PSI
CUMANN CÓGAISEOIRÍ NA hÉIREANN
The Pharmaceutical Society of Ireland

AN RIALTÓIR CÓGAISÍOCHTA
THE PHARMACY REGULATOR

Closed Circuit Television Policy (CCTV)

October 2018

Table of Contents

1. Introduction

The purpose of this policy is to regulate the use of Closed Circuit Television (CCTV) and its associated technology, monitoring both the internal and external environs of the Pharmaceutical Society of Ireland's (PSI) premises, PSI House.

A copy of this CCTV Policy will be made available on the PSI website, provided to all PSI full time and temporary staff, Council, and Committee members. A copy will also be provided to visitors to PSI House, on request.

2. Scope

This policy is relevant to all personnel in, and visitors to, PSI House, Fenian Street, Dublin 2. Moreover, it relates directly to the location and use of CCTV, and the monitoring, recording and subsequent use of such recorded material.

The CCTV Policy is in place to enable Apleona (the PSI's facilities management service provider) to operate the CCTV system within the PSI.

This policy prohibits CCTV monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. gender, sexual orientation, ethnic origin, or disability. Furthermore, CCTV monitoring is limited to uses that do not violate the reasonable expectation to privacy as defined by law.

This policy prohibits the use of the CCTV network in PSI House to monitor members of PSI staff, or PSI office holders.

The CCTV cameras will be used to:

- protect PSI House and the assets held within it, both during and outside of operational hours (the system will be in operation 24 hours a day, every day);
- ensure the safety of PSI personnel, and visitors to PSI House;
- deter and detect crime; and
- assist in identifying, apprehending and prosecuting offenders.

The personal data recorded and stored by the CCTV system will be used only for the purposes outlined in this policy document. Collection, storage and use of CCTV footage shall be in compliance with the Data Protection Acts 1988- 2018 and the General Data Protection Regulation (the data protection legislation).

3. Data Controller

The PSI is the data controller in respect of images recorded and stored by the CCTV system at PSI House. The PSI's contracted facilities management service provider, Apleona, is a data processor for the purposes of this policy. The PSI Registrar has sole responsibility for monitoring the implementation of, and compliance with, the CCTV policy.

4. Lawful, Fair and Transparent Processing

The fair obtaining principles inherent in data protection legislation, require that those people whose images may be captured on camera are informed by having adequate signage in place in PSI House. Adequate signage will be placed at each location in PSI House where CCTV cameras are situated to indicate that CCTV is in operation (locations listed below). Signage shall include the name and contact details of the data controller as well as the specific purpose for which the CCTV camera is in place in each location. As well as this, the PSI Data Protection Officer will provide a copy of this CCTV Policy to PSI staff, Council, and Committee members, and on request to visitors to PSI House. The CCTV Policy is made available also in the Data Protection Statement on the PSI website, and in a Privacy Notice provided to PSI personnel and office holders.

5. Location of Cameras

CCTV cameras in PSI House are located in the following areas:

- Ground Floor Car Park
- Ground Floor Front and Rear Entrances
- Ground Floor Reception and Museum area
- Ground Floor Staircase 1
- Ground Floor Staircase 2 & Emergency Exit
- Ground Floor Corridor
- Lift Lobby on all floors
- 2nd Floor external to Evidence Storage room
- Staircase 1 at 1st, 2nd, 3rd & 4th Floors
- Staircase 2 at 1st, 2nd, 3rd & 4th Floors

Cameras are positioned so that they cannot capture non-relevant images in their vicinity (for example neighbouring properties, or passers-by).

6. Operation of the System

The system can only be accessed by authorised personnel from Apleona and IC Services Engineering (installers of system), and the PSI's ICT Unit. A Service Level Agreement has been put in place between the PSI and Apleona which details the terms of the contract including confidentiality agreements, data security and disclosure. The system is housed in a secure, locked room, which is accessible to facilities administrative staff, in addition to Apleona and IC Services staff, when required.

The system can be accessed remotely using a unique password only available to Apleona and IC Services. Access by IC Services is only by request of Apleona and must be logged.

Should the system be accessed or works conducted on it by unauthorised personnel or without Apleona instruction, this will be viewed as extremely serious and will be grounds for automatic termination of contract.

7. Data Protection, Storage and Retention

The data captured from the CCTV cameras is securely stored as electronic data. Typically, this data is recorded on a loop and will be retained for maximum of 30 days. It will be over-written after that period. However, data may be retained for longer periods where the events captured give rise to court proceedings.

Access to the data is restricted to authorised personnel (see Section 6 for list). The area where the data is stored is secured by swipe card access, with only the individuals identified in section 6 having access. The storage devices are password protected. Supervising the access and maintenance of the CCTV system is the responsibility of Apleona. Unauthorised access will be viewed as a data breach. In such an event, the PSI Data Breach Management Policy and Procedure will be followed.

8. Access Requests

Access to the CCTV system and stored images will be restricted to authorised personnel only (as indicated in Section 6). In relevant circumstances, CCTV footage may be accessed:

- By An Garda Síochána, where the PSI is required by law to make a report regarding suspected crime;
- Following a written request by An Garda Síochána when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place in PSI House;
- To data subjects (or their legal representatives) in response to an access request where the time, date and location of the recordings is furnished to the PSI;
- To individuals (or their legal representatives) subject to a court order;

- To the PSI's insurance company where the insurance company requires the same in order to pursue a claim for damage done to the insured property.

Any person whose image has been captured has a right to be given a copy of the information recorded, providing that such an image/recording exists (i.e. that it has not been deleted), and provided that an exemption/prohibition does not apply to the release. To exercise that right, a person must make an application in writing to the PSI using the Subject Access Request Form available on the PSI website, and provide proof of identity, and proof of address, giving a reasonable indication of the time period sought, and identifying the location of the camera. If the person is under eighteen years, the parent or guardian may make an application**.** Access requests must be responded to by the PSI within one month (30 days) of receipt.

Access requests can be made to:
The Data Protection Officer, The Pharmaceutical Society of Ireland, PSI House, 15-19 Fenian St, Dublin 2,D02 TD72
Email: dataprotection@psi.ie

When a subject access request is received, the relevant footage is copied and a specific retention time is assigned to this copy. In giving a person a copy of his/her data, the data controller may provide a still/series of still pictures, a tape or a disk with relevant images. However, other people's images should be obscured or blurred before the data is released. Data will be delivered to the requester ensuring that security measures have been considered and implemented. A log of access to images will be maintained. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data.

9. Providing CCTV Images to An Garda Síochána

With regard to requests from An Garda Síochána to download footage, the Data Protection Commission recommends that requests for copies of CCTV footage should only be granted when a formal written (or fax) request is provided to the PSI stating that An Garda Síochána is investigating a criminal matter.

For practical purposes, and to expedite response to an urgent request, a verbal request may be sufficient to allow for the release of the footage sought. However, any such verbal request must be followed up with a formal written request.

A log of all Garda Síochána requests will be maintained by the PSI and its data processors. Any such requests should be on An Garda Síochána headed paper, quote the details of the CCTV footage required and should also cite the legal basis for the request under the Data Protection legislation. Prior to the PSI issuing any CCTV images to An Garda Síochána, it will be discussed and agreed with the PSI's Data Protection Officer.

There is a distinction between a request by An Garda Síochána to view CCTV footage and to download copies of CCTV footage. In general, An Garda Síochána making a request to simply view footage on the premises of a data controller or processor would not raise any specific concerns from a data protection perspective.

10. Review and Approval of the CCTV Policy

This policy will be reviewed and updated regularly to take into account changing Data Protection legislation or guidelines.

Revision	Date	Description	Approved by
1	July 2016	Policy developed and issued to all staff, Council and Committee Members, placed on the PSI website and a copy made available at reception for visitors.	SMT
2	May 2018	GDPR Update	DPO
3	October 2018	Service provider update.	DPO

Appendix: Glossary of Terms

Subject Access Request (SAR) – this is where a person makes a request to the organisation for the disclosure of their personal data held by the PSI under the applicable data protection legislation.

Closed Circuit Television (CCTV) – is the use of video cameras to transmit a signal to a specific place on a limited set of monitors, generally for security purposes. The images may then be recorded on video tape or DVD or other digital recording mechanism.

The General Data Protection Regulation and Data Protection Acts 1988-2018 (together these can be referred to as the data protection legislation) Data protection legislation confers rights on individuals as well as responsibilities on those persons processing personal data. All staff must comply with the provisions of the data protection legislation when collecting, storing, sharing, or otherwise processing, personal information. This applies to personal information relating both to personnel of the organisation and individuals who interact with the organisation.

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a filing system or with the intention that it should form part of a filing system).

Personal Data – data (information) relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Data Breach - any event which results in the integrity or security of personal data being compromised. It can include loss or theft of electronic equipment on which personal data is stored, equipment failure, human error, mis-directed emails, loss or sharing of information, or a cyber-attack. Breaches also include accidental loss of personal data (e.g. fire and flood).

Data Controller - a person who (either alone or with others) controls the contents and use of personal data.

Data Processing - the umbrella term that refers to any operation or set of operations which is
performed on personal data or on sets of personal data, 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. Processing may or may not be by automated means.

Data Processor - a person who processes personal information on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data

controller out-sources work. The data protection legislation place responsibilities on such entities in relation to their processing of the data.

Data Subject – an individual who is the subject of personal data.