDPR also gives individuals the right to object to the processing of their personal data in certain circumstances.

8.7. We must respond to all data subject requests that we receive within one month of receipt.

**9. Responsibility for CCTV systems and staff training**

9.1. The Harbour Master may nominate a suitable and qualified manager or senior member of the department with the day-to-day responsibility of the systems and the training of staff responsible for operating or administering CCTV. However, the overall responsibility lies with the Harbour Master.

**10. Complaints**

10.1. Enquiries relating to data protection laws should be addressed to the Harbour Office at Cattewater Harbour Commissioners 2, The Barbican, Plymouth, Devon, PL1 2LR, United Kingdom.

10.2. If a member of staff believes that there has been a breach of data protection laws they must contact either the Harbour Master or their line manager as a matter of urgency.

10.3. If a complainant or enquirer is not satisfied with the response received, they can write to the ICO. Details of how to do this can be found on the ICO website: www.ico.org.uk.

**11. Enforcement and compliance**

11.1. The misuse of our surveillance systems and unauthorised use of images and CCTV footage may constitute a criminal offence.

11.2. Any concerns regarding the use of CCTV should be shared with your line manager or, if you are not comfortable with escalating concerns via your line manager, with the Harbour Master or a member of the Board of Commissioners.

**PRIVACY POLICY**

This privacy policy sets out how the **Cattewater Harbour Commissioners** the Statutory and Competent Harbour Authority for the Port of Plymouth ("**we**", "**us**", "**our**") collects, uses and protects personal data about you.

When we collect and use your personal data we will usually be subject to the UK General Data Protection Regulation (UK GDPR), however in certain limited circumstances, where we may be processing your personal data for criminal law enforcement purposes, we will instead be subject to the rules for law enforcement processing set out in the Data Protection Act 2018.

Please see the "How to contact us" section at the end of this privacy policy if you have any questions about this privacy policy or the data we hold about you.

**Our collection and use of your personal data**

How will we collect your personal data?

We will typically collect your personal data from you directly, for example:

- If you visit our website.
- If you complete an online contact form.
- If you otherwise request details of our leisure moorings.
- When you sign up as a customer for any of our commercial services, for example mooring, pilotage, diving permits or licences
- If you respond to tender opportunities.
- If you visit our premises.

We may also collect your personal data indirectly from a third party, for example: where a vessel is under shared ownership and your co-owner provides your personal data to us when purchasing a product or service; or where we request information for enforcement purposes such as from the Police or DVLA.

What information do we collect?

The personal data we collect will vary based on the purposes for which we engage with you. We may collect and use the following information about you:

- **Identity Data** - your title, name, address and date of birth.
- **Contact Data** - email address and telephone numbers.
- **Vessel Data -** particulars of any vessel using our moorings and evidence of boat insurance from which we will be able to identify you.
- **Transaction Data –** details of payments or purchases made with us.
- **Financial Data** - bank account and payment card details.
- **Technical Data -** we may gather information when you visit our website, such as internet protocol (IP) address, other device information, which pages you visit or how long you spend reading a particular page.
- **CCTV footage –** we collect CCTV footage throughout our premises, operated slipways and supervised areas of the harbour, please see the "CCTV" section below for more information.

We may also collect **Criminal Offence Data** about you where it relates to our statutory enforcement duties. We therefore only process Criminal Offence Data in an official capacity.

We do not collect any special categories of personal data about you (this includes for example details about your race or ethnicity, religious or philosophical beliefs, political opinions or information about your health).

You may refuse to provide us with some or all of your personal data, however this might restrict how we interact with you.

How do we use your information?

We will only use your personal data if we are permitted to do so, for example if we have a lawful basis under the UK GDPR or we are processing it for law enforcement purposes:

- **Public task**. Where our use of your personal data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us.
- **Contract.** Where you agree to enter into a contract or purchase a product or service from us such as: an annual or temporary mooring licence; a visitor mooring; licences or leases of buildings or property, and miscellaneous services.
- **Legitimate interests.** If we are processing personal data for any purpose other than the performance of our tasks as a public authority and our use of your personal data is necessary for our legitimate interests or the legitimate interests of a third party (unless there is a good reason to protect your personal data which overrides our legitimate interests).
- **Legal obligation**. Where our use of your personal data is necessary for us to comply with the law (not including contractual obligations).
- **Law enforcement processing.** Authorised activity in our capacity as Statutory Harbour Authority for the Cattewater Harbour relating to the investigation and recording of incidents or accidents, and prosecution of criminal offences committed under harbour legislation.

The table below explains what we use your personal data for and why:

| **Purpose/Activity** | **Type of data** | **Lawful basis** |
|---|---|---|
| Operation of the port and our facilities, including<br><br>(a) authorised activity in our capacity as Statutory Harbour Authority for Cattewater Harbour<br><br>(b) organising the voluntary jet ski registration scheme on behalf of the Navy and other statutory authorities operating within the Plymouth Port | (a) Identity<br><br>(b) Contact<br><br>(c) Vessel<br><br>(d) Transaction<br><br>(e) CCTV<br><br>(f) Criminal Offence | (a) Public Task<br><br>(b) Law Enforcement Processing |
| Investigating incidents within the harbour, including contacting you in relation to any incidents or accident in the harbour that you were directly involved in or have witnessed. | (a) Identity<br><br>(b) Contact<br><br>(c) Vessel<br><br>(d) CCTV<br><br>(e) Criminal Offence | (a) Public Task<br><br>(b) Law Enforcement Processing |
| Sending communications including emailing Local Notices or weather warnings to Mariners, which may affect you or your vessel's safety. | (a) Identity<br><br>(b) Contact<br><br>(c) Vessel | (a) Public Task |
| To register you as a new customer | (a) Identity<br><br>(b) Contact<br><br>(c) Vessel | (a) Performance of a contract with you<br><br>(b) Public Task |
| To provide products or services to you for example mooring licences or visitor mooring, including:<br><br>(a) to manage payments, fees and charges<br><br>(b) to collect and recover money owed to us | (a) Identity<br><br>(b) Contact<br><br>(c) Vessel<br><br>(d) Financial<br><br>(e) Transaction | (a) Performance of a contract with you<br><br>(b) Public Task |
| To manage our relationship with you which will include: | (a) Identity | (a) Performance of a contract with you |

| | | |
|---|---|---|
| (a) Notifying you about changes to our products or services, terms or privacy policy<br><br>(b) Responding to customer enquiries or complaints | (b) Contact<br><br>(d) Vessel<br><br>(e) Profile | (b) Necessary to comply with a legal obligation |
| To administer and protect our organisation and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data) | (a) Identity<br><br>(b) Contact<br><br>(c) Technical | (a) Necessary for our legitimate interests (for running our organisation, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise)<br><br>(b) Necessary to comply with a legal obligation |
| To use data analytics to improve our website, customer relationships and experiences | (a) Technical | Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant and to develop our organisation) |
| To keep a record of customers and vessels within the harbour from time to time. | (a) Identity<br><br>(b) Contact<br><br>(c) Vessel<br><br>(d) Transaction | (a) Public Task<br><br>(b) Legal obligation |

**Who might we share your information with?**

We routinely share personal data with:

- Third parties we use to help provide our products and services to you, e.g. payment service providers.
- Other third parties we use to help us run our business, e.g. our IT infrastructure provider, Acronyms and our CCTV management software provider Blue Iris.

We only allow our service providers to handle your personal data if we are satisfied they take appropriate measures to protect your personal data. We also impose contractual obligations on service providers to ensure they can only use your personal data to provide services to us and to you.

We may also disclose your personal data to law enforcement agencies and regulatory bodies to comply with our legal and regulatory obligations and duties, or to assist them, or enable them to assist us, in investigating potential breaches of the law. Such third parties include the Police, the DVLA, other statutory harbour authorities and the local authority.

**Transferring your personal data outside of the UK**

To provide our function and services, it is sometimes necessary for us to share your personal data outside the UK for example with our service providers which are also themselves located within the UK but that transfer personal data outside of the UK i.e. Acronyms our IT infrastructure provider, is hosted within the US.

Transfers of personal data outside of the UK are subject to special rules under UK data protection law. This is because non-UK countries do not have the same data protection laws as the UK. We will, however, ensure the transfer complies with UK data protection law and all personal data will be secure.

When personal data is transferred outside of the UK we will ensure that the transfer complies with data protection law by following one of the below steps:

- Confirming that the recipient is located in a country which has been recognised as having an adequate level of protection for personal data, for example countries located within the EEA.

- Putting in place safeguards (such as approved standard contractual clauses) so that you have enforceable rights and effective legal remedies.

- Confirming that a specific exception applies under data protection law.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the UK.

**CCTV**

We collect CCTV footage throughout our premises, operated slipways and supervised areas of the harbour for:

- Deterring crime.
- Pursuing civil recovery where an individual has used our services without payment.
- Assisting in the prevention and detection of crime and/or serious breaches of policies and procedures.
- Assisting with the identification, apprehension and prosecution of offenders.
- Monitoring security and health and safety at our premises.

Reasonably accessible cameras are supported with CCTV notices so that the cameras are brought to your attention. Our CCTV cameras do not record sound.

We restrict access to CCTV footage to only personnel that require access to this as part of their job role and implement robust security measures to prevent unauthorised access or disclosure of footage.

Footage is only shared with third parties:

- Where necessary in relation to incidents, accidents and investigations, including police and other law enforcement agencies and legal representatives.
- Where necessary for us to pursue civil recovery where an individual has used our services without payment.
- Where a data subject is requesting to exercise a legal right under data protection legislation and we conclude that disclosure is appropriate (see “Your rights” below).

Additionally, CCTV images will be overwritten on a recycling basis once the storage is full, and unless authorised by the Harbour Master (for example in relation to an ongoing investigation) footage will not be held for more than 28 days. Cameras are triggered by movement and so the retention period will vary, depending on the amount of movement and therefore amount of footage recorded by the particular camera.

You can request further details about our use of CCTV by contacting us (see “How to contact us” below).

**Cookies and other tracking technologies**

Cookies on our website allow us to recognise and count the number of visitors and see how visitors navigate around our website. This helps us to improve the way our website works, for example by making sure users are finding what they need easily.

These also collect some basic information about the device including the operating system/web browsers. We use this to ensure that website is suitable for all devices that view it for example to ensure the site is mobile friendly to tablet/smartphone users etc.

For further information about cookies, our use of cookies and how to disable them, please see our cookie policy here: https://plymouthport.org.uk/cookie-policy/.

**Marketing**

We do not send any marketing communications and will only contact you with service communications, for example renewal notifications and emails containing Local Notices or weather warnings, which may affect you or your vessel’s safety.

**Your rights**

You have the following rights related to your personal data:

| | |
|---|---|
| Access | The right to be provided with a copy of your personal data (the right of access) |
| Rectification | The right to require us to correct any mistakes in your personal data |
| To be forgotten | The right to require us to delete your personal data—in certain situations |
| Restriction of processing | The right to require us to restrict processing of your personal data—in certain circumstances, e.g. if you contest the accuracy of the data |
| Data portability | The right to receive the personal data you provided to us, in a structured, commonly used and machine-readable format and/or transmit that data to a third party—in certain situations |
| To object | The right to object:<br><br>—at any time to your personal data being processed for direct marketing (including profiling);<br><br>—in certain other situations to our continued processing of your personal data, e.g. processing carried out for the purpose of our legitimate interests. |
| Not to be subject to automated individual decision making | The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you |

For further information about your rights please contact us or see the guidance provided by the UK Information Commissioner's Office (ICO) on individuals' rights.

If you would like to exercise any of your rights, please:

- Email, call or write to us — see the 'How to contact us' section at the end of this policy.
- Let us have enough information to identify you e.g. your full name, address and customer or matter reference number.
- Let us have proof of your identity.
- Let us know which right you want to exercise and the data to which your request relates.

**How long will we keep you personal data for?**

We will not retain your personal data for longer than necessary for the purposes set out in this policy. Different retention periods apply for different types of personal data. When it is no longer necessary to retain your personal data, we will delete or anonymise it.

As an indication, if you purchase products or services from us, such as mooring licences, we will keep your personal data while we are providing such licences. Thereafter, we will keep your personal data for as long as is necessary:

- To respond to any questions, complaints or claims made by you or on your behalf.
- To show that we treated you fairly.
- To keep records required by law.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

You can request further details of retention periods for different aspects of your personal data by contacting us (see "How to contact us" below).

**How do we keep you personal data secure?**

We have appropriate security measures to prevent personal data from being accidentally lost, or used or accessed unlawfully. We limit access to your personal data to those who have a genuine business need to access it. Those processing your data will do so only in an authorised manner and are subject to a duty of confidentiality. Our policies and processes ensure your information is only available to our personnel who need to see it to do their job.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

**How we will make changes to this privacy policy**

The privacy policy will be updated from time to time to reflect changes in law and regulations as well as changes to our processing activities. If any changes are made to the way we treat your information, then we will make this clear on our website ***www.plymouthport.org.uk***.

**Complaints and how to contact us**

Any questions, queries or comments with regards to this policy or how we handle your personal data are welcomed. If you have any queries or comments or wish to exercise any of your legal rights under applicable data protection legislation, you can do so by email to ***info@plymouthport.org.uk*** or by letter to: **Cattewater Harbour Commissioners, 2 The Barbican, Plymouth. PL1 2LR.**

If you have any concerns about our processing of your personal data, we hope that we will be able to resolve these.

However, you also have the right to lodge a complaint with the Information Commissioner. The Information Commissioner may be contacted at https://ico.org.uk/make-a-complaint or telephone: 0303 123 1113

**Last updated November 2021**