POLICY IDENTIFICATION PAGE

Is Public disclosure approved? Yes

Policy title: External CCTV Network Policy
Policy reference number: PO.2021.07.28.1 **Issue number: 1** **Last review date: July 2021** **Next review date: July 2024** **Underlying procedures:**
Chief Officer: Robin Smith **Policy written by:** Third party **, Data Protection Officer** **Department responsible: Uniform Operations** **Policy Lead:** Third party **Links to other policies:** **The UK Home Office's "Surveillance Camera Code of Practice" available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf**

1. Introduction

1.1 This policy details the standards for the use of the St Helier Town Centre and outlying districts' CCTV network (hereinafter referred to as the "External CCTV Network"), which officers and staff must adhere to. This policy has been designed to ensure that the External CCTV Network is managed effectively and regulates how the system is to be used. This is an essential document to ensure that both personal privacy and civil liberties are respected and preserved.

1.2 The External CCTV Network is owned and operated by the States of Jersey Police (SOJP) and is compliant with the Data Protection (Jersey) Law 2018 (DPJL) (see section 2), the Human Rights (Jersey) Law 2000 (see section 3), and the UK Home Office's Surveillance Camera Code of Practice. SOJP Chief Officer is the controller, as defined by the Data Protection Law, for this network.

1.3 The system will be operated in a manner that is sensitive to the privacy of the people using, living and working in the area covered by the network.

1.4 This policy does not apply to the following CCTV networks:-

- Within the States of Jersey Police Station, Route Du Fort, or its immediate vicinity. This is installed for the primary purpose of the security of the Police station.
- The Custody CCTV system.
- The Jersey Customs and Immigration Service/ SOJP CCTV systems located at the Airport and Harbours.
- Automatic Number Plate Recognition (ANPR).
- Body Worn Video (BWV).

The above systems are governed by their own separate policies.

1.5 Overall responsibility for the management and administration of the External CCTV network rests with the Superintendent of Operations.

2. Data Protection Principles

1. Lawfulness, fairness and transparency.
2. Purpose limitation.
3. Data minimization.

4. Accuracy
5. Storage limitation.
6. Integrity and confidentiality.

3. Human Rights (Jersey) Law 2000

3.1 Article 8 protects individuals' rights to respect for private life; however, this is a qualified right. This means that a public authority can sometimes interfere with their right to respect for private life if it is in the interest of the wider community or to protect other people's rights. Justification for interference of these rights may include the protection of other people's rights, public safety, prevention of crime and protection of health. The interference must be no more than what is necessary. Full consideration to the requirements of Article 8 has been given in the design, installation and use of the external CCTV infrastructure.

3.2 All police officers and staff must ensure that at all times, and in all instances, any such interference with a data subject's human rights are necessary and proportionate.

4. Confidentiality

4.1 All officers engaged in the management and operation of the External CCTV Network will ensure that all information gained during the course of this work remains confidential at all times.

4.2 Officers will not discuss with, or disclose to, unauthorised personnel any aspect of their work. Any breaches will be dealt with as a serious disciplinary matter.

5. Purpose of the External CCTV Network

To assist and enhance SOJP's ability to undertake its core policing duties to:-

- Protect life and property
- Preserve order
- Prevent the commission of offences
- Bring offenders to justice

- Undertake any duty or responsibility arising from common or statute law

6. Camera Locations

6.1 The siting of cameras is designed to assist with maximising SOJP's ability to perform its core policing duties and to minimise potential access to private premises. Cameras will be situated in fixed positions, in areas to which the public have unrestricted access and within public view. No camera will be hidden or obscured and, as far as possible, all cameras should be out of risk from malicious damage.

6.2 A full list of cameras linked to the External CCTV Network, and their locations, can be found at Appendix 1.

7. System specifications

Images are received in the Combined Control Room (CCR) and recorded digitally onto a server-based system. CCTV recording is at 25 frames per second. Cameras are capable of panning, tilting and zooming (PTZ). Footage is subject to both live and recorded monitoring. There are no audio recording or facial recognition capabilities.

8. Transparency

8.1 Members of the public must be made aware of the existence of the External CCTV Network. Maximum deterrent value will be achieved by having cameras clearly visible. Information as to the location of all cameras will be published on the SOJP website. No hidden cameras will be used within the network.

8.2 Suitable signage must be erected at the entrances to, and/or within each network's zone. These signs:-

- must be clearly readable and visible
- state that SOJP are operating the cameras
- state the purpose of the network
- provide information on how to contact SOJP

9. Restrictions on Use

9.1 The individual's entitlement to go about their lawful business is respected and supported, and this is the primary consideration in the operation of the system. There is inevitably some loss of privacy when CCTV cameras are installed. Cameras will not be used to monitor progress of individuals in the ordinary course of lawful business in the areas under surveillance. Individuals will only be monitored for a genuine policing purpose as defined in Section 5.

9.2 Some cameras are positioned in areas that include residential areas. Individual right to privacy within private premises is significantly greater than when in a public area. Cameras must never be focused on such private premises unless required to support operational response to a serious incident that has or is occurring within those particular premises.

10. Combined Control Room

10.1 Live data will be relayed back to the CCR by private network connections and will be available to police staff on duty within the CCR. Police staff working within CCR are authorised to move any camera in response to immediate events or circumstances.

10.2 Police staff may make live footage available to Ambulance/Fire CCR Operators only if such incident requires a response from either of these emergency services.

10.2 Access to CCR is strictly controlled. Only staff working within CCR or those with regular and genuine policing purposes are granted access with a "swipe card". The entry to and exit from CCR of all officers will be recorded by their individual swipe card, and this control must not be by-passed by "tailgating". A list of authorised officers is maintained.

10.3 Any officer attending CCR, whose swipe card does not provide access, and any escorted or unescorted visitor must ensure the date, time, duration and purpose of their visit is recorded in the Visitor's Log Book. By signing the Visitor's Log Book, the visitor is also signing a declaration of confidentiality. The CCR Supervisor is obliged to ensure this logbook is maintained. No visitor may enter and remain in CCR unsupervised.

10.4 The Police CCR Supervisor is responsible for ensuring that this policy is adhered to, and that access is strictly controlled and recorded.

Visitors may only access CCR with the Police CCR Supervisor's permission.

10.5 Operators must, if maximum operational benefit is to be obtained from the system, as well as observing individual privacy rights, be mindful of the position in which the cameras are left if not in use. When resting, each camera should provide a wide view of the particular public area. Private premises must be avoided (see 9.2).

11. Officer Training

11.1 SOJP will ensure that all officers and staff are trained to a proficient level before they are allowed to take up a position in CCR. All training will be provided and supervised by persons qualified and experienced in all aspects of the management and operation of the CCTV system.

11.2 CCR officers and staff will be appropriately trained on the implementation of this policy.

11.3 SOJP will ensure that all its CCR officers and staff are provided with regular refresher training to ensure that the highest operating and management standards are maintained. Training records are maintained for each officer engaged in CCR.

12. Public Access to Information

12.1 Persons whose images are recorded on the SOJP External Network may be entitled to request access to the CCTV recordings under the provisions of the Data Protection (Jersey) Law 2018. Individuals requesting such information should be asked to complete the relevant request for which is available at https://jersey.police.uk/accessing-information/personal-information-access/subject-access/ . Such requests should be forwarded to the Compliance and Audit Officer who will decide the appropriate level of response and whether such images need to be edited to protect the right to privacy of other individuals.

12.2 As a public authority, SOJP may receive requests for information under the Freedom of Information (Jersey) Law 2011. Such requests should be forwarded to the States of Jersey Freedom Of Information Central Referral Unit at https://www.gov.je/government/freedomofinformation/pages/makefoirequest.aspx

13. Defence Legal Advisors/Defendants

Disclosure to defence legal advisors or defendants will be considered in the following circumstances:

- Where there is a prosecution and CCTV footage is being exhibited as evidence.
- Where the defence claim the CCTV footage undermines the prosecution case or assists the defence case. No material will be released until the officer in the case has consulted the CJD Disclosure Unit and the prosecutor.
- Disclosure of CCTV footage may, at the discretion of SOJP, also be made for additional legal proceedings that do not fall into the above categories, or by court order. A charge may be made for such services.

All disclosures for legal proceedings will be handled by the Criminal Justice Department (CJD) Disclosure Unit.

14. Other third party sharing

Other law enforcement agencies, such as Jersey Customs and Immigration or Ports of Jersey may request recorded footage as part of their own investigations. If there is any doubt about the suitability of release, advice should be sought from the Compliance and Audit Officer.

15. Retrieving CCTV and audio recordings

15.1 Only police personnel trained and authorised to view CCTV system will be able to extract recorded images.

15.2 All requests to view or download images will be made on the electronic "Authority to View CCTV Recording" form on the relevant Masterfile. The requesting officer will set out the reasons for the request, and include the date, time, and location of the incident. The request must be approved by an officer of the rank of Sergeant or above (or equivalent). Authority may be granted only if the request is considered to be proportionate, legal, appropriate and necessary. Where a request is approved, any relevant footage will be exported to the relevant Masterfile.

15.3 This process will be fully auditable to provide transparency and ensure accountability.

16. Retention Period for Downloaded CCTV and audio recordings

16.1 Recordings which may be relevant to an investigation must be retained until a decision is taken whether to institute legal proceedings against a person for an offence.

16.2 If a criminal investigation results in proceedings being instituted, all material which may be relevant must be retained at least until the accused is acquitted or convicted or a decision is taken not to proceed with the case.

16.3 Where the accused is convicted, all material which may be relevant must be retained at least until:

- The convicted person is released from custody, and
- Six months from the date of conviction, and
- Six months after any appeal against conviction

17. Retention Period for Non-downloaded CCTV

The DPJL requires that personal information must not be kept for longer than is necessary. The relevance of CCTV footage is not always immediately apparent in a criminal investigation. To ensure that evidential footage is not lost, recorded data that has not been exported to a relevant Masterfile will be kept for 60 days, before being automatically and securely disposed of.

18. Audit and Review

18.1 An audit of the system may be carried out by the Compliance and Audit Officer to ensure the system's effectiveness and continuing justification. The audit will include CCR visitor record keeping, effectiveness of individual cameras, and supervisor authorities to view and download CCTV footage.

18.2 Any aspects of this policy may be subject to review following the outcome of an audit.

19. Personal responsibility

19.1 The use of the CCTV network is a valuable tool for policing. SOJP management will fully support each operator's use providing this policy has been followed.

19.2 Obtaining or disclosing personal data outside the terms of this policy is likely to amount to a personal data breach as defined in Article 1(1) of the DPJL. An officer who blatantly misuses the system for a purpose other than policing (see Section 5) may even commit a criminal offence as defined in Article 71 of the DPJL.

19.3 Any breach of this policy should immediately be reported via the ***Report Security Incident*** button on the intranet home page. Such reporting will assist to identify any shortcomings in training, and whether or not it is necessary to formally inform the Jersey Office of the Information Commissioner, etc.

20. Changes to the Network

20.1 Before any major technological improvement is proposed, any extension, or any change to the location of any camera, a full data privacy impact assessment (DPIA) in accordance with Article 16 of the DPJL must be conducted.

20.2 Where applicable, any changes must comply with planning restrictions.

21. Responsibility for the External CCTV Network

21.1 Overall technical responsibility for the External CCTV Network, which includes day-to-day operation and integrity of the system, rests with the IT Senior Infrastructure Manager.

21.2 Officers working within CCR should ensure that the system is working satisfactorily and report any issues without delay.

APPENDIX 1 – CAMERA LOCATIONS

1. Charing Cross / King Street Junction

2. King Street

3. Broad Street / Conway Street

4. King Street / Don Street Junction

5. Queen Street / Halkett Street Junction

6. Bath Street/ Hilgrove Street junction

7. Bath Street/ Minden Street junction

8. Minden Place / Minden Street Junction

9. Beresford Street / Cattle Street Junction

10. Halkett Place/Waterloo Street junction

11. Burrard Street

12. New Street

13. New North Quay / La Route De Liberation / Liberation Square

14. Weighbridge

14A. Mulcaster Street

15. Caledonia Place / Weighbridge

16. Esplanade / Liberation Square

17. Gloucester Street / Esplanade Junction

18. West Park / Victoria Avenue

19. Waterfront (opposite Cineworld)

20. Esplanade Carpark / Route De Liberation roundabout

21. La Route De Part Elizabeth roundabout (outside Maritime House)

22. The Parade / Gloucester Street Junction

23. Snow Hill / La Motte Street Junction

24. Parade Gardens

25. Hill Street/Halkett Place junction

26. Colomberie/Grenville Street junction

27. Royal Square

28. West Centre/Beresford Street/Bath Street/Peter Street junction

40. Castle Quay grass area

41. Castle Quay Marina

42. Jardin De La Mer

43. Jardin de la Mer car park

48. Gorey

49. St Aubin

xx. Harve des Pas