

Data Protection Policy of the Irish Railway Record Society in respect of the use of CCTV in its Heuston Premises

Risk Analysis

The Board of the Irish Railway Record Society (the Society) has identified the following risks:

- It holds an extensive collection of books, drawings and archives which have significant historical and monetary value and which in many cases are unique or rare.
- It has a duty to protect that collection for the Society and as part of Ireland's heritage.
- Many of the items in the collection are small and capable of being easily concealed and removed from the premises.
- Between June 2011 and September 2016 there have been 89 occasions recorded in the Society's incident logs on which the security of the premises was compromised for a variety of reasons, including the alarm not being armed and windows and doors not being properly secured. The use of CCTV will provide a second line of defence in the event of a failure of the primary security measures.
- The Society's premises are used for meetings and research and have a significant throughput of persons who have an expectation that their property will be safe while on the premises.
- The premises are currently shared with staff from Irish Rail which means that persons other than members of the Society and its visitors have access to the shared common areas.
- The Society's portion of the premises is only occupied for a relatively short period each week. The premises are located in a relatively remote part of the station complex and there is little vehicular or pedestrian movement in the vicinity outside of office hours. CCTV will permit remote monitoring of the premises while unoccupied.
- The Society is a voluntary body which employs no staff and does not have the financial capability to employ staff. It depends entirely on the voluntary efforts of a small number of volunteers. Only limited surveillance can be provided by volunteers and then only at the cost of diverting them from work relevant to the Society's objectives. CCTV will support those volunteers in ensuring the security of the premises and leave them free to pursue work relevant to the Society's objectives.
- In the event that a breach of security occurs CCTV will provide valuable information to enable an effective investigation and prosecution where an offence is detected. It will also provide information which can be used to improve the security of the premises.

In the light of this analysis the Board of the Society has concluded that the installation of CCTV for the purpose of securing the premises, the library and archive collections and the property of persons on the premises is justified.

Privacy Analysis

The Board of the Society has considered how best to achieve a balance between the right to privacy for persons on the premises and the security of the premises, the library and archive collections and personal property. It has concluded that this balance can best be achieved by:

- Limiting the locations covered by CCTV to the minimum consistent with ensuring the effective security of the premises, the library and archive collections and personal property;

- Ensuring that CCTV is not used in places where people have a right to privacy, particularly toilets;
- Collecting CCTV data only for the purpose of protecting the security of the premises, the library and archive collections and personal property;
- Keeping the CCTV data secure and strictly limiting access to it;
- Retaining CCTV data for no longer than 30 days unless required for the investigation of a specific incident;
- Providing notices on the premises alerting persons to the use of CCTV;
- Providing a right of access to personal CCTV data.

Consistent with this analysis:

- CCTV cameras have been installed at the following locations: facing the front door, at the top of the stairs, in the library and in the back corridor.
- Only the following persons are authorised by the Board to have access to CCTV data collected on the Society's premises: Alan Hyland, Tim Moriarty, Anthony O'Shaughnessy and Michael Walsh.

Privacy Policy

Purpose of our Policy

The Irish Railway Record Society ("the Society"), in its capacity as a data controller, has a legal obligation to comply with the Data Protection Acts.

Scope of our Policy

This policy concerns the collection and retention of CCTV data relating to the Society's premises at Heuston Station, Dublin 8.

The provisions of the Society's overall Data Protection Policy apply to the collection and retention of CCTV data. This policy concerns matters specific to the use of CCTV and does not restate matters which are adequately covered in the overall policy.

Purpose for which CCTV is used

CCTV is used and CCTV data is collected and retained only for the purpose of protecting the security of the premises, the library and archive collections and personal property and for the investigation or detection of an alleged breach of such security or the law.

Notification of CCTV Use

Signs notifying persons that CCTV is in use on the premises will be provided. They will be in prominent positions, easily readable and well lit.

Data Controller

To ensure compliance with Data Protection Acts and the implementation of this policy, the Society has designated Michael Walsh as Data Protection Officer. All enquiries relating to the holding of CCTV data should be referred to him in the first instance.

Authorised Persons

The following are the only persons authorised by the Board to have access to CCTV data collected on the Society's premises:

Alan Hyland
Tim Moriarty
Anthony O'Shaughnessy
Michael Walsh.

Where an issue arises relating to the security of the premises which appears to require action by CIE as landlord, the Society's Data Protection Officer may, as an exceptional measure, grant access to the CCTV data by a CIE representative. The access granted shall be the minimum required for the specific purpose and shall be supervised by one of the authorised persons named above.

Security of CCTV Data

Only the persons named above will have access to the live CCTV feed and to retained CCTV data.

The retained CCTV data will be securely stored and a log of all access to it will be kept.

Retention of CCTV Data

CCTV data collected on the Society's premises will be retained for a period not exceeding 30 days unless it is required for the investigation or detection of an alleged breach of security or the law.

Access to CCTV Data

Access to CCTV data will only be provided to:

- Authorised persons as specified above;
- A CIE representative in the specific circumstances stated above;
- An Garda Siochana;
- Persons requesting access to their own personal data.

No other person will be permitted to access to CCTV data.

Garda Siochana Access to CCTV Data

The Garda Siochana will only be provided with a copy of CCTV records in response to a formal written request to the data controller stating that they are investigating a criminal matter. For practical reasons, and to expedite a request speedily in urgent situations, a verbal request may be sufficient to allow the release of a copy of the data requested but it must be followed up by a written request. The data controller may permit the Garda Siochana to view, as distinct from obtaining a copy, of CCTV data without a formal written request.

Requests for Access to Personal CCTV Data

Requests for access to personal data will be dealt with under the Society's overall Data Protection Policy, subject to what follows.

A person requesting access to personal CCTV data should, as far as possible, provide details of the approximate time and the specific date(s) on which their image was recorded. The request should be made within 30 days of the date in the light of the Society's policy on the retention of CCTV data.

The personal CCTV data will be provided in the form of video footage. If the data is technically incapable of being copied to another device, or in other exceptional circumstances, stills will be provided from the CCTV data.

Where the requested personal CCTV data contains images of other persons:

- Their images will be pixilated, redacted or darkened out so as to prevent identification; or
- The consent of the persons affected will be sought to release an unedited copy of the data.

Updating and Review of our Policy

This policy will be updated at regular intervals to reflect best practice in data management, security and control and to ensure compliance with any amendments made to the Data Protection Acts.

Approved by the Board on 17 November 2016
Reviewed and updated by the Board on 16 July 2020
Next Review Date: July 2022