

This policy sets out the use and management of closed-circuit television (CCTV) equipment and collected images within the Trust in compliance with the UK General Data Protection Regulation, the Data Protection Act 2018 and the Surveillance Camera Code of Practice. This policy should be read in conjunction with the Trust's Privacy Policy.

## **1. Introduction**

- 1.1. Stratford Town Trust has CCTV at one location, the Guild Chapel where we consider there is need for security or safety of the public and building users.
- 1.2. With this policy, Stratford Town Trust wishes to inspire public confidence by ensuring that our surveillance cameras are being used appropriately and preserves the civil liberties of law-abiding individuals at all times. It has been developed in accordance with the Government's recommended guidance: Amended Surveillance Camera Code of March 2022.
- 1.3. This policy aims to set out how the scheme operates and what rights the public have in respect of access to images and privacy. The policy takes into account Stratford Town Trust's obligations including the Human Rights Act 1998 and the principles of good information handling as contained in the Data Protection Act 2018.
- 1.4. When referring to CCTV technology this is the capture, recording and processing of images of persons and / or other forms of personal data, as set out in this Policy.

## **2. Purpose of Stratford Town Trust's CCTV Scheme**

- 2.1. Stratford Town Trust purpose for the use of Surveillance Camera Technology is to:
  - Enhance security of our buildings
  - Protect the health and safety of our staff and volunteers
  - Prevent and detect crime
  - Assist in identifying offenders leading to their arrest and successful prosecution
  - Discourage aggressive or violent behaviour towards staff
  - Reduce any staff and volunteers fears of crime or aggressive behaviour.
  - As evidence of wrong doing
- 2.2. These purposes will define any installation and continual use of surveillance systems by Stratford Town Trust.

### 3. Use of CCTV

3.1. An individual's right to privacy is paramount in our approach to the use of Surveillance Cameras. As such we will:

- Position cameras that will only capture images that meet our purposes identified above.
- Take care to position cameras to ensure that they are not (in general circumstances) located in areas where there would be an expected need for privacy.
- Ensure that camera systems are only operated by trained and authorised personnel.
- Put in place sufficient safeguards to ensure any wireless transmission of data is protected from interception.
- Only use sound recording in exceptional circumstances and when permitted, not for continuous recording.
- Ensure that the public are aware, through appropriate signage, of any surveillance camera systems.

3.2. To ensure we comply with the Amended Surveillance Camera Code March 2022, we will regularly review our Surveillance Camera systems to ensure that they remain justified. To do this we will every two years complete a Privacy Impact Assessment (PIA) to ensure that the camera systems remain proportionate and justified. These will be approved by the Chief Executive.

### 4. Roles and Responsibilities

4.1. To ensure we meet the requirements of the Surveillance Camera Code we have clearly identified below, those responsible and accountable for the images, and information, collected, held and used.

- The **Chief Executive** will have overall responsibility for the implementation of this policy.
- The **Buildings and Facilities Manager** will take operational responsibility for the implementation of this policy by ensuring all those involved in operating the scheme do so in accordance with our aims and undertake their roles in a responsible manner.
- All CCTV operators will be provided with training to ensure conformity to our Policy, including the recording and retention of images, the handling of images securely, and dealing with image access requests from the data subjects, the police and third parties.

- 4.2. All CCTV operators will be provided with training to ensure conformity to our Policy, including the recording and retention of images, the handling of images securely, and dealing with image access requests from the data subjects, the police and third parties. The CCTV operator is defined at The Guild Chapel is the Volunteer Co-ordinator.

## **5. Access to images**

### 5.1. Live Images

- Monitors displaying live images will not be viewed by anyone other than authorised staff and will only be viewed in Stratford Town Trust premises or on Stratford Town Trust's equipment (unless under exceptional circumstances approved by the CEO or their appointed manager).
- All monitors must not be in view of other non-authorised staff, trustees, volunteers or members of the public.
- Cameras cannot be used to monitor the progress of individuals in their ordinary course of lawful business. Individuals will only be continuously monitored if there is a reasonable cause to suspect that an offence has been, or may be about to be, committed.

### 5.2. Recorded Images

- Access to recorded imagery is restricted to those staff who need to have access to meet the schemes purposes or to respond to an incident.
- Data will not be disclosed for any other purpose other than those set out in the Stratford Town Trusts purpose of the scheme, (Para 2.1).
- Anyone wishing to get copies of camera images must contact Stratford Town Trust, as soon as possible to allow Operators to be able to secure the footage and ensure it is not overwritten. A formal request for the footage should also be provided which should include sufficient information to be able to locate the data e.g., within 30 minutes of a given time date and place.

- 5.3. After consideration by the Chief Executive or their appointed manager, if it is agreed to release data images, the Buildings and Facilities Manager or an appointed manager will arrange for these images to be viewed at Stratford Town Trust premises or in the case of responding to a request from the police or other formal agencies we may provide a secure USB copy of these images.

## **6. Requests under FOIA and Data Protection**

- 6.1. Any requests for images via a Freedom of Information Act (FOIA) / Environmental Information Request (EIR), and the person requesting it is the subject of the images; the request will be exempt from FOIA / EIR and will be dealt with under the Data Protection Act 2018 (DPA) outlined below in para 6.2.
- 6.2. Requests for images containing an individual's own personal data can be made under Section 45 of the DPA. However, where third parties are also shown in the images requested, consideration must be given to whether it would be appropriate to disclose these images. At present Stratford Town Trust CCTV technology does not have the ability to obscure images, and as such, the images may have to be withheld from the requestor.
- 6.3. There may also be requests for images where the use is required for legal proceedings that have either started or are contemplated. In such circumstances, the request will be considered under Schedule 2: Part 1: Paragraph 5 of the DPA.
- 6.4. In addition, statutory bodies may request images to assist with enforcement action. We will comply with these requests under DPA Chapter 2 Para 35, if we believe the request is in accordance with our scheme's purpose.
- 6.5. Where data is being collected for the purposes of crime detection, we will seek to provide clear images that can be used for enforcement agencies e.g. the Police.

## **7. Use of recorded images**

- 7.1. Recorded images should not normally be made more widely available e.g. for use by the media or placed on the internet.

## **8. Retention Policy**

- 8.1. Images will not usually be stored longer than 30 days. However, if a request for images has been received, or if this information is required as part of formal investigations, the specific images will be kept securely on a USB in a secured area with restricted access to ensure that the evidence remains admissible. Alternatively, data will be stored in a secure Stratford Town Trust computer folder with access only available to authorised personnel. Security measures will be in place to prevent unauthorised access to, alteration, disclosure, destruction, accidental loss, or destruction of recorded material.

## **9. Published Information**

- 9.1. We are aware of the requirement under the Amended Surveillance Camera Code March 2022 to ensure that there must be as much transparency in the use of surveillance camera systems as possible, including a published contact point for access to information and complaint. As such we will ensure that for every system we operate, signage will be provided, which in addition to confirming CCTV is in operation, will identify who to contact for further information.
- 9.2. The Code also state that surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use. We will ensure that for every system we operate the access to images and information is restricted to few authorised personnel and the handling of images and data stored is handled in accordance with the UK General Data Protection Regulation and the Data Protection Act 2018.

## **Procedural Guidance**

This guidance sets out how designated Town Trust staff should carry out their responsibilities in relation to Surveillance Camera Technologies in order to meet the requirements of our Policy.

## **Privacy Impact Assessment (PIA)**

These must be completed by the Buildings and Facilities Manager prior to any proposed new installation or enhancement of an existing CCTV system. All PIAs must be approved by the Chief Executive, to ensure that this is appropriate to the needs of the organisation and meets both the purposes and appropriate use of any CCTV systems (as identified in para 2 and 3 of the Policy). Town Trust PIAs are contained within the CCTV Policy folder.

These PIAs should be reviewed at least every other year, to ensure that their use remains proportionate and justified.

## **Training**

Training will be carried out by the Buildings and Facilities Manager for all those identified as Operators. This training is to ensure that everyone is aware and comply with the Policy and procedures. Training will include details for recording and retaining images, the handling of images securely and dealing with image access requests from the police and third parties.

### **Biennial Assessment**

Every two years, the Buildings and Facilities Manager will assess the PIAs to evaluate the effectiveness of the systems and whether or not the Surveillance Camera Devices are adequate to achieve the Scheme's purpose.

If the Buildings and Facilities Manager determines that a, or number of Surveillance Camera Devices are not adequate, they may confirm that such equipment is no longer used.

### **Audits**

Periodically the Buildings and Facilities Manager may carry out random checks. The aim will be to confirm the operation of the Scheme and compliance with both the Procedural guidance and Policy. These checks will consider:

- Whether the scheme purposes are being achieved.
- Whether the release of information has been appropriate.
- Any complaints received in relation to a particular system.
- Compliance with procedures by operators and other staff.

### **Access to images**

All access to images must be logged. This includes:

- All checks on whether the systems are operating
- Any image downloads (see form in Appendix 1)

Operators may receive contact direct from members of the public seeking copies of images from the Surveillance Camera Systems. When this occurs, the Operators needs to secure the footage, whilst the requestor follows the information request process.

Requests will be determined by the Chief Executive, and handled in accordance with this guidance, the Policy and Data Protection Policy.

### **Freedom of Information Act/ Environmental Impact Requests**

In the event that the request has been made under FOIA / EIR then the Chief Executive should, prior to responding to the requestor, consider the following:

- Is this request for the requestor's own information? If so, then this should be treated as a subject access request and recorded as such.
- Can the information be located? If not go back to the requestor to clarify. If it still cannot be located, inform the requestor that the information is not held

- Do the images include personal data of third parties (e.g. registration numbers, images of people that are recognisable)? If so, it is unlikely to be appropriate to disclose the images, unless the images are of a crowded place where there would not be an expectation of privacy.

In the event that the images cannot be disclosed, the requestor should be issued with a refusal notice.

### Subject Access Requests

In the event that the request has been made under the DPA then the Chief Executive should consider the following:

- Do you have the relevant proof of identify to be able to disclose the information? If not, go back to the requestor to obtain it.
- Can you locate the information being requested? If not, go back to the requestor to clarify.
- Do the images include the personal data of third parties (e.g. registration numbers, images of people that are recognisable)? If so, then you will need to make a judgement as to whether or not it would be appropriate to disclose the images, having had regards to what information the requestor already knows from being present at the location of the camera.

Requests may also be made by insurers or other parties on an individual's behalf. Provided they can demonstrate that they have the relevant consent, the request should be processed as above.

### Release of information to statutory prosecuting bodies

If the request has been made under the DPA then the Buildings and Facilities Manager should consider the following:

- Has the statutory body filled in the appropriate organisational disclosure form? If not, go back and ask them to do so, as they may not be able to rely on the footage as evidence if it has not been appropriately obtained.
- Can you locate the information being requested? If not, go back and ask for more information.
- Are you satisfied that the purposes that they are seeking the images for are compatible with the scheme purpose? If not, you should not disclose the image.

### Internal requests

Internal requests from employees for images in public locations (i.e. where personal data of members of the public may also be included) should be treated as an FOIA or DPA request.

Where the personal data is of another employee, careful consideration should be given to whether disclosure is appropriate, particularly where the person themselves is not present (e.g. damage caused to a vehicle whilst it is parked). In such circumstances it may be appropriate to direct the individual to the Police or their insurers to obtain the footage on the basis of legal action being contemplated. In limited circumstances, at the sole discretion of the person with responsibility for managing the cameras, the Operator may review the footage to see if an Incident occurred in order to enable the individual to determine whether they wish to refer the matter to the Police or their insurers.

In exceptional circumstances, access to recorded images will be authorised to managers who are investigating disciplinary offences against a member of staff. Such authorisation can only be given by the Chief Executive.

Document created February 2022  
Reviewed by A&G March 2023  
Reviewed by A&G March 2024



## CCTV Access Request form

### How third parties can access information from us.

This form is to be used by police, solicitors or court representatives requesting CCTV footage for investigations or court proceedings.

### Contact details

Full name of police officer or third party \*

Police officer badge number

Police station

Address of third party (including full postcode) \*

Crime Incident ref no, or Court case ref no \*

Telephone no. \*

Work email \*

Give details of the incident under investigation or subject to court proceedings \*

**Information to enable us to deal with this request**

Location of the CCTV camera (e.g. the address or location) \*

If you're seeking access to a particular image (if known) please indicate below:

Date and time the image would have been recorded (please estimate)

Please provide description of the person or incident you are investigating

STRATFORD TOWN TRUST  
CCTV POLICY  
February 2024

---

If known, please provide the name of the Stratford Town Trust employee you have been dealing with about this incident or investigation

**Declaration**

Please tick the box to declare that the information given in this form is true \*

**I confirm that I am making this request under one of the following exemptions in DPA 2018 Schedule 2 (please tick which one applies)**

- For crime and taxation purposes, OR
- By order of the court or for legal advice/ proceedings

Date \*

Requestor: \_\_\_\_\_  
Please print

Signed: \_\_\_\_\_