Policy Title
CCTV Policy

Policy Owner	Owning Dept
Nicky Nelson	Legal

Last Updated	Next Review Date
01/02/2023	01/02/26

Reason for Policy

This policy outlines the purpose, use and management of CCTV systems on RNLI premises and details the procedures to be followed in order to ensure the organisation complies with relevant legislation and guidance.

Objective of Policy

To provide a framework to ensure the RNLI install, operate and monitor CCTV cameras and footage in line with statutory requirements.

Scope and Applicability

All staff and volunteers and involved in the installation or management, or usage of CCTV Camera on RNLI premises.

Policy

1. Policy Introduction

The organisation owns Closed Circuit Television Systems (CCTV) that are managed by the RNLI and it's appointed agents at RNLI locations primarily to:

- protect the RNLI's buildings and assets
- increase personal safety and reduce the risk of crime.
- support law enforcement bodies in a bid to deter and detect crime
- assist in identifying, apprehending and prosecuting offenders
- protect members of the public and private property.
- in accordance with the RNLI Disciplinary Policy and/or the Volunteer Problem Solving Policy

CCTV footage will not be used for any other purposes and its use will be reviewed regularly.

CCTV images will be retained for a period no longer than 31 days, after which they will be disposed of, unless there is an ongoing reason to keep them for the purposes named above.

Images from CCTV are stored securely and can only be accessed by authorised individuals. With the exception of law enforcement bodies, auditors or insurance companies in the instance of damage to property, images will not be provided to third parties.

The RNLI is the 'data controller' for the images produced by the CCTV system. The RNLI is registered with the Information Commissioner's Office and operates to meet the requirements of the Data Protection Act and the Information Commissioner's guidance.

2. Procurement

To raise a request for a new system, see the IT Self Service page on Compass and submit a CCTV request, a risk assessment will then be carried out to determine what is required.

Donations of systems will not be accepted unless in line with approved RNLI systems.

3. Camera sites

The RNLI operates CCTV at a number of locations across its estate.

- Across the RNLI Poole Support Centre, West Quay Road Poole
- Regional Bases (RNLI RB)
- Support Centres (RNLI SC)
- Inshore Lifeboat Centre (ILB)
- Lifeboat Stations (LBS)
- Lifeguard Stations (LGS)
- Any other RNLI site (whether single occupancy or shared) (e.g. museum, shop, etc.)

4. Camera locations

- Cameras (fixed and dome) are located at strategic points throughout the RNLI estate, principally at the perimeters, entrance and exit points of buildings.
- Cameras must be located in such a way that it only monitors those spaces which are intended to be covered by the equipment.
- Permission must be obtained from adjoining landowners if cameras are required to capture images beyond RNLI land boundaries.
- Cameras must be restricted so that operators cannot adjust or manipulate them to overlook spaces which are not intended to be covered by the scheme.
- Where practicable, systems must be capable of masking neighbouring spaces to prevent inadvertent collateral intrusion.

5. Signage

Warning signs, as required must be placed at access points to areas covered by the CCTV System to inform of the existence of the system. The following locations required the following signage:

- Lifeboat stations, shop. See Appendix A
- Beach huts and car parks. See Appendix B

6. Storage and Retention of Images

- The recorded images shall be stored on secure systems in a place to which access is restricted and controlled.
- Any copies made for evidential purposes must be stored in a fire-proof safe/container to ensure their safety.
- Images and footage must not be retained for longer than a maximum of 31 days unless there is a legal reason to do so.
- CCTV footage retained for the purposes of disciplinary processes will be retained until the expiry of two years following the completion of all disciplinary procedures, including any appeals process and statutory reporting to professional bodies.
- The standard required retention period is:
    - Sites with 24-hour operational security staff - 31 days
    - Sites with no 24-hour operational security staff - 31 Days.

7. Management of Poole Support Centre Security Gatehouse Control Room

- When not manned the Control Room must be kept secured.
- Access to the Control Room will be limited to authorised personnel while recorded data is being viewed.

- If out of hours emergency maintenance arises, the System Manager must be satisfied of the identity and purpose of contractors before allowing access to the Control Room. Details of visitors including time/data of entry and exit will be recorded.
- The System Manager(s) must satisfy themselves over the identity of any other visitors to the Control Room and the purpose of the visit. Where any doubt exists access will be refused.
- Images displayed on monitors must not be visible from outside the Control Room and access to the Control Room is strictly limited.
- All Security staff working in the Control Room must be aware of the sensitivity of handling CCTV images and recordings.
- Detailed procedures for the management of the CCTV System are included in the overall Control Room Standard Operating Procedures "SOPs".

8. Covert recording

The use of covert cameras will be restricted to the rare occasions where a series of criminal acts have taken place in an area not normally covered by CCTV. A request to use covert cameras will clearly state the purpose and will require the written authorisation of the relevant Director, the RNLI Data Protection Officer, and, where this may involve members of staff, the Head of People Services.

Covert surveillance may be carried out in cases of suspected specific criminal activity only, where the objective of making the recording would be seriously prejudiced should the individual(s) concerned be informed of such surveillance.

Any covert recording authorisation must be reviewed every 14 days.
Any decision to use covert surveillance for any reason must be fully documented and records of such decision retained securely.

9. Applications for Disclosure of Images

Disclosure of recorded material will only be made to third parties under the lawful basis of legal obligation. All such requests must be referred to data_protection@rnli.org.uk for processing.

- Viewing of live images on monitors must be restricted to the operator.
- Recorded images can only be viewed by authorised staff in a restricted area.
- Requests for staff to view images must be authorised via data_protection@rnli.org.uk. If authorisation is agreed a CCTV Images Form must be completed, logged and stored securely.
- Images will only be released to the law enforcement bodies on the clear understanding that the recording remains the property of the RNLI.
- Applications received from any outside bodies (e.g. solicitors, insurers, media) to view or release personal data stored by the RNLI will be referred to data_protection@rnli.org.uk
- At no time will unauthorised persons be permitted to view recorded images or live feeds.

10. Subject Access Request

Anyone who believes that they have been filmed by the CCTV System can request to see the recording by contacting; data_protection@rnli.org.uk. Any such requests received must be forwarded to the Data Protection Team immediately to ensure statutory time periods for completion can be met.

11. Use of CCTV for disciplinary purpose

Only in the following circumstances may CCTV footage may be used in disciplinary proceedings

- CCTV footage reveals activity that the RNLI could not reasonably be expected to ignore, Acts which constitute Gross Misconduct in accordance with the RNLI's Disciplinary Policy.
- Practices which seriously jeopardise the health and safety of others.

Access given to the employee during disciplinary proceedings:

- CCTV footage identified will be presented to the employee. Therefore, the employee will not be required to make a Data Subject Access Request to view the CCTV footage as part of this procedure.
- 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 make representations with regard to the CCTV footage in any disciplinary hearing.

Definitions

For ease of use this policy utilises the definitions set out in the General Data Protection Regulation which have been incorporated into the UK Data Protection Act 2018. The most relevant/important of these definitions are:

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'CCTV' means close circuit television used to survey and monitor RNLI buildings and property.

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Roles and Responsibilities

DPO – Data Protection Officer.
The DPO is responsible for advising the organisation, its staff and volunteers of their data protection responsibilities and ensuring the organisation manages personal data lawfully. The DPO reports directly to the Executive Team on RNLI's data protection risk and compliance status.

Accountable Data Executive
The Accountable Data Executive (at Director level) is ultimately accountable for the legal, ethical and effective use of defined data entities which are assigned to them. In addition, they are accountable for all processes consuming data within their business stream.

Data Owner
Appointed by the Accountable Data Executive, the Data Owner has delegated accountability for governing the collection, use and management of data within a defined data set or within a specific process.

Data Manager
The Data Manager is appointed by, supports and deputises for the Data Owner. They are responsible for the day-to-day operation and management of processes involving (creating, updating, utilising, removing, etc.) data.

Data Steward
The Data Steward supports the understanding, embedding and operation of the Data Governance principles and other initiatives within the department they represent.

Appendices

- Appendix A - Lifeboat Station Signage
- Appendix B - Beach huts and car park Signage

Related Policies, Procedures & Guidance

- CCTV Procedures for Regional Lifeboat, Lifeguard, Retail and Other Premises
- RNLI SOP 40
- RNLI SOP 42
- Data Protection Policy
- Information & Data Retention Policy
- Information Security Policy
- Acceptable Use Policy
- Data Governance Policy
- RNLI Privacy Policy
- Data Subject Request Procedures
- Data Protection Impact Assessment Procedures